هيئة تنظيم مركز قطر للمال
QATAR FINANCIAL CENTRE
REGULATORY AUTHORITY

Guidance for Financial Institutions and DNFBPs on Countering Proliferation Financing

1. Introduction

1.1 The following guidance should be read within the framework and provisions of:

(a) Law No. 20 of 2019 on Combatting Money Laundering and Terrorism Financing (AML/CFT);
(b) Law No. 27 of 2019 on Combating Terrorism;
(c) Council of Ministers' Decision No. (41) of 2019 Promulgating Law No. 20 of 2019;
(d) The Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019 and the Anti-Money Laundering and Combating the Financing of Terrorism (General Insurance) Rules 2019;
(e) Other guidance papers issued by the Regulatory Authority from time to time;
(f) FATF Guidance on Counter Proliferation Financing ("CPF"): The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, issued in February 2018;[1]
(g) FATF's publication "Combating Proliferation Financing: A status report on policy development and consultation", issued in February 2010;[2]
(h) FATF Proliferation Financing Report, issued in June 2008;[3]

Note that for the purposes of this paper:

- the term "firm" should be construed as meaning Financial Institutions and Designated Non-Financial Professions and Businesses ("DNFBPs"); and
- the term "account" should be construed as also meaning policy, mandate, matter, instruction, or engagement.

1.2 This guidance is commensurate with Financial Action Task Force ("FATF") Recommendation 7.

1.3 Recommendation 7 states that countries are required to implement targeted financial sanctions imposed under United Nations Security Council Resolutions related to the proliferation of Weapons of Mass Destruction ("WMDs") and the financing of proliferation. Implementation of these resolutions requires countries to freeze without delay:

[1] See https://www.fatf-gafi.org/publications/financingofproliferation/documents/guidance-counter-proliferation-financing.html.
[2] See https://www.fatf-gafi.org/publications/financingofproliferation/documents/combattingproliferationfinancingastatusreportonpolicydevelopmentandconsultation.html.
[3] See https://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf

(a) All funds or other assets that are owned or controlled by the designated person or entity, not just those that can be tied to a particular act, plot or threat of proliferation;

(b) All funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities;

(c) Funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities; and

(d) Funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

1.4 Recommendation 7 further emphasises the need for firms to implement preventive measures to counter the flow of funds or assets to proliferators or those who are responsible for weapons' proliferation.

2. Purpose

2.1 This guidance is issued to firms so that they may guard against the threats of proliferation financing ("PF"). It is being issued to raise awareness of proliferation financing threats, vulnerabilities, and risks, and to highlight the relevant requirements for firms.

2.2 Any firm that plays a role in PF, either knowingly or unknowingly, would cause immense damage to itself, and to the security and integrity of Qatar and the Qatari financial system. The identification, assessment, understanding, and management of PF risks by firms is essential to a robust AML/CFT regime. It is critical that every firm includes CPF in its AML/CFT programme and risk management strategies.

2.3 This guidance provides common definitions surrounding PF and describes the regulatory framework in Qatar, coupled with international standards and obligations.

2.4 This guidance also focuses on indicators of possible PF risks, and the relevant risk management practices and tools firms should implement and incorporate in their AML/CFT programmes to counter the risks and vulnerabilities associated with PF.

3. Definitions

Proliferation

3.1 FATF's 2008 Typologies and Proliferation Financing Report's definition of "Proliferation" is: "Proliferation has many guises but ultimately involves the transfer and export of technology, goods, software, services or expertise that

could be used in nuclear, chemical or biological weapon-related programmes, including delivery systems; it poses a significant threat to global security."

Proliferation financing

3.2 The 2010 FATF Status Report on Combating Proliferation Financing defines PF 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-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations".

Proliferator

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

4. General framework for managing CPF

4.1 Firms must include CPF in their AML/CFT programme and risk management strategies, including in their Business Risk Assessment ("BRA");

4.2 Firms must effectively mitigate PF risk through application of their general AML/CFT programme and measures, including through monitoring for and reporting suspicious transactions;

4.3 Firms must conduct enhanced due diligence ("EDD") when dealing with:

(a) countries that are subject to UN or other high-risk countries identified by FATF;

(b) entities established in, or having a significant presence in, those countries; or

(c) transactions associated with those countries;

4.4 Firms that choose to do business in or involving countries that are high-risk for PF (as identified in the National Risk Assessment ("NRA") of ML, TF and PF, by supervisors, or by the firm's own risk assessment), or accept customers with substantial ties to such countries, must:

(a) perform EDD on any transaction involving any such country;

(b) perform EDD on all customers with substantial ties to such countries and any transactions conducted by such countries.

EDD must be designed to ensure that the firm understands and manages the PF risk of the relationship. Firms should recognise that such measures are unlikely to manage the risks of business relationships with individuals or entities with high exposure to proliferation risks. EDD measures must be designed to ensure that the firm understands and manages the PF risk of the relationship; and

4.5 Firms must be sensitive to the risks of transactions involving nuclear, dual-use, or military goods. Firms must perform EDD on:

(a) all customers with substantial ties to these goods or sectors; and

(b) all transactions involving these goods or sectors.

5. PF threats and risks

5.1 PF threats are primarily external and relate to foreign state and non-state actors attempting to exploit banks, companies, or transportation infrastructure to clandestinely finance, procure, ship, or trans-ship goods for use in the proliferation of WMD. Traditionally, 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 threats are:

(a) **State actors - listed countries** 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. Other states with existing or developing WMD capabilities pose a more limited threat.

(b) **Non-state actors - terrorist groups** that have targeted countries for fundraising have at least stated an intent to pursue nuclear weapons and radiological materials.

5.2 Firms should be aware, however, that the absence of direct links to these countries or non-state actors does not mean that a transaction or customer is necessarily low risk. Proliferators have shown a high level of ability to hide their involvement and the nature of the activity underlying a transaction or business relationship. Every firm faces a certain amount of risk and must remain vigilant in protecting against proliferation and PF.

6. Vulnerabilities to PF

6.1 Examples of factors specific to PF that raise the level of risk are:

(a) Licit commercial and financial links with high-risk jurisdictions;

(b) Weaknesses in shipping and transhipment controls, including transparency, monitoring capabilities or any other discrepancies in the trade finance requirements;

(c) Insufficient familiarity with the list of dual-use goods for monitoring; and

(d) Insufficient understanding, awareness, and expertise of PF risks.

Sanctions Evasion and Proliferators' Efforts to Hide their Activities

6.2 Proliferators in high-risk jurisdictions know that sanctions filters and due diligence procedures used by firms will detect and freeze transactions involving their true names. Instead, these actors employ a variety of tactics to evade detection and gain access to the international financial system. Examples of such tactics include:

(a) **Disguising themselves as residents of another jurisdiction.** Proliferators will structure transactions or corporate actions in order to appear to be a legitimate business based in a lower-risk jurisdiction, often one neighbouring the sanctioned country. Shell and front companies and firms in some countries have been implicated in recent sanctions evasions schemes directed from the UN listed countries; and

(b) **Use of opaque shell and front companies and complex corporate forms.** Proliferators use shell and front companies, particularly those established in jurisdictions with weak company formation regimes, to disguise their identities. These bad actors may use multiple complex layers of companies to further disguise ownership.

Proliferators may use both strategies at the same time to increase their chances of success.

7. Incorporating PF risk in the firm's risk assessment

7.1 Firms must adopt a risk-based approach to managing their PF risks, as with ML and TF risks. The first step in adopting a risk-based approach is understanding PF risk, including by conducting an assessment of the overall PF risk in the firm's operations. This assessment should be conducted as part of the firm's enterprise-wide BRA.

7.2 The BRA must consider the following PF risks that a firm can be exposed to, directly or indirectly:

(a) **Customers** - the nature of customers;

(b) **Products and services** - the nature of the products and services offered to customers;

(c) **Delivery channels** - the means employed to deliver products and services to customers; and

(d) **Jurisdictions** - the countries or geographic regions in which the firm does business or where the customer is located or operates.

7.3 Each of these risks is addressed below.

Customer risk

7.4 There are several sources of PF risk from customers:

(a) Designated names - Firms are prohibited from offering financial services to UN-designated individuals and entities;

(b) Individuals and entities owned or controlled by designated names:

i. Even if firms are legally allowed to accept as a customer a company that is partly owned by a sanctioned person, they must be aware that such a company may also be involved in proliferation activity and poses elevated risks;

ii. In the case of higher-risk companies, firms should consider lowering the 20% ownership and control threshold to verify the identity of additional beneficial owners;

iii. Firms should make a risk-based decision about whether they are willing to accept customers in which a designated person has a non-controlling ownership interest; and

iv. Sanctioned individuals may also seek to obscure their interest through family members or close business associates.

(c) 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 firm:

i. Shipping companies, particularly those serving high-risk regions, may also present risks;

ii. Customers who produce dual-use goods may not be familiar with the rules and regulations governing exports. Customers that are unaware of the need to implement their own PF safeguards present higher risk to firms; and

iii. Proliferation networks often rely on shell and front companies to disguise end-users and payments. These companies are high-risk for a number of reasons, including their potential roles in PF typologies.

Product and service risk

7.5 Trade finance transactions that involve controlled goods or technology present elevated PF risk:

(a) The complexity of these transactions can allow individuals and entities to hide their intentions or underlying illicit activities; and

(b) Both traditional document-based trade finance transactions and cross-border wires related to trade present high PF risk to firms.

7.6 Cross-border wires involve greater PF risk than traditional trade finance and are often more attractive to bad actors:

(a) Wires transfers often include less information on the underlying activity, making it more difficult for firms to fully understand the transaction;

(b) Firms might find it difficult to obtain information on and understand the activity underlying cross-border wire transfers;

(c) Wire transfers also provide a less complicated means for conducting trade transactions because they can be processed more easily than traditional trade finance instruments such as letters of credit, which usually involves extensive documentation and diligence.

7.7 Correspondent banking services are another important source of PF concern:

(a) Activities such as clearing intermediary wires expose the firm to additional risk because the institution must process or execute transactions for the customers of the firm's customer; and

(b) The risk is elevated when the correspondent relationship exposes a firm to a region with links to proliferation activity.

Delivery channel risk

7.8 Firms should assess the risks associated with the delivery channels and apply special attention and EDD to the identified high-risk areas as per their risk-based approach;

7.9 Firms should consider the channels used to take on new clients, as well as how those clients are accessing the products and services.

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

Jurisdiction risk

7.11 Countries that are known or strongly suspected to be developing WMD present the highest jurisdiction risk for firms. The NRA identifies the DPRK and Iran as the

main sources of PF threat for Qatar. These countries are top priorities in global counter-proliferation efforts because of their longstanding WMD programmes.

7.12 Proliferation risk, however, is not solely tied to countries at high-risk for proliferation or PF. Countries and terrorist groups rely on transnational connections to procure illicit goods and services. For instance, the DPRK relies on extensive corporate networks hosted in China, Hong Kong, Singapore, and Malaysia; within China, related companies are especially active in Liaoning and Jilin provinces. Proliferators may aim procurement efforts at countries with weak export control laws, and they may choose to have sensitive or dual-use items delivered initially to transhipment hubs rather than directly to their home countries.

8. Implementation of preventive measures and supervisory obligations

8.1 Firms must ensure that their comprehensive AML/CFT programme – as well as their group-wide AML/CFT programme – is designed to manage PF risks identified in the institutional risk assessment effectively. AML/CFT policies and procedures must cover PF and reflect counter-PF guidance and warnings issued by the QFCRA and the FATF.

8.2 Firms are required to:

(a) Offer relevant staff training on all AML/CFT risks as well as PF risks and red flags (Appendix B);

(b) Design and implement transaction monitoring systems to identify transactions that may be linked to PF; and

(c) Include potential PF-related activity in their transaction reporting and monitoring system.

Enhanced Due Diligence

8.3 Firms must conduct EDD on all customers and transactions that are assessed to be high risk for PF. EDD is a crucial preventive measure, that, when properly conducted, can help firms manage their PF risk.

8.4 EDD should focus on obtaining information regarding expected customer behaviour, with special attention to the expected end-users of any sensitive products and the customer's expected exposure to high-risk jurisdictions, including transhipment hubs. Customers in this group should also be monitored carefully, since unusual behaviour, even if not clearly suspicious, is more concerning in the case of customers that may potentially be exploited by proliferators.

8.5 Firms should also apply EDD to transactions found to involve any proliferation-sensitive goods or services, regardless of whether the firm's customer is itself in

a high-risk category. As with onboarding, special attention should be paid to identifying the end-users of any sensitive goods.

8.6 Examples of EDD measures include, but are not limited to:

(a) Identifying beneficial owners below the 20 per cent threshold;

(b) Requiring the customer to sign a warrant or other agreement that it complies with all UN and Qatari sanctions;

(c) Requiring customers to submit a list of important suppliers and customers, and conducting basic due diligence and public records searches on these entities;

(d) Reviewing the customer's customer acceptance policy, sanctions policy, and any policies related to export controls, and requiring the customer to make changes if these policies are not sufficient;

(e) Subjecting the account to special transaction monitoring rules designed to raise alerts about new counterparties or other changes; and

(f) Reviewing the customer's transactions on the account on a more frequent basis to identify irregular transactions, changes in the customer's behaviour, or new counterparties.

8.7 In addition, firms should consider applying enhanced measures for individual transactions, such as asking the customer to provide a valid export license or a reference to the export control requirements in the relevant jurisdiction showing that the exported goods do not require a permit.

Customer Screening

8.8 Firms are required to screen the entire customer file for all customers, including beneficial owners, authorised signatories, and addresses, whenever a new designation is announced. For customers being onboarded, all such customers should be screened before onboarding. If no customer relationship is formed (*e.g.*, the customer is a walk-in or wants to engage in a one-time transaction), customers must be screened before making a transaction.

8.9 It is not sufficient for a firm to simply screen its customer lists against the names of sanctioned individuals or entities. To ensure that they are complying with the requirement to freeze all funds that the designated person controls, even indirectly, firms must conduct appropriate due diligence to satisfy themselves that they know who their customers are and, if their customers are controlled by a third party, who that individual or entity is.

Example: *Company A is a customer of a QFC firm. To identify whether Company A's accounts must be frozen, the firm must screen not just the name of Company A, but the names of its beneficial owner(s), anyone identified as having operational control of the company including persons holding a Power of Attorney, all signatories on the*

account, and all addresses provided by Company A during the CDD process (or available through a public records search).

8.10 In addition, firms must maintain real-time sanctions screening systems in place for all incoming and outgoing payments. These systems must be capable of identifying a match against any internal and vendor-supplied lists maintained by the firm, and if there is a match, holding the transaction until an appropriate employee of the firm reviews it.

8.11 Screening lists used in transaction monitoring must be updated immediately upon notice of designation. Where the firm uses a screening list provided by a third-party vendor, the vendor's Service Level Agreement with the firm must ensure that the screening list is updated within 24 hours of a new or updated designation being issued. Transaction screening and monitoring systems should be capable of screening and monitoring all aspects of customer onboarding as well as payment messages, including all additional information provided by the ordering institution or the customer. **Firms are strongly urged to include relevant terms, such as common types of dual-use goods, jurisdictions subject to sanctions, and major cities and ports within those jurisdictions, on their sanctions screening lists**.

Freezing accounts

8.12 Implementing targeted financial sanctions requires firms to place a restriction on any account meeting the following criteria.

(a) The account represents funds or other assets that are owned or controlled by the designated person or entity, beyond those that can be tied to a particular act, plot or threat of proliferation.

(b) The account represents funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities.

(c) The account represents funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities.

(d) The account represents funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

Holding/stopping transactions

8.13 Firms must screen all outgoing and incoming transfers in real-time and monitor transactions to detect any transactions that must be stopped or take any further actions. If a customer of a firm seeks to make a transfer or carry out a transaction to an individual or entity subject to UN or Qatari sanctions, the firm should immediately if the match is identified:

(a) hold the funds that would have been subject to the transfer and/or transaction;

(b) file an STR; and

(c) inform its supervisor.

8.14 The funds should not be returned to the customer and should remain with the firm until the competent authorities have carried out a full investigation into the purpose of the payment and the nature of the customer's relationship with the designated person. Firms should comply with the directions of the competent authorities regarding ultimate disposition of the funds. Firms should in no case provide the customer with any information indicating that an STR has been filed.

8.15 In addition, the Public Prosecutor can permit certain transactions when the transactions meet requirements imposed in UN Security Council Resolutions and Qatari law. In these cases, the Public Prosecutor and the relevant supervisor will give any relevant firms instructions as to their responsibilities in permitting such transactions.

Reporting

8.16 Firms are required to immediately and within at most 24 hours implement the designation order, and report any actions taken in compliance with the designation to their supervisor within 48 hours of issuance of the designation order. This includes:

(a) any accounts frozen;

(b) any transactions stopped, held or blocked;

(c) all screening performed; and

(d) any other efforts to comply with sanctions.

8.17 Firms must report again to their supervisor 30 days after issuance of the designation order whether or not they have taken any additional actions.

8.18 Once the above reports have been made, firms are required to report if they freeze any additional accounts or funds or block any transactions. Account and /or customer relationship should be subject to enhanced monitoring as well

False positives

8.19 List-based screening may result in hits where a person related to an account or transaction has the same name or the same address as a designated person. Firms are required to take a conservative approach to sanctions hits; that is,

they cannot assume that a hit is a false positive and must thoroughly investigate every hit.

8.20 Generally, in such an investigation, firms should compare information that is known about the party in question, such as date of birth and address, with other information provided in the designation order. If the party in question is not a customer, the firm may need request that its customer provide reliable proof of its counterpart's identity, such as a copy of a government-issued photo identification document. If the firm identifies information that establishes that the party in question is not a designated person, then the firm does not need to block a transaction or hold an account. Detailed records should be kept of the process followed, the evidence obtained, and the rationale for releasing a transaction.

8.21 **To avoid duplicative investigations, firms may create a "false hit list / white list" and records of customers that have the same name as designated persons and whom the firm has determined, after a thorough investigation, not to be the person that has been designated**. Firms can use this list to instruct their automated monitoring software not to alert on such matches. While this practice is acceptable, it does carry risk, and therefore firms should regularly review and update the list to ensure that bona fide matches are not suppressed. Firms would be well-advised also to subject the list to independent or external audit periodically.

8.22 Firms may also be approached by persons who claim that their funds or accounts have been mistakenly frozen because they share the same name as a designated person. These claims must be carefully investigated, using the same process as used for hits from automated monitoring systems. If there is any doubt as to the identity of the claimant, the firm should refuse to unfreeze the funds or accounts and should allow the claimant to pursue the remedies provided in the Counterterrorism Law (27) of 2019 and the Public Prosecutor Order.

Unfreezing

8.23 Unfreezing will generally take place when a formerly designated person is no longer designated.

8.24 Although rare, designations may be rescinded. For example, a designated person may cease to be involved in proliferation activities and therefore be removed from UN and Qatari sanctions list. A designated individual can also be removed from the sanctions lists after that individual's death upon request from NCTC or from the heirs.

8.25 Firms may also receive court orders, or orders from the Public Prosecutor, to unfreeze funds and accounts for certain purposes, including, for example, to

reflect the rights of third parties. Firms should seek guidance from the Public Prosecutor and their supervisors if they have any questions about compliance with such orders.

8.26 Firms must continue to monitor updates to the Qatari sanctions list so that they are aware that a person has been de-listed. Unfreezing should take place promptly but with appropriate due diligence and deliberate caution, consistent with the terms of de-listing and any guidance from authorities. Firms must continue to be vigilant to ensure that accounts or funds are not transferred to other designated persons. Firms that have questions about unfreezing the assets of a person that has been de-listed should seek guidance from the PPO.

Penalties

8.27 The Counterterrorism Law sets strict penalties for failure to comply with the legal requirements, including the freezing of funds, that results from Qatari or UN designations. Any person contravening a designation order can be sentenced to imprisonment for a period of up to three years and to a fine of up to ten million Qatari Riyals, or one of these two penalties. There is no requirement that a person knew that they were contravening the designation order, or that the person intended to contravene the order. Since freezing of accounts or transactions is a consequence of a designation order, failure to comply with these requirements can lead to extremely high fines and even a prison term. Each violation could be penalised separately.

8.28 In addition, Law No. (20) of 2019 gives supervisors the power to levy strong penalties on firms that fail to comply with relevant requirements. These include fines of up to 100 million Qatari Riyals, or of up to 100 thousand Qatari Riyals per day that a firm is in violation. Managers of a non-compliant firm can be banned from employment in the Qatari financial sector.

Red flag indicators and typologies of potential PF risks

8.29 Customer:

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

(b) The customer or counterparty, or its address, is the same or similar to that of an individual or entity found on publicly available sanctions lists.

(c) The customer is a military or research body connected with a higher risk jurisdiction of proliferation concern.

(d) The customer's activities do not match the business profile.

(e) The customer is vague about the end-user(s) and provides incomplete information or is resistant when requested to provide additional information.

(f) A new customer requests a letter of credit from a firm, while still awaiting approval of its account.

(g) The customer uses complicated structures to conceal involvement, for example, uses layered letters of credit, front companies, intermediaries and brokers.

8.30 Transactions/Orders:

(a) The transaction(s) concern(s) dual-use, proliferation-sensitive or military goods, whether licensed or not.

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

(c) The transaction reflect(s) a link between representatives of companies (e.g. same owners or management) exchanging goods, to evade scrutiny of the goods exchanged.

(d) The transaction(s) involve(s) the shipment of goods inconsistent with normal geographic trade patterns, i.e. where the country involved does not normally export or import the types of goods concerned, or the vessel is listed in the UN sanctions lists.

(e) Companies or individuals from countries, other than the country of the stated end-user, place the order for goods.

8.31 Jurisdiction:

(a) Countries with weak financial safeguards and which are actively engaged with a sanctioned country.

(b) The presence of an industry that produces dual-use goods, proliferation-sensitive items or military goods.

(c) Deliberate insertion of extra links into the supply chain.

(d) Countries that are known to have weak import/export control laws or poor enforcement.

(e) Countries that do not have the required level of technical competence concerning certain goods involved.

8.32 Other:

(a) The final destination or end-user is unclear.

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

(c) Declared value of shipment under-valued in relation to shipping cost.

(d) Inconsistencies in information contained in trade documents and financial flow e.g. names, addresses, final destination.

(e) The use of fraudulent documents and identities e.g. false end-use certificates and forged export certificates.

(f) The use of facilitators to ensure the transfer of goods avoids inspection.

(g) A freight forwarding company being listed as the product's final destination.

(h) Wire instructions or payment from or due to entities not identified on the original letter of credit or other documentation.

(i) Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

APPENDICES

A. UN North Korea/DPRK Sanctions Regime

UN sanctions include a list-based component (which lists vessels as well as individuals and other entities) targeting those involved in the proliferation of WMD or the development of ballistic missiles. The multilateral sanctions effort also includes a number of import and export prohibitions or limits, as described below.

The UN Security Council's 1718 Sanctions Committee was established pursuant to UN Security Council Resolution 1718 (2006) to oversee North Korea/DPRK sanctions measures. Additional functions were entrusted to the Committee in resolutions 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2371 (2017), 2375 (2017), and 2397 (2017).

While narrow exemptions do exist, most related to humanitarian ends and most requiring 1718 Sanctions Committee approval, the following prohibitions (laid out by the 1718 Sanctions Committee) apply, among others. Firms should be aware that facilitating a transaction relating to these prohibited activities could itself be a sanctions violation.

Measure	Description
Arms and related materiel embargo	All Member States are required to prevent the direct or indirect supply, sale, or transfer to the DPRK, through their territories or by their nationals, or using their flag vessels or aircraft, and whether or not originating in their territories, of all arms and related materiel, including small arms and light weapons and their related materiel, a ban on related financial transactions, technical training including hosting of trainers, advisors, or other officials for the purpose of military-, paramilitary-, or police-related training, services or assistance related to manufacture, maintenance or use, and with respect to the shipment of items to or from the DPRK for repair, servicing, refurbishing, testing, reverse-engineering and marketing.
Proliferation networks	All Member States are required to close the representative offices of designated persons and entities, as well as on any persons or entities acting on behalf of such designated persons or

	entities, as well as prohibit them from participating in joint ventures and any other business arrangements.
	All Member States are required to limit the number of bank accounts (in their territory) to one per DPRK diplomatic mission and consular post, and one per accredited DPRK diplomat and consular officer. All Member States are required to prohibit the DPRK from using real property (owned or leased) in their territory for non-diplomatic or consular activities' purposes.
Interdiction and transportation	All Member States are required to prohibit the provision of insurance or re-insurance services to vessels they have reasonable grounds to believe were involved in activities or the transport of items prohibited by the relevant resolutions.
	The Committee, if it has information that provides reasonable grounds to believe that the vessel(s) are or have been related to prohibited programmes or activities, and pursuant to the vessels' designation, will require any or all of the following actions: de-flagging of the vessel(s) by the Flag State; directing the vessel(s) to a port identified by the Committee (in coordination with the port State) by the Flag State; the prohibition of the vessel(s) entering into ports by Member States; and for the vessel(s) to be subject to assets freeze.
	All Member States should improve mutual information-sharing on suspected attempts by the DPRK to supply, sell, transfer or procure illicit cargo, with support and facilitation by the 1718 Committee and the Panel of Experts. All Member States are required to notify the Committee of relevant identifying information as well as measures taken to carry out appropriate actions as authorised by the relevant provisions regarding vessels in their territory or on the high

	seas designated as subject to the assets freeze, the port entry ban or other relevant measures.
Assets freeze	All Member States are required to freeze the assets, funds, and economic resources of the entities of the Government of the DPRK and Korean Workers' Party, that the State determines are associated with the prohibited activities, including designated persons and entities, as well as any persons or entities acting on behalf of or at their direction, or those owned or controlled by them. These assets include tangible, intangible, movable, immovable, actual or potential, which may be used to obtain funds, goods or services, such as vessels, including maritime vessels. Designated vessels are subject to assets freeze by Member States.
Disposal of seized items	All Member States are required to seize and dispose (such as through destruction, rendering inoperable or unusable, storage or transferring to a State other than originating or destination States for disposal) of prohibited items by the relevant resolutions in a manner consistent with their international obligations.
Financial measures	All Member States are required to prevent the provision of financial services, including bulk cash and gold, the opening of banking subsidiaries, the provision of public financial support, new commitments for grants, and financial assistance or concessional loans that could contribute to the DPRK's prohibited programmes/activities, or to the evasion of sanctions. Companies performing financial services commensurate with those provided by banks are considered financial institutions for the purposes of implementing relevant provision of the resolutions.
	All Member States are prohibited from opening any new branches, subsidiaries and representative offices of DPRK banks; must close existing branches, subsidiaries and representative

	offices; and terminate any joint ventures, ownership interests or correspondent banking relationships with DPRK banks in their territory.
	All Member States are prohibited from opening any new representative offices, subsidiaries or bank accounts in the DPRK. All Member States must close existing offices, subsidiaries and banking accounts in the DPRK within 90 days.
	All Member States are required to prohibit public and private financial support from within their territories or by persons/entities within their jurisdiction for trade with the DPRK, including granting of export credits, guarantees or insurance to their nationals, or entities involved in such trade.
	If a Member State determines that an individual is working on behalf of or at the direction of a DPRK bank/financial institution, then the individual is to be expelled by the Member State from their territory for the purpose of repatriation.
	All Member States are required to prohibit, by their nationals or in their territories, the opening, maintenance and operation of all joint ventures or cooperative entities, new or existing, with DPRK entities or individuals, whether or not acting for or on behalf of the government of the DPRK. All Member States are required to close any such existing joint venture or cooperative entity within 120 days of 11 September 2017 unless approved by the Committee on a case-by-case basis, and to close any such existing joint venture or cooperative entity within 120 days after the Committee has denied a request for approval.
Ban on export of textiles from the DPRK	The DPRK shall not supply, sell or transfer, textiles (including but not limited to fabrics and partially or completed apparel products). All Member States are required to prohibit the procurement of such items from the DPRK by their nationals, or

	using their flag vessels or aircraft, whether or not originating in the territory of the DPRK.
Ban on DPRK workers abroad	All Member States are prohibited from providing work authorisations for DPRK nationals in their jurisdiction in connection with admission to their territories. All Member States are required to repatriate to the DPRK all DPRK nationals earning income in their jurisdiction and all DPRK government safety oversight attachés within 24 months from 22 December 2017. Member States are required to submit a midterm report after 15 months from 22 December 2017 and a final report after 27 months from 22 December 2017 to the Committee of all DPRK nationals that were repatriated based on this provision.
Fuel ban	All Member States are prohibited from selling or supplying of aviation fuel, jet fuel and rocket fuel to the DPRK. All Member States should exercise vigilance to ensure that fuel provided to DPRK-flagged civil passenger aircraft is no more than necessary (for the relevant flight) and includes a standard margin for safety of flight.
Other bans: statues, new helicopters, and vessels	The DPRK is prohibited from supplying, selling, transferring, of statues. All Member States are prohibited from procuring statues from the DPRK by their nationals, or by using their flag vessels or aircraft, whether or not originating in the territory of the DPRK. All Member States are required to prevent the supply, sale or transfer to the DPRK, of new helicopters, and new and used vessels.
Luxury goods ban	All Member States are required to prevent the direct or indirect supply, sale or transfer to the DPRK, through their territories or by their nationals, or using their flag vessels or aircraft, and whether or not originating in their territories, of luxury goods (including those items listed in Annex IV of resolution 2094 (2013), Annex IV of resolution 2270 (2016) and Annex IV of resolution 2321 (2016).

B. UN Iran Sanctions Regime

Through the passage of UNSCR 2231 in July 2015 and implemented in January 2016, the Joint Comprehensive Plan of Agreement (JCPOA) provided relief to Iran from most sanctions imposed by United Nations Security Council Resolutions (UNSCRs) and by extension Member States' sanctions implementing those UNSCRs. At the same time, UNSCR 2231 established a mechanism for re-imposition of sanctions if Iran re-engages in nuclear weapons proliferation.

UNSCR 2231 served four basic purposes:

- Formally endorsed the JCPOA negotiated by the United States, China, Russia, Germany, France, the United Kingdom, and Iran;
- Lifted most UN sanctions on Iran upon verification by the IAEA that Iran implemented the JCPOA (which occurred in January 2016);
- Instituted a monitoring and dispute resolution programme providing for re-imposition of UN sanctions under the JCPOA's "snapback" framework; and
- Provided an approval process for trade activities related to designated nuclear materials, goods, equipment, and technology, as well as other goods and services identified by a Member State as potentially contributing to enrichment, reprocessing, or heavy-water reactor activity.

UN sanctions lifted pursuant to UNSCR 2231 have not been re-imposed. Pursuant to UNSCR 2231, restrictions on arms and ballistic missile technology remain in place for eight years.

C. Dual Use Goods

Export controls are intended to prevent sensitive goods and dual-use goods (both listed and unlisted) from being exported to known individuals and entities that are involved in WMD proliferation. However, it is challenging to designate and monitor trade in all relevant dual-use goods, defined as goods that have commercial applications as well as applications for WMD and WMD delivery systems. In addition to national export controls, there are several relevant international export control regimes.

- **Nuclear Suppliers Group.** Focuses on nuclear materials and technology needed for nuclear programmes, as well as on technology that is considered dual-use and may be used in nuclear programmes.
- **Missile Technology Control Regime.** Focuses on technology needed for developing WMD delivery systems.

- **Wassenaar Arrangement.** Limited to conventional arms trade controls, as well as specific dual-use goods that may be applicable to illicit proliferation programmes.
- **The Australia Group.** Focuses on materials and technology needed for chemical and biological weapons development.
- **Zangger Committee.** Includes a list of technology needed for the production of fissile nuclear material.

The EU maintains a list of dual-use and controlled items, incorporating the above export control regimes.

The examples of general dual-use items in the table below are drawn from a report by the Swedish Security Service.

Nuclear	Chemical	Biological	Missile and delivery
Centrifuges	Scrubbers	Bacterial strains	Accelerometers
High-speed cameras	Mixing vessels	Fermenters	Aluminium alloys
Composites	Centrifuges	Filters	Aluminium powders
Maraging steel	Elevators	Mills	Gyroscopes
Mass spectrometers	Condensers	Presses	Isostatic presses
Pulse generators	Connectors	Pumps	Composites
X-ray flash apparatus	Coolers	Spray dryers	Maraging steel
Pressure gauges	Precursors	Tanks	Homing devices
Ignition	Pumps	Growth media	Oxidants
Vacuum pumps	Reactors		Machine tools
	Heat exchangers		

Table 1: Selected examples of general dual-use items.

REFERENCES

Financial Action Task Force
International Standards on Combating ML and the Financing of Terrorism & Proliferation (The FATF Recommendations)
Updated June 2019
https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

Financial Action Task Force
FATF Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT Systems (The FATF Methodology)
Updated October 2019
https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

Sound Practices to Counter Proliferation Financing
August 2018
https://www.mas.gov.sg/regulation/guidance/sound-practices-to-counter-proliferation-financing

United Nations
https://www.un.org/sc/suborg/en/

United Nations Sanctions
https://www.un.org/sc/suborg/en/sanctions/information

FATF Guidance on Counter Proliferation Financing
February 2018
http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf

FATF Combating Proliferation Financing: A status report on policy development and consultation
February 2010
http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf

FATF Proliferation Financing Report
June 2008
http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf