TURKS AND CAICOS ISLANDS
FINANCIAL SERVICES COMMISSION

PROLIFERATION FINANCING GUIDANCE
FOR
FINANCIAL INSTITUTIONS AND DESIGNATED NON-FINANCIAL BUSINESSES & PROFESSIONS

Contents

TERMINOLOGY

Proliferation

Proliferation is defined by the Financial Action Task Force (FATF) as the illegal manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling or illegal use of nuclear, chemical, or biological weapons and their means of delivery and related materials.

Proliferation Financing

Proliferation Financing (PF) is defined as the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials*(including both technologies and dual-used goads for non-legitimate purposes),* in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services, or expertise.

Proliferator

The 2010 FATF Status Report on Combating Proliferation Financing defines a proliferator as an individual or group of individuals that abuse both the formal and informal sectors of the financial system or resort to cash in order to trade in proliferated goods.

INTRODUCTION

Given the immense power of nuclear weapons (atomic weapons, radiation weapons), chemical weapons (such as poison gas) or biological weapons (such as natural toxins and pathogens, like the anthrax bacterium), which are referred to as weapons of mass destruction (WMD), international treaties have imposed restraints on the development and use of these weapons[1] because of their ability to eliminate large numbers of people in a short time.

WMDs have not only been pursued by countries but also by terrorists who seek to possess these weapons for committing or threatening attacks. For example, the well-known Muslim extremist and founder of Al Qa'ida, Osama Bin Laden, openly declared himself in favour of this idea.

Proliferation, or the spread of WMDs, does not only involve the development or purchase of WMDs and their means of delivery, but also buying or otherwise obtaining (procuring) the goods and knowledge required for WMD development. This procurement takes place mainly in industrialised countries[2] where high technology is available. Much of this technology can be used for both military and civilian purposes ('dual use').

Given the high technological level of products and knowledge in the industrialised countries, states and terrorists seeking to possess weapons of mass destruction are likely to see these countries as an interesting procurement area. However, countries like the TCI can be exploited by proliferators to enable financial flows or assist in the shipment of illicit goods, services and technology needed for the development of WMDs and their means of delivery.

Therefore, preventing proliferation financing is an important part of combatting proliferation. It is essential to disrupt the financial flows available to proliferators and to obstruct and complicate the procurement of the illicit goods, services and technology needed for the development of WMDs and their means of delivery.

This paper will outline the legal obligations of FIs and DNFBPs regarding proliferation financing, the characteristics that makes certain sectors more vulnerable to PF than others, as well as red flag indicators for PF. This paper will also outline preventative measures that FIs and DNFBPs can take under the TCI's AML/PTF framework.

---

1 See Annex 1

2 Oxford reference lists Canada, Japan, Turkey, Australia, New Zealand, the United States, and eighteen European countries: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, and the United Kingdom as industrialized countries.

SCOPE AND OBJECTIVES OF GUIDANCE

To whom does this Guidance apply?

This guidance applies to FIs and DNFBPs, which include the following categories of business and professions as listed in Schedule 2 of the AML Regulations:

- Banks
- Money Service Businesses
- Trust Companies
- Company Managers and Agents
- Investment Dealers
- Long Term Insurers
- Independent Legal Professions
- Accountants, Auditors and Bookkeepers
- Realtors
- Jewellers
- Pawn Shops
- Vehicle Dealers
- Boat Dealers
- Lenders
- Debt Purchasers
- Payment Service Providers

Related Guidance Documents

This guidance should be read in conjunction with the following documents:

- DNFBP Customer Due Diligence Guidance;
- the Commission's Guidelines on Risk Assessment;
- Targeted Financial Sanctions Guidance for Financial Institutions and DNFBPs;
- Financial Sanctions Guidance issued by the Attorney General's Chambers;
- TCI Financial Sanctions Survey Report;
- Anti-Money Laundering and Prevention of Terrorist Financing Regulations;

- Anti-Money Laundering and Prevention of Terrorist Financing Code;
- Anti-Money Laundering and Prevention of Terrorist Financing Guidance Notes;

STATUS OF THIS GUIDANCE

This guidance is supplemental to the AML Regulations and AML Code. It is not legal advice and is not intended to replace the AML Regulations and the AML Code. The guidance is intended for use by senior management and compliance staff of FIs and DNFBPs to assist in the development of internal systems and controls. Compliance with this guidance will be taken into consideration by the Commission when assessing an FI's or DNFBP's compliance with their legal obligations.

TCI PF LEGAL FRAMEWORK

In October 2020, the FATF[3] revised Recommendation 1 and its Interpretive Note (R.1 and INR.1) to require countries and FIs and DNFBPs to identify, assess, understand, and mitigate their proliferation financing risks (PF risk[4]). The FATF has also issued specific Recommendations that require countries to impose obligations on FIs and DNFBPs to implement preventive measures, including specific measures for compliance with targeted financial sanctions (TFS) related to PF. This is due to the fact that international trends reveal the abuse of FIs and DNFBPs by proliferators to enable the financing or the movement of goods to facilitate proliferation.

FATF Recommendation 7 requires countries to effectively implement TFS to comply with the UNSCRs relating to the prevention, suppression and disruption of proliferation and its financing. The obligations apply to two country-specific regimes for the DPRK and Iran and requires countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly to or for the benefit of (a) any person or entity designated by the United Nations (UN), (b) persons and entities acting on their behalf or at their direction, (c) those owned or controlled by them.

In addition, the FATF Recommendations require countries to enforce specific obligations on financial institutions (FIs) and DNFBPs and to adopt measures to effectively monitor and ensure compliance by FIs and DNFBPs with the relevant laws or enforceable means governing the obligations under Recommendation 7.

---

3 The Financial Action Task Force (FATF) is an inter-governmental organization that designs and promotes policies and standards to combat financial crime. Recommendations created by FATF target money laundering, terrorist financing, and other threats to the global financial system. FATF was created in 1989 at the behest of the G7 and is head-quartered in Paris.

4 The FATF Guidance on Proliferation Financing Risk Assessment Mitigation sets out that proliferation financing risk refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions (TFS) obligations referred to in Recommendation 7.

The FATF requirements under Recommendation 7 are set out in TCI law through the UK Terrorist Asset-Freezing etc, Act 2010, as extended to the TCI by the Terrorist Asset-Freezing etc. Act 2010 (Overseas Territories) Order 2011 and section 3 of the Prevention of Terrorism Ordinance (PTO).

The PTO applies to both natural and legal persons who are penalized in the same way for committing TF offences. Conviction for PF offences in sections 6 and sections 9 to 12 of the PTO occurs on indictment and carries a penalty of a fine or a term of imprisonment of 14 years or both. The following sections of the PTO make it an offence for a person (legal or natural), either aggregate or sole, and any club, society, association, or other body, of one or more persons[5], to –

- Section 6: be a member of a terrorist organisation[6];
- Section 9: raise funds for terrorism;
- Section 10: use and possess money or other property for terrorism;
- Section 11: arrange funds for terrorism;
- Section 12: arrange for the retention or control of terrorist property.

Part 3 of the PTO contains provision in sections 13-20 that makes it an offence if a person fails to disclose to the Financial Intelligence Agency (FIA), a police officer or customs officer as soon as is reasonably practicable his belief or suspicion that another person has committed an offence under any of sections 9 to 12; and the information on which the belief or suspicion is based. Section 16 makes provision for financial institutions' obligation to disclose information, and the conditions that must be satisfied for the offence of failure to disclose. A person guilty of an offence under sections 13 or 16 would be liable on conviction on indictment to a fine or a term of imprisonment of seven years, or to both. Legal persons may also be subject to civil and administrative liability and sanctions pursuant to section 33 of the FSCO.

Additionally, under section 127 (1)(a) of the POCO, FIs and DNFBPs have a duty to disclose where they know or suspect or have reasonable grounds to know or suspect that a person is engaged in money laundering, terrorist financing or proliferation financing. Section 128 of the POCO requires the Money Laundering Reporting Officer (MLRO) to make a disclosure to the FIA where he knows or suspects or have reasonable grounds to know or suspect that a person is engaged in money laundering, terrorist financing or proliferation financing. Section 29(1)(e) of the Anti-Money Laundering and Prevention of Terrorist Financing Code 2011 (AML-PTF Code) makes the MLRO duty bound to report suspicions of ML or TF activity as soon as is reasonably practicable and in any event within 24 hours to the FIA.

---

5 Section 3 of the Interpretations Ordinance

6 Section 2 of the Prevention of Terrorism (Amendment) Ordinance 2016 terrorist organization is defined to include an organisation proscribed under section 5 of the PTO or an entity, group of persons or an organisation that—

- participates as an accomplice in acts of terrorism or the financing of terrorism;
- organises or directs others to commit acts of terrorism or the financing of terrorism; or
- contributes to the commission of acts of terrorism or the financing of terrorism by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering acts of terrorism or the financing of terrorism with the knowledge of the intention of the group to commit acts of terrorism or the financing of terrorism.

The Terrorist Asset-Freezing etc. Act 2010 (Overseas Territories) Order 2011, in sections 11-15, provides that a person must not deal with or make funds, economic resources, or financial services available to designated persons[7] or for the benefit of designated persons. The Order further provides for the freezing of assets by financial businesses without delay, and for restrictions on the provision of financial services to designated persons or for the benefit of designated persons.

Regulation 17(2)(c)(iii) of the AML/CFT Regulations imposes an obligation on FIs and DNFBPs to determine whether a business relationship or transaction, or proposed business relationship or transaction, is with a person or entity sanctioned by the EU or UN. Where a FI or DNFBP discovers that it is engaged in a business relationship or transaction, or proposed business relationship or transaction, with a designated person or entity, the FI or DNFBP is required to comply with the Terrorist Asset-Freezing etc. Act 2010 (Overseas Territories) Order 2011 by –

i) Freezing such accounts or other funds without delay.

ii) Refraining from dealing with or making available, directly or indirectly, such funds or economic resources to the sanctioned individual or entity, unless a licence has been granted.

iii) Reporting to the Governor and the Commission that you are in possession or control of, or are otherwise dealing with, the funds or economic resources of a designated person.

Sanctions Orders have been implemented in respect of all the current UN Sanctions Regimes, including the Democratic People's Republic of Korea (Sanctions) (Overseas Territories) Order 2020 and the Iran (Sanctions) (Nuclear) (Overseas Territories) Order 2020.

Section 4(1)(d) of the Financial Services Commission Ordinance and section 161(3)(a) of the POCO establishes the role of the Financial Services Commission to monitor compliance by FIs and DNFBPs with their AML/CFT obligations set out in the AML/PTF Regulations and such other Ordinances, regulations, codes, or guidance relating to money laundering or the financing of terrorism. The referenced legislation requires FIs and DNFBPs to ascertain the risk of money laundering, terrorist financing and proliferation financing that they are exposed to, to apply appropriate internal controls to manage this risk, to keep records, to vet and train staff, and to periodically assess the effectiveness of their AML Compliance Program.

FIs and DNFBPs play a vital role in preserving the integrity of the TCI and the TCI's financial system. The identification, assessment, understanding, and management of PF risks by FIs and DNFBPs is essential to a robust AML/CFT regime. It is critical that every FI and DNFBP includes counter-proliferation financing (CPF) in their AML/CFT programme and risk management strategies.

[7] A designated person is an individual or entity listed under TCI law as being subject to sanctions. The list of designated persons can be found on the Office of Financial Sanctions Implementation website by clicking here.

PF vs ML and TF

Differences between Money Laundering, Terrorist Financing and Proliferation Financing:

	Money Laundering (ML)	Terrorist Financing (TF)	Proliferation Financing (PF)
Purpose	Use of illicit funds in the regulated system	Supports terrorist activities	Acquisition of WMD
Source of Funds	From illegitimate activities. Funded via the illicit activity of the criminal/criminal organisation ie corruption, tax evasion, the sale of drugs, robberies, ransomware attacks, illegal arms trade, prostitution etc. The crime may not have been committed in TCI Organised crime groups may collaborate with terrorists and may also be classified as proscribed terrorist organisations.	From illegitimate/legitimate activities Numerous funding streams, including, for example: – Sponsored by financier/benefactor sympathetic to the cause – Self-funded – Funds raised via commercial activities (e.g. web shops, music festivals) – Funds raised via organised fund-raising activities (e.g. via non-profit sector, social media, crowdfunding platforms, groups' own magazines) – Exploitation of natural resources in conflict zones (e.g. ISIL – Oil in the Middle East; Al-Shabaab – Gold in West Africa and Daesh – Timber in East Africa) – Looting and sale of cultural artifacts – Real estate (generating income, acting as an investment, and which certain terrorist groups use as club houses etc.) It is not unusual for terrorists to be involved in, or operating in close proximity to, conflict zones and criminal methods to raise funds tend to emerge, either in isolation or working with criminal groups (e.g. illicit smuggling, human trafficking, extortion, drugs trafficking and kidnap for ransom). The United Nations reports that during the COVID-19 pandemic cash smuggling to territories where Daesh was active became less prominent, whilst crypto transfers increased (e.g. using personal crypto wallets).	Often state-sponsored programs but also through fundraising activities by non-state actors

Conduits	Favours formal financial system	Favours cash carriers or informal financial systems such as Hawala and currency exchange firms.	Formal financial system preferred up until the point of entry into DPRK, where the money is taken out in cash in a neighbouring country and carried into DPRK. Additionally, the use of distributed ledger technology has become a widely used mechanism to settle transactions for DPRK.
Detection Focus	Suspicious transactions such as deposits uncharacteristic of customer's wealth or the expected activity	Suspicious relationships, such as wire transfers between seemingly unrelated parties	Individuals, entities, states, goods and materials, activities
Transaction Amounts	Large amounts often structed to avoid reporting requirements	Small amounts usually below reporting thresholds	Moderate amounts
Financial Activity	Complex web of transactions often involving shell or front companies, offshore secrecy havens, etc.	Varied methods including formal banking systems, informal value transfer systems, smuggling of cash and valuables	Transactions look like normal commercial activity, structured to hide connection to proliferator or proliferations activities
Money Trail	Circular-money eventually ends up with the person who generated it	Linear money generated is used to propagate terrorist groups and activities	Linear money is used to purchase goods and materials from brokers or manufacturers. The money can also move in the opposite direction (i.e., from the broker/manufacturer to the proliferator).

PF THREATS TO THE TCI

The TCI is not an industrialised country with high technology; accordingly, states and terrorists seeking to possess WMDs are not likely to see the TCI as a procurement area. On this basis PF threats to the TCI are likely to be external from state actors and non-state actors that seek to exploit the TCI's financial system, financial services businesses, gatekeepers, or transportation infrastructure to clandestinely finance, procure, ship, or trans-ship goods for use in the proliferation of WMD.

Based on reports from the UNSC Panels of Experts (PoE), PF risk assessments prepared by other countries, the most active PF threats have been states seeking to obtain or expand capabilities related to nuclear weapons and other WMD, although non-state actors also pose proliferation and PF threats. The current priority PF threats are:

i) State actors – Iran and North Korea have created global networks of front and shell companies and employ complex, deceptive methods to conceal their proliferation finance activity and evade international sanctions levied against them.

ii) Non-state actors - terrorist groups (e.g. Al Qaida) that have targeted countries for fundraising have at least stated an intent to pursue nuclear weapons and radiological materials.

FIs and DNFBPs may find it difficult to relate to PF and why they need to include PF risk in their AML/CFT compliance framework. Typologies have shown that designated persons and entities continue to explore new ways to evade targeted financial sanctions, regardless of the geographical proximity to proliferating states (i.e. the DPRK and Iran). These states have been shown to arrange circuitous financial transactions and/or shipments, passing through countries that have weak AML/CFT/CPF controls. Additionally, the UNSCR 1718 PoE had identified designated persons and entities routing their transactions through countries as far away as those in Africa and Europe to disguise the fund and shipment flows.

The TCI is an international financial centre and the major target of financial services is directed towards foreign customers; these characteristics contribute to higher PF risks. While there is currently no evidence to suggest that TCI regulated entities are involved in proliferation financing activities, the exposure of the TCI's financial system when conducting business in the international financial markets poses PF risks.

VULNERABILITIES TO PF

The TCI needs to guard against vulnerabilities which may be exploited by proliferators to enable financial flows or assist in the shipment of illicit goods, services and technology needed for the development of WMDs and their means of delivery. These vulnerabilities can exist because of insufficient familiarity with the list of dual-use goods for monitoring, and insufficient understanding, awareness, and expertise in identifying PF risks.

Sectoral Vulnerabilities

Banks and money or value transfer sectors

These sectors are vulnerable because they can be used by designated persons and entities to access the international financial system to process payments for components or materials from overseas sources.

Trust and company service providers, independent legal professionals, accountants

These sectors are used for creating legal persons and legal arrangements (or assisting in their creation and operation) that designated persons and entities may use to obscure the links between a financial

transaction and a designated person or entity. Legal persons and legal arrangements can have ownership and control exercised through nominees.

Dealers in precious metals and stones

These sectors can provide an alternative method for designated persons and entities to surreptitiously move financial resources across international borders.

The maritime sector

Given the challenges with securing borders, designated persons and entities can exploit the maritime sector to deliver components and materials for use in WMD or their delivery systems, to illicitly engage in economic activities in violation of the provisions of UNSCRs, the revenue from which can provide the underlying financing for a WMD programme.

PREVENTATIVE MEASURES

Proliferation and its financing can be mitigated by strong export controls, risk assessment of customers and products, application of customer due diligence measures, including enhanced due diligence on high-risk customers and transactions.

Risk Assessment

Given that criminals may exploit FIs and DNFBPs to finance proliferation, FIs and DNFBPs must adopt a risk-based approach to managing their PF risks, as required with ML and TF risks. To apply a risk-based approach, FIs and DNFBPs will need to understand PF risks based on the same risk factors for ML and TF which are listed below (note: PF risk should be incorporated into FIs and DNFBPs existing ML/TF business risk assessment):

i) the organisational structure of the FI/DNFBP, including the extent to which it outsources activities;

ii) the FI/DNFBP customers;

iii) the countries with which the FI/DNFBP customers are connected;

iv) the products and services that the FI/DNFBP provides or offers to provide;

v) the persons to whom and how the FI/DNFBP delivers its products and services;

vi) the nature, scale, and complexity of the activities of the FI/DNFBP;

vii) reliance on third parties for elements of the customer due diligence process; and

viii) new business practices and new or technological developments for new and existing products

A detailed guide explaining the steps to be taken to carry out a proper business risk assessment is set out in the Commission's Guidelines on Risk Assessment. The following features should be borne in mind:

Customer risk

- Designated persons[8] – FIs and DNFBPs are prohibited from offering financial services to UN-designated individuals and entities
- Individuals and entities owned or controlled by designated names
- Legitimate customers in industries that produce sensitive goods, dual-use goods, or companies or institutions involved in advanced research can pose PF risk to a FI/DNFBP

Product and service risk

- Trade finance transactions that involve controlled goods or technology present elevated PF risk
- Cross-border wires involve greater PF risk than traditional trade finance and are often more attractive to bad actors

Delivery channel risk

- Special attention should be paid to the channels that are not normally used by customers or are not aligned with the normal behavioural pattern of the customer.

Country risk

- Countries that are known or strongly suspected to be developing WMD present the highest jurisdiction risk for firms.
- Countries with transnational connections to procure illicit goods and services. The DPRK relies on extensive corporate networks hosted in China, Hong Kong, Singapore, and Malaysia;
- Countries with weak export control laws.

Additional tips for FIs and DNFBPs when assessing PF risk are as follows:

- Understand proliferation financing methods and trends;

[8] FIs and DNFBPs must screen the names of existing and prospective clients to determine if they are a designated person or entity. If during the process of screening or monitoring of customers or potential customers a positive or potential match is found, the DNFBP shall: Freeze such accounts and other funds or economic resources; Refrain from dealing with the funds or assets, or from making them available (directly or indirectly), to the entries unless licensed by the Governor; Report any findings to the Governor and the Financial Services Commission, with any additional information, that would facilitate compliance with the Regulation; Provide any information concerning the frozen assets of the entry that the Governor may request, noting that information reported to the Governor may be passed on to other regulatory authorities or law enforcement.

- Understand how the economy might be exposed to proliferation;
- Identify areas of high exposure to proliferation financing;
- Concentrate resources where they are most needed.

Internal policies and procedures

FIs and DNFBPs are required to have written internal procedures relating to the implementation of freezing measures. The procedures should be approved by the directors (or equivalent) of the FI/DNFBP, relevant to the size, structure, and activity of the FI/DNFBP, and disseminated to all the FI/DNFBP's employees concerned and updated regularly.

FIs and DNFBPs should put in place procedures that clearly explain how to implement asset freezing measures and should specifically and clearly set out:

- the legal framework for asset freezing measures, including the risk of criminal or disciplinary sanctions in the event of non-compliance with obligations;
- the screening system in place by the FI/DNFBP;
- the scope of screening and its frequency;
- the electronic lists used (OFSI Consolidated List, external service providers, UN lists, etc.)
- the information sources used by the FI/DNFBP for screening individuals and entities (including commercial databases used to identify adverse information on individuals and entities);
- the roles and responsibilities of the employees involved in the screening, reviewing, and discounting of alerts, maintaining and updating of the various screening databases, and escalating potential matches;
- the necessary authorisations to access and process the alerts;
- the process for analysing the alerts from screening and determining whether a potential match is a false positive or a confirmed match;
- the steps to be taken by the FI/DNFBP's employees for reporting confirmed matches to the FI/DNFBP's senior management;
- the measures to be taken by the FI/DNFBP to report any confirmed match to the Governor and the Commission;
- the steps to be taken to freeze or restrict access to funds by sanctioned persons.
- the management of the customer or the business relationship impacted by a freezing measure and the information to be provided to the customer whose funds/assets have been frozen;
- procedures to request/apply to lift the freezing measure;

- the implementation of the lifting of the freezing measure.

The procedures should include the timeframe to conduct or undertake the needed step or action. For more information on the implementation of freezing measures, please refer to the Commission's Targeted Financial Sanctions Guidance for FIs and DNFBPs.

Application of CDD Measures

The application of CDD measures is integral in the AML/CFT framework of FIs and DNFBPs. Knowledge of the customer helps to understand the general activities in which the customer would usually be expected to engage. As part of their due diligence process, FIs and DNFBPs must:

1. Obtain customer due diligence information on every customer, third party and beneficial owner comprising—

    (a) identification information in accordance with regulation 14 of the AML Code, which must include:
        (i) the full legal name of the customer, any former names and any other names used by the customer;
        (ii) the gender of the individual;
        (iii) the principal residential address of the individual;
        (iv) the date of birth of the individual

    (b) relationship information in accordance with regulation 12 which must include:
        (i) the purpose and intended nature of the business relationship;
        (ii) the type, volume and value of the expected activity;
        (iii) the source of funds and, where the customer risk assessment indicates that the customer, business relationship or occasional transaction presents a high risk, the source of wealth of the customer, third party or beneficial owner;
        (iv) details of any existing relationships with the company;
        (v) the reason for using a company based in the TCI where the customer is not resident in the TCI; and
        (vi) such other information concerning the relationship that, on a risk-sensitive basis, the company considers appropriate.

2. Consider, on a risk-sensitive basis, whether further identification or relationship information is required

3. Based on the information obtained through identification and relationship information (including where obtained through enhanced due diligence measures), prepare and record a risk assessment with respect to the customer. The customer risk assessment must particularly consider the relevance of the following risks—
    (a) customer risk;

(b) product risk;
(c) delivery risk; and
(d) country risk.

4. Verify the identity of the customer; and

5. Periodically update the customer due diligence information that it holds and adjust the risk assessment that it has made accordingly

The Commission's DNFBP Customer Due Diligence Guidance provides more information on the application of CDD measures including the enhanced due diligence measures that should be taken for high-risk customers.

Staff Training

It is the responsibility of FIs and DNFBPs to remain abreast and current regarding TFS risks, maintain and execute suitable mitigation measures, and to ensure that all employees are adequately informed and trained on the relevant policies, processes, and procedures.

ANNEX 1 – Proliferation Financing Red Flags

The following list is not uniquely determinative of proliferation financing, and proliferation financing activities may share similar traits with money laundering (especially trade-based money laundering) and terrorist financing activities.

Customer Specific Red-Flags

i) Customer is involved in the supply, sale, delivery or purchase of dual-use, proliferation sensitive or military goods, particularly to higher risk jurisdictions.

ii) Customer or counterparty, or its address, is the same or similar to that of an individual or entity found on publicly available sanctions lists.

iii) Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.

iv) Customer vague/incomplete on information it provides, resistant to providing additional information when queried.

v) The customer is a research body connected with a higher risk jurisdiction of proliferation concern.

vi) The customer's activities do not match with the business profile provided to the reporting entity.

vii) The customer is vague about the ultimate beneficiaries and provides incomplete information or is resistant when requested to provide additional information

viii) The customer uses complicated structures to conceal connection of goods imported /exported, for example, uses layered letters of credit, front companies, intermediaries and brokers.

ix) A freight forwarding / customs clearing firm being listed as the product's final destination in the trade documents.

x) Use of professional intermediaries and firms to mask parties to transactions and end users.

xi) The final destination of goods to be imported / exported is unclear from the trade related documents provided to the reporting entity.

Transaction Specific Red-Flags

i) Project financing and complex loans, where there is a presence of other objective factors such as an unidentified end-user.

ii) The transaction(s) involve an individual or entity in any country of proliferation concern.

iii) Transaction involves person or entity in foreign country of diversion concern.

iv) The transaction(s) related to dual-use, proliferation-sensitive or military goods, whether licensed or not.

v) Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.

vi) Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.

vii) Transaction involves possible shell companies (e.g. companies that do not have a high level of capitalisation or displays other shell company indicators).

viii) Transaction demonstrates links between representatives of companies exchanging goods i. e. same owners or management.

ix) Use of cash or precious metals (e.g. gold) in transactions for industrial items.

x) The transaction(s) involve the shipment of goods inconsistent with normal geographical trade patterns i.e. where the country involved does not normally export or import or usually consumed the types of goods concerned.

xi) Over / under invoice of dual-use, proliferation-sensitive or military goods, trade transactions.

xii) When goods destination/shipment country is different from the country, where proceeds are sent/ received without any plausible reason