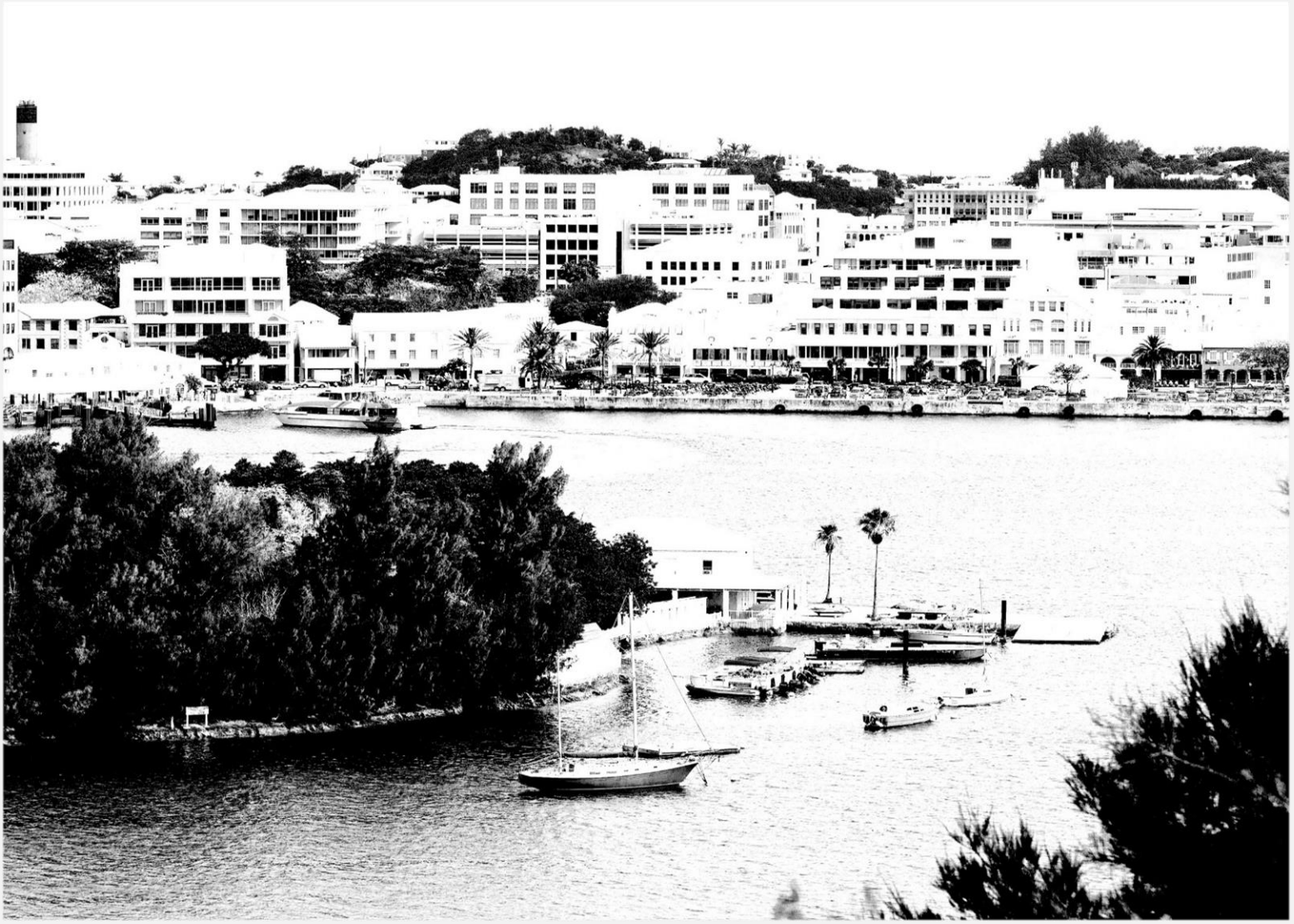
BERMUDA

Financial Sanctions Implementation Unit

Bermuda CPF Guidance

General guidance on countering the financing of proliferation of weapons of mass destruction



May 2025

This general guidance on countering the financing of proliferation of weapons of mass destruction is produced by the Financial Sanctions Implementation Unit (FSIU), a unit of the Ministry of Justice Headquarters, which, pursuant to the Governor's delegation, is responsible for carrying out certain functions with respect to the implementation of financial sanctions for terrorism, terrorist financing and proliferation financing in Bermuda.

The general guidance provides important information outlining obligations under Bermuda's sanctions regime as it relates to proliferation financing, including key indicators that should raise red flags when complying with proliferation sanctions.

As sanctions measures are subject to change you should also refer to the relevant, up-to-date legislation as well as sector specific guidance where it is applicable.

This guidance does not constitute legal advice and the FSIU cannot provide legal advice in relation to the application of international sanctions measures to specific cases. As appropriate you should obtain independent legal advice to assist in understanding your obligations to ensure your compliance with Bermuda's sanctions regime.

Financial Sanctions Implementation Unit
Ministry of Justice
Global House, Fourth Floor
43 Church Street Hamilton HM 12
Bermuda

General enquiries: (441) 292-2463
Email: fsiu@gov.bm

Acknowledgements:

Jersey Financial Services Commission – Guidance: Countering proliferation of weapons of mass destruction and its financing, April 2022

Contents

1 Scope

1. This guidance has been produced by the Financial Sanctions Implementation Unit (FSIU) in collaboration with the National Anti-Money Laundering Committee (NAMLC) Sanctions Working Group, which represents the operational partners responsible for Financial Sanctions. The focus of this guidance is to provide industry with relevant information to ensure they are employing adequate processes to counter or mitigate the risk of activities that may finance the proliferation of weapons of mass destruction (WMD).

2. This guidance does not constitute legal advice. It should be read in conjunction with the '*Bermuda Financial Sanctions: General Guidance for Financial Sanctions'* which can be found on the International Sanctions Measures page of the government portal: https://www.gov.bm/international-sanctions-measures.

2 Introduction

The importance of combatting proliferation of weapons of mass destruction

3. As an international financial centre (IFC), Bermuda has a rigorous AML/ATF/CPF regime that is consistent with the relevant international standards. The Government is committed to maintaining and updating this regime and exercises a zero-tolerance approach to money laundering (ML), terrorist financing (TF), and proliferation financing (PF) activities within the jurisdiction.

4. Whilst there has been no evidence to indicate Bermuda entities are involved in proliferation or PF activities, there may be potential exposure for exploitation of IFCs as proliferation networks work tirelessly to exploit weaknesses in global financial systems and export controls. Bermuda continues to review its systems and controls to combat illicit activity regarding PF and to assist financial services providers to identify potential vulnerabilities and indicators that should be taken into account when putting adequate processes and systems in place to mitigate, detect, prevent, and report PF.

5. Bermuda has a robust sanctions framework to combat PF (See Annex E). This includes restrictions on access to the global financial systems for persons designated or sanctioned for PF.

6. The Financial Action Task Force (FATF) is the global watchdog that sets international standards to tackle money laundering, terrorist and proliferation financing. These standards require countries to implement United Nations Security Council Resolutions (UNSCRs) for the prevention, suppression and disruption of proliferation of weapons of mass destruction (WMD) (Proliferation) and PF. UNSCRs also require countries to:

    i. freeze the funds or other assets of designated persons/entities (DP) without delay; and
    ii. to ensure that funds and other assets are not made available, directly or indirectly, to or for the benefit of a DP.

    Such designations are made under the authority of the United Nations Security Council (UNSC) (Chapter VII of the Charter of the United Nations).

7. In October 2020 the Financial Action Task Force (FATF) adopted amendments to FATF Recommendations 1 and 2 and their Interpretive Notes requiring countries and the private sector to identify and assess the risks of potential breaches, non-implementation or evasion of the targeted financial sanctions related to proliferation financing, as contained in FATF Recommendation 7, and to take action to mitigate these risks, as well as to enhance domestic co-ordination.[1]

8. Bermuda, as a member jurisdiction of the Caribbean Financial Action Task Force (CFATF), a FATF–Style regional body (FSRB) which is an associate member of the FATF, is required to give effect to and implement UNSCRs regarding PF and the proliferation of WMDs.[2] Thus, Bermuda based entities must be aware of the risks to their businesses and professions, to prevent them from unwittingly supporting or becoming involved in proliferation financing networks or schemes intended to evade sanctions, in contravention of UN obligations.[3]

[1] FATF. Public Statement on Counter Proliferation Financing. < https://www.fatf-gafi.org/en/publications/Financingofproliferation/Statement-proliferation-financing-2020.html>
[2] FATF. FATF Guidance on Counter Proliferation Financing - The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction. <https://www.fatf-gafi.org/en/publications/Financingofproliferation/Guidance-counter-proliferation-financing.html>
[3] FATF. Proliferation Financing. <https://www.fatf-gafi.org/en/topics/proliferation-financing.html>

3 Proliferation and Proliferation Financing

What is Proliferation?

9. Proliferation is 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, international obligations.[4]

10. Dual Use goods are items that can be used for military and civil purposes. Examples of PF sensitive, Dual Use goods lists is provided in **Annex A**. These items include software and technology. Everyday items such as household cleaners may be considered Dual Use and their absence on export control lists does not disqualify them from being subject to restrictions.[5]

11. The proliferation of weapons of mass destruction (WMD) has a number of elements, including use of, legitimate goods and technology, software, services, and expertise. For instance, this could involve scientific research (such as giving lectures or presentations in or to PF-sanctioned jurisdictions or individuals/entities), the transfer or export of advanced technology, or even the use of basic dual-use goods that have the potential to be used to create explosive devices.

12. While Bermuda does not manufacture or trade in weapons of mass destruction or proliferation goods, Bermuda law requires all natural and legal persons to comply with international sanctions obligations relating to proliferation and PF. This includes legal persons/entities incorporated or formed under Bermuda law.

[4] FATF, Combating Proliferation Financing: A Status Report on Policy Development and Consultation, 2010
[5] Wassenaar Arrangement formally established in July 1996, is a voluntary export control regime whose 42 members exchange information on transfers of conventional weapons and dual-use goods and technologies.

What is Proliferation Financing?

13. The Financial Action Task Force (FATF) definition of PF is "*the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transhipment, 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"*.[6]

14. PF activities are not limited to limited to traditional financial services. PF can be linked to legal and illegal revenue streams that may not overtly suggest that financing of proliferation is occurring. In addition, PF networks are often complex, with financial services forming only a small part of an intentionally intricate puzzle. Understanding the ways those seeking to evade PF prohibitions use different industries and actors to enable access to funds for their illegal proliferation activities provides insight to PF.

15. For example, UN Panel of Experts reports have highlighted the different tactics utilised by the Democratic People's Republic of Korea such as[7]:

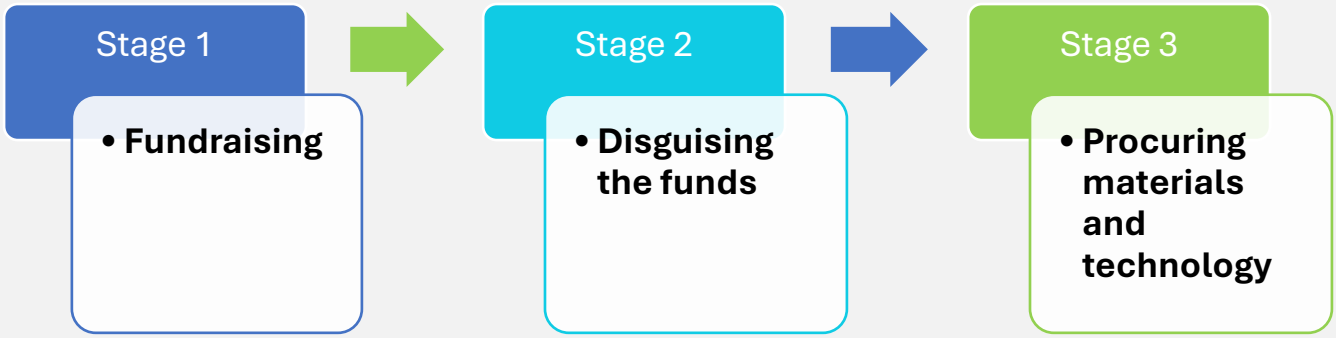
    i. Obfuscation of ownership structures which allows for 'legitimate' access to the international financial system.
    ii. Cyber-attacks and theft of crypto assets worth hundreds of millions of dollars.
    iii. Use of workers (DPRK nationals) to earn income overseas; and
    iv. Sale of arms and military equipment to other countries.

    It is noteworthy that DPRK revenue sources, and therefore its economy, is significantly dependant on external international markets and industries.

[6] FATF, Combating Proliferation Financing: A Status Report on Policy Development and Consultation, 2010
[7] UN Security Council. 1718 Sanctions Committee (DPRK)
https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

Stages of PF

16. There are three stages of proliferation financing. The Centre for a New American Security (CNAS) describes them as follows[8]:



17. **Fundraising:** During stage 1 financing is secured from legitimate and/or illegitimate revenue sources. This may include state budgets, overseas criminal activity as well as overseas commercial enterprises.

18. **Disguising the funds**: Stage 2 is the movement or transfer of the funds through the international financial system. Where a country is not sanctioned, the movement of funds should be uncomplicated. Actors in PF sanctioned jurisdictions (such as DPRK) will employ sophisticated methods to obscure the source of funds in order for the funds to flow into the international financial system. By way of example, funds may be obscured using various techniques such as the use of accounts controlled by foreign nationals; use of false documentation; use of front companies; use of opaque ownership structures; and use of companies in neighbouring countries that support sanctioned regimes.

19. **Procuring materials and technology:** During the final stage, funds that have been transferred (or disguised) into the international financial systems are used to pay for goods, materials, technology and/or logistics needed to for a WMD program. This stage uses international financial institutions to complete such transactions.

[8] Jonathan Brewer, 'The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation', CNAS, January 2018, p. 5.

20. UNSCR 1718 Sanctions Committee Panel of Experts' Reports provide analysis of DPRK's PF stages. The analysis sets out steps taken by DPRK to obtain financing, obscure the source of funds and inject them into the international financial system, followed by procurement and transfer of proliferation goods and technology[9] .

PF Typologies

21. PF typologies illustrate the techniques adopted by bad actors to acquire and conceal funds to produce WMDs. This may include goods, activities and structures employed to evade sanctions measures. The FATF provides typologies of PF relevant activities that could be used to develop weapons or delivery capability, including the transfer of complete systems or the transfer of components, dual-use goods, services, technology, expertise and training, as well as the theft of high value materials from authorised storage facilities with the intention of resale. [10]

22. Direct and indirect categories of PF activities have been identified by the Royal United Services Institute (RUSI, - an independent think tank engaged in cutting-edge research on defence, security and international affairs, including sanctions and proliferation financing):

Activities directly related to the trade in proliferation-sensitive goods

23. Financial products and services related to the trade of proliferation sensitive goods include but are not limited to the following examples[11]:

    i. Use of trade finance products and services and clean payment services for the procurement of proliferation-sensitive goods.
    ii. Use of legal structures such as:
        a. Front companies, i.e. companies that appear to undertake legitimate business, but which serve to obscure illicit financial activity.

[9] UNSC 1718 Sanctions Committee Panel of Experts' Reports <https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports>
[10] FATF Typologies Report on Proliferation Financing < https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf>
[11] Guide to Conducting a National Proliferation Financing Risk Assessment. RUSI <https://static.rusi.org/20190513_guide_to_conducting_a_national_proliferation_financing_risk_assessment_web.pdf >

b. Shell companies, i.e. inactive companies used as a conduit for money that do not have a high level of capitalisation; or which displays other shell company indicators such as long periods of account dormancy followed by a surge of activity.
c. Brokers and professional intermediaries to obtain trade finance products and services, or as parties to clean payments.

iii. Nationals or dual citizens of States that undertake Proliferation, or family members of such persons (regardless of citizenship), used as intermediaries in countries not of Proliferation concern, to facilitate procurement of goods and/or for payment of funds. This method is likely to involve use of personal banking products.
iv. Money transfer services used to transfer cash related to procurement of goods.
v. Use of professional intermediaries and firms to obscure parties to transactions and end users.
vi. Use of fake or fraudulent documents related to shipping, customs or payments to facilitate transactions or trade finance.
vii. Use of financial routes that are indirect to the movement of sensitive goods, or to countries or institutions (such as universities or research institutes) which are not of Proliferation concern.
viii. Use of shipping companies, brokers and agents to obtain insurance or other financial services related to maritime transport. This is often combined with use of Front companies with opaque ownership structures.

Activities indirectly related to the trade in proliferation-sensitive goods

24. The following examples illustrate indirect revenue-raising techniques[12]:

i. Cybercrime, such as hacking accounts to obtain value, largely used by State actors.

[12] Guide to Conducting a National Proliferation Financing Risk Assessment. RUSI <https://static.rusi.org/20190513_guide_to_conducting_a_national_proliferation_financing_risk_assessment_web.pdf >

ii. Use of banks and other financial institutions with foreign or local branches operating in countries of proliferation concern or use of financial institutions with known links to proliferating actors.
iii. Use of cryptocurrencies to avoid the formal financial system, and cybercrime to obtain illicit funds.
iv. Use of diplomats, consular officers or diplomatic or consular missions to build networks which facilitate a range of revenue raising activities. These networks also aide in the use of financial products or services to facilitate trade in goods.
v. Use of trade or other economic relations of countries with links or significant exposure to a country known for proliferation. Often facilitated by a complex corporate network.
vi. Use of organised or transnational criminal networks, particularly their transport corridors and intermediaries in their networks.

25. Generating access to foreign currency and the international financial system is one of the key objectives of PF activity. Gaining such access can occur through what appears to be a legitimate trading transaction. Thus, to combat PF, it is critical to understand the entire payment chain and consider whether any trade may be used to facilitate illicit activity [see Annex C, which illustrates the use the international financial system for proliferation evasion].

PF vs Money laundering and Terrorist financing

26. PF can be described as both a distinct financial crime risk and a sanctions risk. It may share certain characteristics with other forms of financial crime, such as Money laundering and/or Terrorist financing.

	PF	ML	TF
Purpose	Acquiring and enabling the proliferation of WMD	Use of illicit funds in the regulated system by obscuring their origins	Supports terrorist acts, activities and organisations
Source of funds	Can be from illicit activities or state-sponsored programs	Funds from illicit activity within criminal organisations	Funds from various sources which may or may not be illicit (e.g. sponsors, fund raising, exploitation of national resources, etc.)
Conduits	Favours formal financial system	Favours formal financial systems	Use of regulated and unregulated financial systems. This may include currency exchange, cash couriers, hawala, etc.
Detection Focus	Individuals, entities, states, goods and materials, activities	Suspicious transactions such as deposits uncharacteristic of customer's wealth or the expected activity	Suspicious relationships, such as wire transfers between seemingly unrelated parties
Transaction Amounts	Small and moderate amounts	Larger amounts that are structured to avoid reporting requirements	Various sized amounts usually below reporting threshold
Financial Activity	Transactions look like normal	Complex web of transactions often	Varied methods including formal

	commercial activity, structured to hide origin of funding	involving shell or front companies, bearer shares, and offshore secrecy havens	banking system, informal value transfer systems, smuggling of cash and valuables
Money Trail	Linear – funds are used to purchase goods and materials from brokers. Traders or manufacturers	Circular – money will eventually end up with the person who generated it after the origins have been sufficiently obscured	Linear – money generated is used to promote terrorist groups, infrastructure and their activities

Source: Adapted from Jersey Financial Services Commission Comparison: Terrorist Financing, Money Laundering, and Financing the Proliferation of Weapons of Mass Destruction and Cayman Islands Guidance Notes on Proliferation Financing

27. PF risk characteristics are significantly different from ML and TF[13]:

i. PF threats are typically posed by Proliferation networks, created by those targeted by UNSCR designated sanctions to disguise their activities, which includes those acting on their behalf of, or at their direction. As a result, their financing needs and methods may not necessarily be the same as those of other criminal actors.
ii. Since PF networks may derive funds from both criminal activity and/or legitimately sourced funds, transactions related to PF may use the international financial system under the umbrella of legitimate business and may not exhibit the same characteristics as Money laundering and/or Terrorist financing.
iii. The number of customers or transactions related to Proliferation activities is likely to be smaller than those involved in other types of financial crime.

28. In addition, although predicate offences and criminal actors are relevant considerations for PF, the complex nature of PF means that the range of possible threats is broader than considering Money laundering, or Terrorist financing, in isolation. That is, with PF there is

[13]Guidance on Countering the Financing of Proliferation of Weapons of Mass Destruction. Jersey Financial Services Commission < https://www.jerseyfsc.org/media/6592/countering-proliferation-of-weapons-of-mass-destruction-and-its-financing.pdf>

also the threat of legitimate funds/resources being employed for illicit purpose to enable PF and circumvent sanction prohibitions.

What are the difficulties faced with identifying and combatting PF?

29. Identifying PF transactions can be challenging as they may appear to be normal commercial activity, structured to conceal connections to the proliferator or proliferation activities. Difficulties associated with identifying PF include: [14]

    i. A growing trend in the purchase and sale of elementary and replaceable components, as opposed to whole manufactured systems, making their identification increasingly problematic. In addition, identification of Dual Use items and Proliferation sensitive commodities often requires specialist knowledge and expertise[15].
    ii. PF networks tend to be complex. This, combined with the use of false documentation, may allow for Proliferation sensitive goods, the entities involved, the associated financial transactions and the ultimate end-user to avoid detection. Front companies, agents and other false end-users may be used to obscure the ultimate end-user.
    iii. The risk of PF will be heightened in cases where the source of funds is legal, but the end-user of the goods involved is obscured, making identification of such activities challenging.
    iv. Trade finance activities, often used for sanctions evasion, tend to have a fragmented nature, where multiple parties (in many cases with limited knowledge of one another) become involved in the PF activity.

Emerging threats in combatting PF

[14] Financial Networks of Mass Destruction. CNAS < >
[15] Financial Crime Risk Controls: Dual-Use Goods and Proliferation Financing. ICC < https://iccwbo.org/wp-content/uploads/sites/3/2019/06/2023-ICC-Financial-crime-risk-controls-Dual-use-goods-and-proliferation-financing.pdf>

30. Emerging threats in combatting PF include[16]:

i. Proliferation networks now have additional ways to evade sanctions through the use of cryptocurrencies as they are difficult to trace and can be laundered repeatedly. "Blockchain" based technologies effectively decentralise processing of transfers. Therefore, a record of transactions can be stored and verified through the consensus of a network's users, rather than through a central data- collection or settlement authority.

ii. Technologies of concern such as three-dimensional printing, synthetic biology, chemical synthesis, nano-biotechnology etc *could allow for the easier production of standard chemical or biological agents, or, less probably, the creation of novel agents with a* substantially lower risk of detection by the international community. The financing of such technologies could be used to evade prohibitions in place to combat proliferation.

31. , In 2021 the EU established a new Union regime for the control of exports, brokering, technical assistance, transit and transfer of Dual Use items as a part of international efforts to combat PF. It covers challenging categories of exporters, such as service providers, researchers, consultants, persons transmitting Dual Use items electronically, especially scientists and academic and research institutions, involved in cutting edge technologies, who all need to be aware of PF risks.

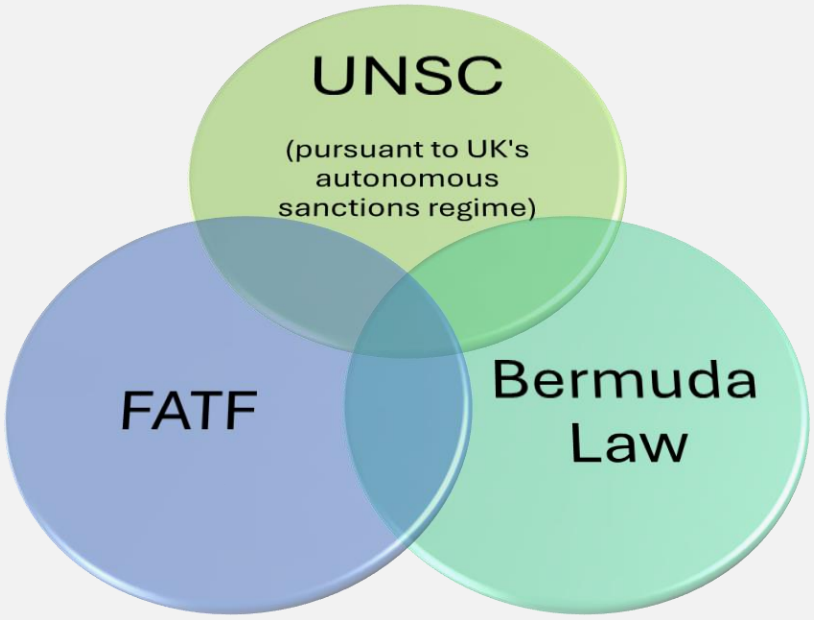
[16] Emerging Threats in Combating Proliferation Finance. CNAS https://s3.us-east-1.amazonaws.com/files.cnas.org/backgrounds/documents/CNAS-Report-Emerging-Threats-Final.pdf

4 Obligations to Counter PF

Overview

32. All individuals and legal entities in who are within or undertake activities in Bermuda must comply with UN and UK sanctions that are in force in Bermuda. Further, sanctions will apply to a 'territory person' wherever they are in the world, as well as apply to Bermuda registered ships and aircraft wherever they are in the world.

33. The Frameworks to combat PF encompasses global obligations and standards as well as domestic law, namely:
    i. International legal obligations put in place by the UNSC (via the UK framework and brought into force via domestic legislation).
    ii. FATF Recommendations; and
    iii. Bermuda Law.



International Obligations

UNSCR

34. United Nations (UN) obligations extend to Bermuda through the membership of the United Kingdom. Accordingly, Bermuda is required to implement PF related UNSCRs:

UN Security Council Resolution 1540 (2004)[17]	Broad based provisions that: i. Prohibit the financing of proliferation related activities by a non-state actor; and ii. require countries to establish develop, review and maintain appropriate controls on providing funds and services (such as financing) related to the export and trans-shipment of items that would contribute to proliferation of WMD.[18]
UN Security Council Resolution 1718 (2006) and UNSCR 2231 (2015) and all successor resolutions	Imposition of an arms embargo, assets freeze, and travel ban on persons involved in the DPRK's nuclear programme, and a ban on a range of imports and exports, to prohibit the DPRK from conducting nuclear tests or launching ballistic missiles.[19]
UN Security Council Resolution 2231 (2015)	Provides for the termination of the provisions of previous Security Council resolutions on the Iranian nuclear issue and establishes specific restrictions that apply to all States without exception. Member States are obligated under Article 25 of the Charter of the United Nations to accept and carry out the Security Council's decisions.[20] This is also referred to as the Joint Comprehensive Plan of Action (JCPOA), which replaces previous resolutions related to Iran.

[17] United Nations. UN Security Council Resolution 1540 (2004) https://disarmament.unoda.org/wmd/sc1540/
[18] FATF Recommendation 2 obligations.
[19] United Nations Security Council. S/RES/1718 (2006) https://www.un.org/securitycouncil/s/res/1718-%282006%29
[20] United Nations Security Council. Resolution 2231 (2015) on Iran Nuclear Issue https://www.un.org/securitycouncil/content/2231/background

FATF Standards

35. The FATF Standards establish global standards for implementing Targeted Financial Sanctions relating to the prevention, suppression and disruption of proliferation of WMD and PF (see key FATF Recommendations in the table below).:

FATF Recommendation	Requirement
Rec 1	requires countries, financial institutions, designated non-financial businesses and professionals, virtual asset service providers, and non-profit organisations to identify and assess the risks of potential breaches, non-implementation or evasion of TFS-PF and to take action to mitigate them.
Rec 2	calls on domestic cooperation and coordination of the relevant authorities to combat money laundering, Terrorist Financing and PF.
Rec 7	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, any person or entity designated by, or under the authority of, the UNSC under Chapter VII of the Charter of the UN.
Rec 15	requires countries to conduct a PF risk assessment and establish mitigation in respect of virtual asset activities and service providers.

The FATF Standards require that private sector entities have processes in place to identify, assess, monitor, manage and mitigate proliferation financing risks. Further, FATF Recommendations clearly set out country obligations to ensure that private sector entities are made aware of the PF risks to their businesses and professions, and that they

understand that they must not engage in activities which support or involve PF networks or schemes.

36. Entities should consult FATF's Guidance on Counter Proliferation Financing - The Implementation of Financial Provisions of United Nations Security Council Resolutions to counter proliferation of weapons of mass destruction as this non-binding guidance aims to assist public and private sector stakeholders in understanding and implementing FATF obligations, as well as provide guidance on how to prevent sanctions evasion.

Domestic sanctions obligations

37. In addition to international obligations, Bermuda legislation creates obligations for legal persons. This framework includes the legislation below:

- International Sanctions Act 2003
- International Sanctions Regulations 2013
    - The Democratic People's Republic of Korea (Sanctions) (Overseas Territories) Order 2020
    - The Iran (Nuclear) (Overseas Territories) Order 2020
- International Sanctions (Delegation of Governors Functions) Notice 2018
- Proceeds of Crime Act 1997
- Proceeds of Crime Regulations 1998
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Designation Order 2012
- Charities Act 2014

Bermuda's sanctions framework targeting PF

38. Recommendation 1 of the FATF standards requires Bermuda to *"identify, assess, and understand the proliferation financing risks for the country and respective private sector, and to take action to mitigate these risks."*.[21]

39. The Minister of Justice is the competent authority responsible for sanctions implementation and Minister's authority is pursuant to the International Sanctions (Delegation of Governors Functions) Notice 2018. The Financial Sanctions Implementation Unit (FISU) provides technical support to the Minister to ensure effective implementation of sanctions in Bermuda. The FSIU also assists with the implementation of trade sanctions. Other sanctions measures, such as arms embargos and other trade restrictions, are implemented by the Bermuda Customs Department.

40. Sanctions in Bermuda are implemented by the International Sanctions Act 2003 and the International Sanctions Regulations 2013. All sanctions regimes listed in the Schedule of the International Sanctions Regulations 2013 have the force of law in Bermuda giving effect to:

    i. international obligations of the United Kingdom relating to economic or other sanctions imposed on any country, organisation, person or group of persons; or
    ii. any sanctions imposed by the United Kingdom for any purpose listed in section 1(2) of the UK's Sanctions and Anti-Money Laundering Act 2018.

41. The Bermuda Customs Department has broad powers to exercise supervision and control of all prohibitions and restrictions on the importation and exportation of goods – including the traditional subjects of export control. UK export controls have been extended to Bermuda by the Export of Goods, Transfer of Technology and Provision of Technical Assistance (Control) (Overseas Territories) Order 2004.

42. This Order provides a framework for the control of strategic goods and brings together controls on the export or transfer of military and Dual Use goods, software and technology, controls on goods, software and technology related to weapons of mass destruction (WMD) and the provision of WMD-related technical assistance. These controls apply to persons in Bermuda and in respect of certain provisions, to United Kingdom persons ordinarily resident in UK Overseas Territories anywhere in the world.

[21] https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf

43. By virtue of Bermuda's Overseas Territory status and the International Sanctions Regulations 2013, the UK's autonomous sanctions framework under the Sanctions and Anti-Money Laundering Act, 2018 (SAMLA) applies in Bermuda. Accordingly, the UK Consolidated List as well as the UK Sanctions List constitute all designations in force in Bermuda.

Sanctions Compliance reporting obligations and process

44. Financial Sanctions obligations under the Bermuda sanctions regime, which include proliferation financing, require all relevant firms, natural and legal persons, entities and bodies to supply the FSIU as soon as practicable, with any information if they know or reasonably suspect a person is designated or has committed offences under the International Sanctions Regulations, where such information is received in the course of carrying on their business.

45. The International Sanctions Regulations 2013, which enforces the UK Regulations, set out specific reporting obligations for relevant firms (see glossary).[22]

46. If you are a relevant firm, you must submit a Compliance Reporting Form (CRF) to the FSIU as soon as practicable if you know or have a reasonable cause to suspect that a person:

    - is a designated person.
    - has committed an offence under the legislation.

47. Failure to report knowledge or reasonable suspicion of proliferation financing where the information or other matter on which the knowledge or cause for suspicion is based came to you while carrying on its business is an offence. On conviction, the penalty for this offence is imprisonment for a term not exceeding 6 months, or a fine not exceeding £5,000 or its equivalent in Bermuda dollars, or both.[23]

[22] The Democratic People's Republic of Korea (Sanctions) (Overseas Territories) Order 2020, Schedule 2, Section 69

[23] The Democratic People's Republic of Korea (DPRK) (Sanctions) (EU Exit) Regulations 2019 as amended (regulation 101)

48. In addition to submitting your report to the FSIU, you must file all Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs) related to Proliferation Financing (PF) with the Financial Intelligence Agency (FIA) via their goAML reporting platform: https://www.fia.bm/sars/.

PF risk assessment and mitigation

49. Key FATF recommendations relating to PF:
    a. FATF Recommendation 1, notes that PF risk refers strictly and only to the potential breach, non-implementation or evasion of the TFS-PF obligations referred to in FATF Recommendation 7.
    b. FATF Recommendation 7 sets out strict obligations to implement, without delay, TFS- PF related to two country specific regimes:
        i. The Democratic People's Republic of Korea (DPRK)
        ii. Iran (Nuclear).

50. The FATF narrowly defines PF risk to access compliance with this obligation as[24]:

    The risk of raising moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual -use technology and dual-use goods for non-legitimate purposes).

    Supervised entities must understand these risks and ensure that they have adequate policies and procedures in place to identify, assess, monitor, manage and mitigate them.

Rules-based approach

51. A rules-based approach to risk involves compliance strictly with the regulations; freezing assets, non-engagement with DPs, it is 'black and white' compliance. This means screening relevant parties (customers, associates, third parties) against relevant designations lists, assessing ownership and control, monitoring and recording export control and related sanctions matches.

[24] Guidance on Proliferation Financing Risk Assessment and Mitigation < https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf>

52. Sanctions compliance is mandatory and does not generally serve as a model for developing a risk-based approach to combat PF. These obligations are not risk-based, instead they are unavoidable in any risk scenario/situation.

Risk-based approach

53. Risk-based approach requires Supervised entities to identify, assess and understand their TFS-PF risks when dealing with their customers, and take appropriate mitigating action commensurate with the level of risks identified in order to fully comply with Recommendation 7 of the FATF Standards.

54. This approach requires wider screening of sources of PF, such as lists of designations under other sanctions regimes in other jurisdictions, customised to a Supervised Person's database, geographical links and other associations relevant to PF. For example, UNSC Panel of Expert reports on DPRK identify legal persons that are involved in PF activities, however they have not been sanctions by the UN. This type of information is critical to the wider screening considerations.

55. RUSI's DPRK Reports database contains structured information relating to the activities of entities that assist North Korea to develop prohibited weapons programmes and evade sanctions. The data is sourced from the United Nations Panel of Experts reports, from 2010 to 2023, as well as the associated UN sanctions resolutions. It includes profiles of the persons, companies, organisations, and vessels that are mentioned in the reports, and contains information such as names, aliases, locations, contact details and sanction designation status. The database also records the relationships between entities and their involvement or relationship to specific events.[25] This tool can buttress one's approach to risk by providing information that could assist in understanding and in mitigation of exposure.

56. Risk-based measures should be proportionate to the overall Proliferation risk associated with customers, geographical location, products and services, transactions and even processes. For example, a business operating internationally or with an international client base will generally involve the assessment of a wider range of risks. A list of

[25] DPRK Reports Database. RUSI https://dprk-reports.org/ - Annex F

examples of PF evasive patterns and potential exposure to PF risks, including detailed case studies can be found in Annex C – Sources for PF case studies.

Chapter 5 provides examples of risk factors which may be relevant to formulating a Proliferation focussed risk assessment within existing sanctions, or general compliance monitoring programmes.

5 PF risks categories

Country/geographic risk

57. Certain relationships with specific countries may indicate an increased PF risk this may include:

i. Business ties and financial relationships with a country that is subject to UN sanctions imposing WMD-related restrictions (for example, DPRK, or friendly countries with geographical proximity) (Annex G).
ii. Business ties and financial relationships in countries with diplomatic, trade, or corporate links to States of Proliferation concern, or geographically close to them, for example, countries involved in Proliferation networks identified in the UNSC's Panel of Experts' reports.
iii. Links to countries subject to other WMD Proliferation restrictions, for example, an "embargoed destination" or other Proliferation concern countries' lists identified in Schedules 1 to 4 of the UK's Export Control Order 2008
iv. Links with countries presenting on-going and substantial financial crime risks, for example countries with strategic trade controls deficiencies identified by the Peddling Peril Index (PPI)
v. Links to countries with high levels of terrorist activities, corruption, civil unrest, organised crime related to arms dealing etc. are also relevant factors to be considered.

Customer risk

58. Customer activities that may indicate a higher PF risk could include:

i. Customers on national lists concerning WMD Proliferation
ii. Military or research body connected with a higher-risk jurisdiction of Proliferation concern.
iii. Customers and third parties involved in the manufacture, supply, purchase, or sale of Dual Use items, Proliferation-sensitive or military goods.
iv. Customers with a small trader/intermediary, who may be a dual- national of a country of Proliferation concern.
v. Customers located in a major financial or trade centre.

vi. Customers involved in the maritime industry, such as those that own, operate, and/or provide services to ships operating in areas that have been identified as posing a high risk for sanctions evasion.
vii. Universities or research institutions with nuclear physics or related departments and a history of violations of sanctions or export controls and/or sanctions circumvention.

Product and services risk

59. Factors relating to Product and service that may suggest higher PF risks:

i. Delivery of services possibly subject to sanctions, e.g. correspondent banking services with institutions subject to UN DPRK sanctions
ii. Project financing in jurisdictions of Proliferation concern for sensitive industries
iii. Trade finance services, transactions, and insurance products involving jurisdictions of Proliferation concern (for example, direct loans or a general credit facility to facilitate export transactions; purchase of promissory notes or bills of exchange issued by foreign buyers to exporters for the purchase of goods and services, freeing up cash for the exporter; factoring - the purchase or discounting of a foreign account receivable for cash at a discount from the face value; provision of guarantees to or by financial institutions on behalf of exporters such as pre-shipment guarantees and performance guarantees; or provision of insurance against certain risks in the trading process)
iv. Shipping/transfer of Dual Use goods, Proliferation-sensitive goods and materials to a country of Diversion concern. (i.e. transactions that diverge funds/resources away from their legitimately intended purpose to directly or indirectly benefit Proliferators)
v. Insurance and re-insurance services relating to the Maritime industry.

60. A risk-based approach should be designed to emphasise the areas of highest perceived vulnerability for a person or entity engaged in the breach, non-implementation, or evasion of TFS-PF to counter PF.

61. Mitigating factors should also be considered. For example, whether a customer is aware of Proliferation risks and has systems and processes in place to ensure its compliance with export control obligations and can provide copies of valid export control licences.

6 Effective approach to PF risk mitigation

62. In order to ensure entities are not dealing with legal persons subject to sanctions (directly or indirectly), effective TFS-PF risk mitigation should be implemented or put in place. PF risk mitigation includes:

    i. Acknowledging that proliferation financing is a common problem for many major financial centers due to the unwitting involvement of various financial institutions worldwide.

    ii. Ongoing monitoring should not be limited to screening clients against the Consolidated List. That is, ongoing monitoring should also extend to identification of assets subject to applicable TFS. Thus, should an existing client be designated, any assets belonging to the client and held by an entity should be frozen.

    iii. Conduct risk assessment of customers and products, country/geographic and delivery channels – with special attention to trade finance and insurance.

    iv. Be alert to the possibility that your customers may be engaging in, or facilitating, proliferation activities.

    v. Conduct enhanced due diligence on high-risk transactions and entities.

    vi. Develop situational awareness around various sanctions regimes by reading UN Panel of Experts reports.

Vulnerabilities/Mitigation for PF Sanctions - Breaches and Evasion

RISK OF BREACH OF SANCTIONS	
Vulnerabilities	i. Poor customer on-boarding procedures ii. Inadequate on-going transaction monitoring and sanctions screening processes and procedures such as use of outdated sanctions lists and poor accuracy in matching names to sanctions lists) iii. staff training that is ineffective or none at all iv. Poor risk management procedures v. Lack of healthy compliance culture (e.g., poor governance and risk management practices, lack of transparency and/or poor accountability) vi. internal controls that are Inadequate and ineffective (e.g., poor customer due diligence and record-keeping procedures) vii. Lack of enhanced TFS-PF controls including screening of direct and indirect third parties and associates, extended supply chain parties, third party payees, Dual Use items or other restricted items, in identified high risk scenarios with connections to jurisdictions known to have strong links to the enhanced risk states.
Mitigation	i. Adequate and effective customer on-boarding processes (including ownership and control thresholds and the nature and purpose of their business relationships) ii. Effective maintenance of customer data iii. Maintaining and managing Internal watch lists of legal persons, vessels and aircraft identified as potentially related to the TFS-PF designations. iv. Adequate controls to ensure effectiveness of procedures for sanctions screening to identify and mitigate potential sanctions evasion. v. Maintenance of sound processes and internal controls, ensuring comprehension of and compliance with them vi. Providing training to staff that includes PF risks, typologies, required risk mitigation measures. vii. Timely and ongoing monitoring and incorporation of amendments to UN designations viii. Demonstration of awareness of non-designated persons and entities that have been reliably identified as having connections to PF activities by third parties such as RUSI.
RISK OF SANCTIONS EVASION	
Vulnerabilities	i. Limited understanding what sanctions risk looks like

	ii. Lack of risk-based measures to mitigate sanctions evasion tailored to an organisation. iii. Failure to screen underlying assets of customers and their subsidiaries (e.g., ships, aircrafts etc.) iv. Outsourcing sanctions screening and reliance on Group policies and third-party providers without adequate controls and testing of their functions.
Mitigation	i. Incorporation of, and continued review and update of, relevant sanctions evasion information into internal risk management policies and procedures ii. Tailored sanctions staff training iii. Supplementing reliance on list-based screening by enhanced customer due diligence measures to also capture indirect relationships and underlying assets which may be included on a sanctions list. iv. Understanding the overall structuring and rationale. v. Maintaining documentation which clearly sets out who is responsible for the screening systems within a Group and maintain access to that function

63. The UK Financial Conduct Authority breaks good and poor TFS-PF compliance down into 5 categories for firms; governance, risk assessment, screening, matches and escalation and weapons proliferation:[26]

GOOD PRACTICE	POOR PRACTICE
GOVERNANCE	
An individual of sufficient authority is responsible for over- seeing the firm's adherence to the sanctions regime. Without a licence from the Asset Freezing Unit, this could be a criminal offence. **It is clear at what stage customers are screened in different situations (e.g. when customers are passed from agents or other companies in the group).**	The firm believes payments to sanctioned individuals and entities are permitted when the sums are small. No internal audit resource is allocated to monitoring sanctions compliance. Some business units in a large organisation think they are exempt.

[26] Financial Crime Guide: A Firm's Guide to Countering Financial Crime Risks (FCG) https://www.handbook.fca.org.uk/handbook/FCG.pdf

There is appropriate escalation of actual target matches and breaches of UK sanctions. Notifications are timely.	
RISK ASSESSMENT	
A firm with international operations, or that deals in currencies other than sterling, understands the requirements of relevant local financial sanctions regimes. **A small firm is aware of the sanctions regime and where it is most vulnerable, even if risk assessment is only informal.**	There is no process for updating the risk assessment. The firm assumes financial sanctions only apply to money transfers and so has not assessed its risks.
SCREENING	
The firm has considered what mixture of manual and automated screening is most appropriate. **There are quality control checks over manual screening.** **Where a firm uses automated systems, these can make 'fuzzy matches' (e.g. able to identify similar or variant spellings of names, name reversal, digit rotation, character manipulation, etc.).** **The firm screens customers' directors and known beneficial owners on a risk-sensitive basis.** **Where the firm maintains an account for a listed individual, the status of this account is clearly flagged to staff.** **A firm only places faith in other firms' screening (such as outsourcers or intermediaries) after taking steps to satisfy themselves this is appropriate.**	The firm assumes that an intermediary has screened a customer but does not check this. Where a firm uses automated systems, it does not understand how to calibrate them and does not check whether the number of hits is unexpectedly high or low. An insurance company only screens when claims are made on a policy. Screening of customer data bases is a one-off exercise. Updating from the Consolidated List is haphazard. Some business units use out-of-date lists. The firm has no means of monitoring payment instructions.
MATCHES AND ESCALATION	

Sufficient resources are available to identify 'false positives'. **After a breach, as well as meeting its formal obligation notify [FSIU], the firm considers whether it should report the breach to the [FSIU and their supervisor]. FSIU Guidance contains general reporting requirements. Firms are required to report frozen assets, suspected designated persons and suspected breaches.**	The firm does not report a breach of the financial sanctions regime to OFSI: this could be a criminal offence. An account is not frozen when a match with the Consolidated List is identified. If, consequently, funds held, owned or controlled by a designated person are dealt with or made available to the designated person, this could be a criminal offence. A lack of resources prevents a firm from adequately analysing matches. No audit trail of decisions where potential target matches are judged to be false positives.
WEAPONS PROLIFERATION	
A bank has identified if its customers export goods to high-risk jurisdictions, and subjects such transactions to enhanced scrutiny by identifying, for example, whether goods may be subject to export restrictions, or end-users may be of concern. **Where doubt exists, the bank asks the customer to demonstrate that appropriate assurances have been gained from relevant government authorities.**	The firm assumes customers selling goods to countries of concern will have checked the exports are legitimate and does not ask for evidence of this from customers. A firm knows that its customers deal with individuals and entities from high-risk jurisdictions but does not communicate with those customers about relevant regulations in place and how they affect them.

7 Risk indicators of the potential breach, non-implementation or evasion of TFS-PF

FATF PF risk indicators

Risk indicators for Customer profile, transaction activity and jurisdiction

CUSTOMER	TRANSACTION	JURISDICTION
• Individual or entity targeted by sanctions or connected to a targeted person. • Customer is involved in the supply, sale, delivery, or purchase of dual-use, proliferation-sensitive or military goods, particularly to higher risk jurisdictions. • Customer is vague, particularly about end user and end use; provides incomplete information or is resistant to providing	• Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws. • The transaction involves an individual or entity in a foreign country of proliferation concern. • Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose. • Missing/ fraudulent documents	• Countries with weak financial safeguards and which are actively engaged with a sanctioned country. • A presence of an industry that produces dual-use goods, proliferation-sensitive items, or military goods.

additional information when sought.		

64. The FATF provided a non-exhaustive list of PF risk indicators related to a potential breach, non-implementation or evasion of TFS-PF in 2021. The information provided below is based on PF typologies to provide further clarity of wider PF risks and also incorporates other expert studies.

i. During on-boarding, a customer provides vague or incomplete information about their proposed trading activities, appearing reluctant to provide additional information when further questions are raised.

ii. When carrying out relevant due diligence processes, a customer, particularly a trade entity, its owners or senior managers, appear on sanctioned lists, or on a list of denied persons for the purposes of export control regimes, or are noted in adverse news reports alleging criminal activity, or on-going or past investigations or convictions.

iii. The customer/client is connected with a country of Proliferation or Diversion concern, e.g. through business or trade relations.

iv. The customer is deemed to be a person dealing with Dual Use items, or goods subject to export control goods, or complex equipment for which they lack technical background, or which is inconsistent with their stated line of activity, or which otherwise does not appear to align with expectations or makes sense.

v. A customer/client engages in complex trade deals involving numerous third-party intermediaries, in lines of business that do not concur with their stated business profile provided during the on boarding of the business.

vi. A customer or counterparty, proclaimed to be a commercial business, conducts transactions consistent with a money-remittance business or as a pay-through account. Such accounts may involve a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons for the transactions. In certain instances, the activity associated with originators appear to be entities who may be connected to a State-sponsored Proliferation programme (e.g. Shell companies operating near countries of Proliferation or Diversion concern), and the beneficiaries appear to be associated with manufacturers or shippers subject to export controls.

vii. Customers associated with a university or research institution involved in the trade of Dual Use goods subject to export control.

viii. Customers dealing directly or indirectly, with trade of sanctioned goods or under embargo, such as oil or other commodities, luxury goods, metals etc.

Account and transaction activity risk indicators

65. The Parties to transactions (originator or beneficiary) are a person or an entity ordinarily resident of or domiciled in a country of Proliferation or Diversion concern (e.g. DPRK and Iran).

66. Account holders conduct transactions that involve items controlled under Dual Use- or export control regimes, or the account holders have previously violated requirements under Dual Use or export control regimes.

67. Transactions and accounts which involve companies with opaque ownership structures, Front companies, or Shell companies.

68. Evidence of links and/or patterns between representatives of companies exchanging goods, e.g. the same owners or management, same physical address, IP address or telephone number, or which otherwise indicates their activities may be co-ordinated.

69. A customer's financial transactions appear to be conducted in an indirect manner; not appearing to make business sense.

70. Account activity or transactions where the Parties (originator or beneficiary) of associated financial institutions is domiciled in a country with weak implementation of UNSCR obligations and FATF Standards, or a weak export control regime (also relevant to correspondent banking services, however Bermuda banks do not offer correspondent banking services).

71. A customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or for trade transactions more generally. Desire to use cash by customers/trading firms for trade transactions or for the purchase of industrial items.

72. For financial institutions, the transactions are visible through sudden influxes of cash deposits to the entity's accounts, followed by cash withdrawals.

73. Transactions are made based on ledger arrangements that remove the need for frequent international financial transactions. Ledger arrangements are conducted by linked companies who maintain a record of transactions made on each other's behalf. Occasionally, these companies will make transfers to balance their accounts.

74. Use of personal accounts to purchase industrial items which are subject to export control, or that are not generally associated with typical lines of business.

Trade finance risk indicators

75. Prior to the account approval, the customer requests letter of credit for a trade transaction for shipment of Dual Use items or goods subject to export control.

76. Gaps in information or inconsistencies in trade documents and financial flows, such as names, companies, addresses, final destination etc.

77. Transactions involving payment instructions/details relating to parties not identified on the original letter of credit or other documentation.

Maritime sector risk indicators

78. Registration of a trade entity at what maybe a mass registration address, e.g. high-density residential buildings, post-box addresses, commercial buildings or industrial complexes, especially when the address does not reference a specific unit and appears incomplete.

79. The entity/person preparing a shipment lists a freight forwarding firm as the final destination for the product(s).

80. The shipping address or destination of a shipment is different from the importer's location and/or address.

81. Inconsistencies are identified across contracts, invoices, or other trade documents. By way of example:
    i. the name of the exporting entity and the name of the recipient of the payment are not the same.
    ii. invoices and underlying contracts have different prices.
    iii. Discrepancies between the quantity, quality, volume or value of the actual goods/commodities and their descriptions, or which otherwise do not appear to correctly reflect what is to be anticipated.
    iv. Low declared value on shipment of goods in comparison with the shipping cost.
    v. Import/ export of goods does not align with the industrial character or with geographical trade patterns of the countries involved, e.g. semi-conductor manufacturing equipment being shipped to a country that has no electronics industry.
    vi. Unusual shipment of goods that is made in an indirect fashion that cannot be easily explained, including multiple destinations with no apparent business or commercial purpose, indications of frequent flags hopping (flags of convenience practices), or using a small or old fleet.
    vii. Shipment of goods is routed through a country with weak implementation of relevant UNSCR obligations and FATF Standards, export control laws or weak enforcement of export control laws.
    viii. Payment made by a person/entity other than the consignee of the commodities for no clear economic reasons, e.g. by a Shell company or Front company not involved in the trade transaction.

Other non-tangible Proliferation and PF sensitive risk indicators

82. These may include:
    a. Overseas research agreements, or training at universities and research centres.
    b. Acquisition of foreign licences or patents.
    c. Merging with/absorbing/acquiring foreign companies that produce sensitive or export control goods.

8 Glossary

Terms used in this document are defined as follows:

CPF	Counter the financing of proliferation of weapons of mass destruction
Diversion	Transactions that divert funds/resources away from their legitimately intended purpose to benefit Proliferators, directly or indirectly
DPRK	Democratic People's Republic of Korea (North Korea)
Dual use items	Items including, for example, software and technology which can be used for both civil and military purposes
EU	European Union
FATF	Financial Action Task Force
FATF Standards	The FATF Recommendations, the international anti-money laundering and combatting the financing of terrorism and proliferation (AML/CFT/CPF) standards, and the FATF Methodology to assess the effectiveness of AML/CFT/CPF systems
Front company	A company that appears to undertake legitimate business, but which is actually serving to obscure illicit financial activity.
IFC	International Finance Centre
The Minister	Minister of Justice
Money laundering	Laundering the proceeds of crime as defined in section 2 of the POCA
NAMLC	National Anti-Money Laundering Committee
PF	Proliferation Financing (financing of Proliferation of weapons of mass destruction)
POCA	Proceeds of Crime Act 1997
Proliferation	Proliferation of weapons of mass destruction - 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 Dual use items used for illicit purposes), in contravention of national laws or, where applicable, international obligations
Proliferator	A State, natural or legal person, or a legal arrangement, undertaking Proliferation may, at times, be referred to as a Proliferator
Relevant firm	Defined as follows[28]: a. a relevant institution. b. an undertaking that by way of business— i.operates a currency exchange office,

	ii.transmits money (or any representation of monetary value) by any means, or iii.cashes cheques that are made payable to customers. c. a firm or sole practitioner that provides to other persons, by way of business— i.accountancy services, ii.advice about tax affairs, iii.auditing services, iv.legal or notarial services, or v.trust or company services. d. a firm or sole practitioner that carries out, or whose employees carry out, estate agency work. e. the holder of a licence to operate a casino in the Territory. f. a person engaged in the business of making, supplying, selling (including selling by auction) or exchanging— i.articles made from gold, silver, platinum or palladium, or ii.precious stones or pearls.
RUSI	Royal United Services Institute
Shell company	A company that does not itself do or own anything but is used to hide a person's or another company's activities, sometimes illegal ones. [29]
Supervised Entity	Persons supervised by a supervised authority as defined in Proceeds of Crime Act 1997.
Terrorist financing	The financing of terrorist act, and of terrorists and terrorist organisations, regulated as conduct which is an offence pursuant to sections 5, 6, 7 or 8 of the Anti-Terrorism (Financial And Other Measures) Act 2004 or an act that would constitute such an offence if carried out in Bermuda.
TFS	Targeted financial sanctions. This means both[30]: i.asset freezing; and ii.prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
TFS-PF	Targeted financial sanctions relating to the prevention, suppression and disruption of Proliferation of weapons of mass destruction and proliferation financing.
UK	United Kingdom

UN	United Nations
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution under article 41 of the UN Charter
WMD	Weapons of mass destruction, including, for example, atomic explosive weapons, lethal biological and chemical weapons, radioactive material weapons and any weapons developed in the future which have comparative destructive effects

9 Annex A – PF sensitive and export control goods

Example documents

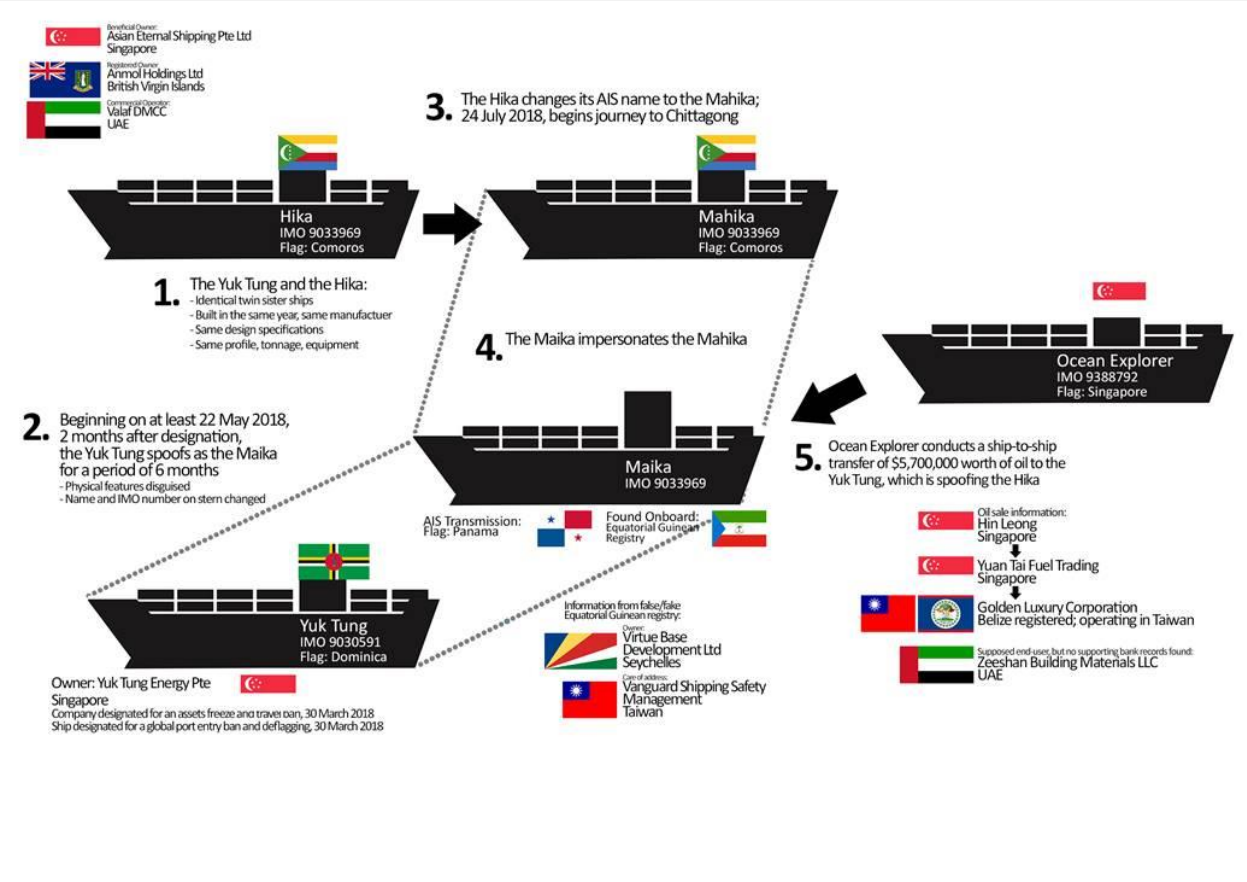
92. Useful export control resources are:

- Nuclear Suppliers Group (NSG) – Nuclear materials and technology, including Dual use items.
- Missile Technology Control Regime (MTCR) – Technology for WMD delivery systems.
- Wassenaar Arrangement – Conventional arms trade and Dual use items.
- The Australia Group – Materials and technology needed for chemical and biological weapons.
- Zangger Committee – Technology needed in production of fissile nuclear material.
- EU - List of all Dual use items and controlled items (Regulation (EU) 2021/821) and subsequent amendments.
- UNSC:
    - DPRK Panel of Experts' reports and
    - Iran designations List
- UK lists of Export control goods, Software and Technology

10 Annex B – Ship-to-ship transfer: the Yuk Tung Case[27]

93. In this case, a disguised ship was renamed and re-flagged repeatedly to bring oil to a purported UAE end-user, but the shipment likely went to North Korea. Actors working for or with the DPRK in the British Virgin Islands, Seychelles, UAE, Singapore, Taiwan, and possibly other countries or territories used methods that had been tried and tested before, such as establishing or utilizing front companies in weak jurisdictions and presenting sanctions evasion activity as legitimate business activity to potential partners and businesses. However, beyond these methods, the DPRK's network also employed advanced evasion techniques in shipping, including identity theft, acquiring multiple registrations, changing ship flags, and automatic identification system spoofing. These techniques demonstrate an intricate knowledge of the weaknesses of the global shipping system, and the ability of DPRK agents to exploit these weaknesses in major shipping jurisdictions – a new normal that shipping and insurance companies, and national regulations, must quickly evolve to effectively combat.

Figure A.1. The advanced evasion techniques utilized by those involved in the Yuk Tung scheme

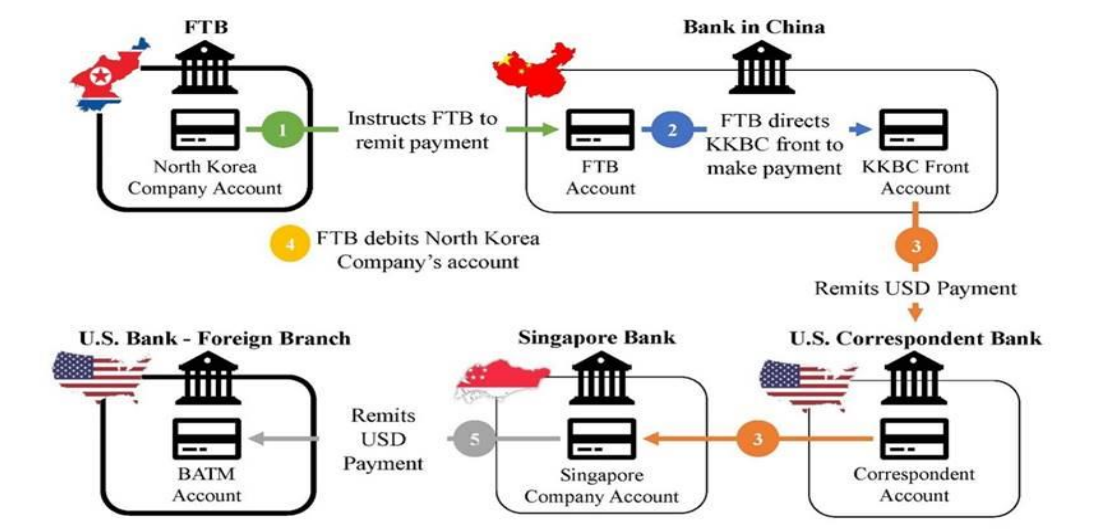


[27] 56 countries [1] involved in violating UNSC Resolutions on North Korea during last reporting period | Institute for Science and International Security (isis-online.org)

11 Annex C - British American Tobacco to Pay $629 Million in Fines for N. Korean Tobacco Sales; Charges Unsealed Against Tobacco Facilitators[28]

93. In 2023, British American Tobacco (BAT) and its subsidiary, BAT Marketing Singapore (BATMS), one of the world's largest manufacturer of tobacco products, agreed to pay penalties totalling more than $629 million to resolve bank fraud and sanctions violations charges with U.S. authorities, arising out of the companies' scheme to do business in North Korea through a third-party company in Singapore, in violation of the bank fraud statute and the International Emergency Economic Powers Act (IEEPA). In addition, charges were unsealed in the District of Columbia against a North Korean banker and Chinese facilitators for their roles in facilitating the illicit sale of tobacco products in North Korea.

94. BAT's scheme involved several critical steps to disguise the source of revenues.
    i. A BAT subsidiary ("BATMS") shipped goods, primarily cigarette components, to the joint venture ("JV"), in care of the front company ("company 1").
    ii. BATM invoiced company 1 for the goods.
    iii. Company 1 sent the invoice to an employee at the North Korean Tobacco Company ("NKTC," joint venture partner).
    iv. NKTC made payments in U.S. dollars to company 1 for the invoice amount, often using a Chinese front company to process the payment.
    v. Company 1 separately made payments to BATM in the same amount, minus a small percentage commission.



[29]

[28] District of Columbia | British American Tobacco to Pay $629 Million in Fines for N. Korean Tobacco Sales; Charges Unsealed Against Tobacco Facilitators | United States Department of Justice

[29] British American Tobacco's Financial Scheme to Avoid Sanctions Detection (Part II of II) - Corruption, Crime & Compliance

12 Annex D – Sources for PF case studies

Examples of sources for PF case studies:

94. International bodies:

i. Annual Reports by the United Nations Panel of Experts established pursuant to resolution 1874 (DPRK). https://www.un.org/sc/suborg/en/sanctions/1718/panel_experts/rep orts

ii. FATF Typologies Report on Proliferation Financing, 18 June 2008. http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf

95. Other sources:

i. Project Alpha, Centre for Science and Security Studies at King's College, London. Comprehensive database of open-source PF case studies. https://acsss.info/

ii. James Martin Center for Non-proliferation Studies, Middlebury Institute of International Studies at Monterey. Conducts research into non- proliferation and export controls. www.nonproliferation.org/

iii. 8 North, US-Korea Institute at the School of Advanced International Studies. Monitors nuclear and missile developments in DPRK through open-source materials. www.38north.org

iv. Stockholm International Peace Research Institute (SIPRI). Academic research on Dual use items and export control policies. www.sipri.org

v. Royal United Services Institute (RUSI). Centre for Financial Crime and Security Studies. Projects: CPF Technical Assistance Programme, PF Risk Assessment, Project Sandstone. https://www.rusi.org

vi. Center for a New American Security (CNAS). Proliferation reports. https://www.cnas.org/

13 Annex E – Legislative Framework

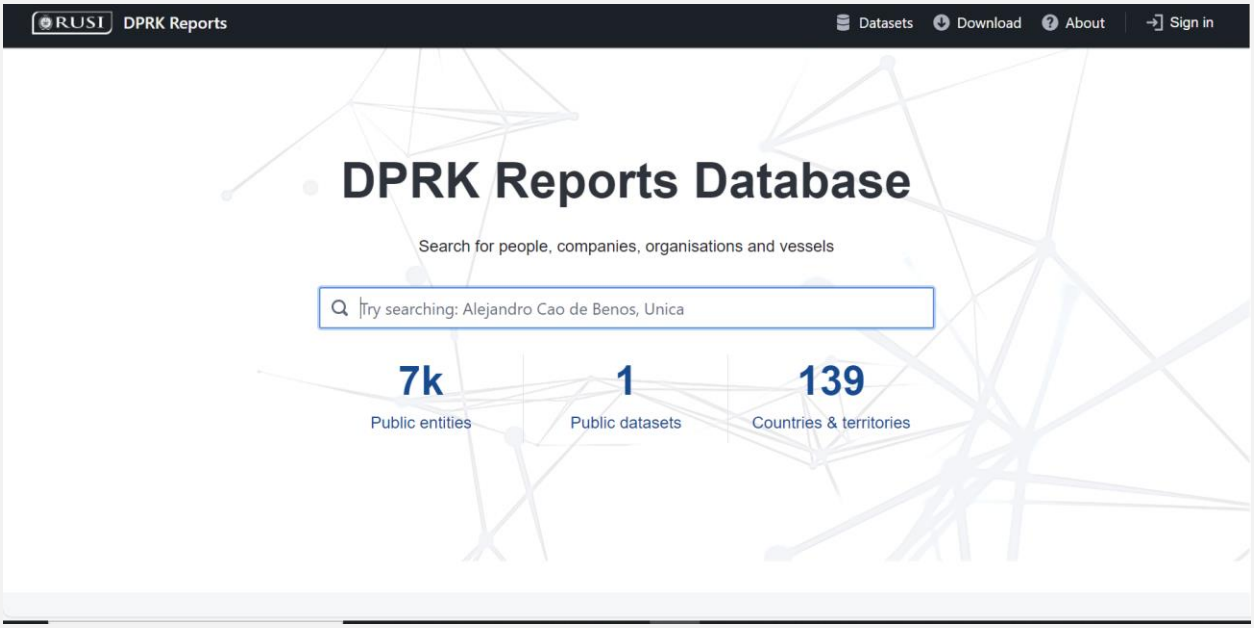
International Obligations

- United Nations Security Council Resolution 1540 (2004)
- United Nations Security Council Resolution 1718 (2006)
- United Nations Security Council 2231 (2015)
- The Democratic People's Republic of Korea (Sanctions) (Overseas Territories) Order 2020
- The Iran (Sanctions) (Overseas Territories) Order 2020

Domestic Obligations

- International Sanctions Act 2003
- International Sanctions Regulations 2013
- International Sanctions (Delegation of Governors Functions) Notice 2018
- Proceeds of Crime Act 1997
- Proceeds of Crime Regulations 1998
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Designation Order 2012
- Charities Act 2014
- Anti-Terrorism (Financial and Other Measures) Act 2004

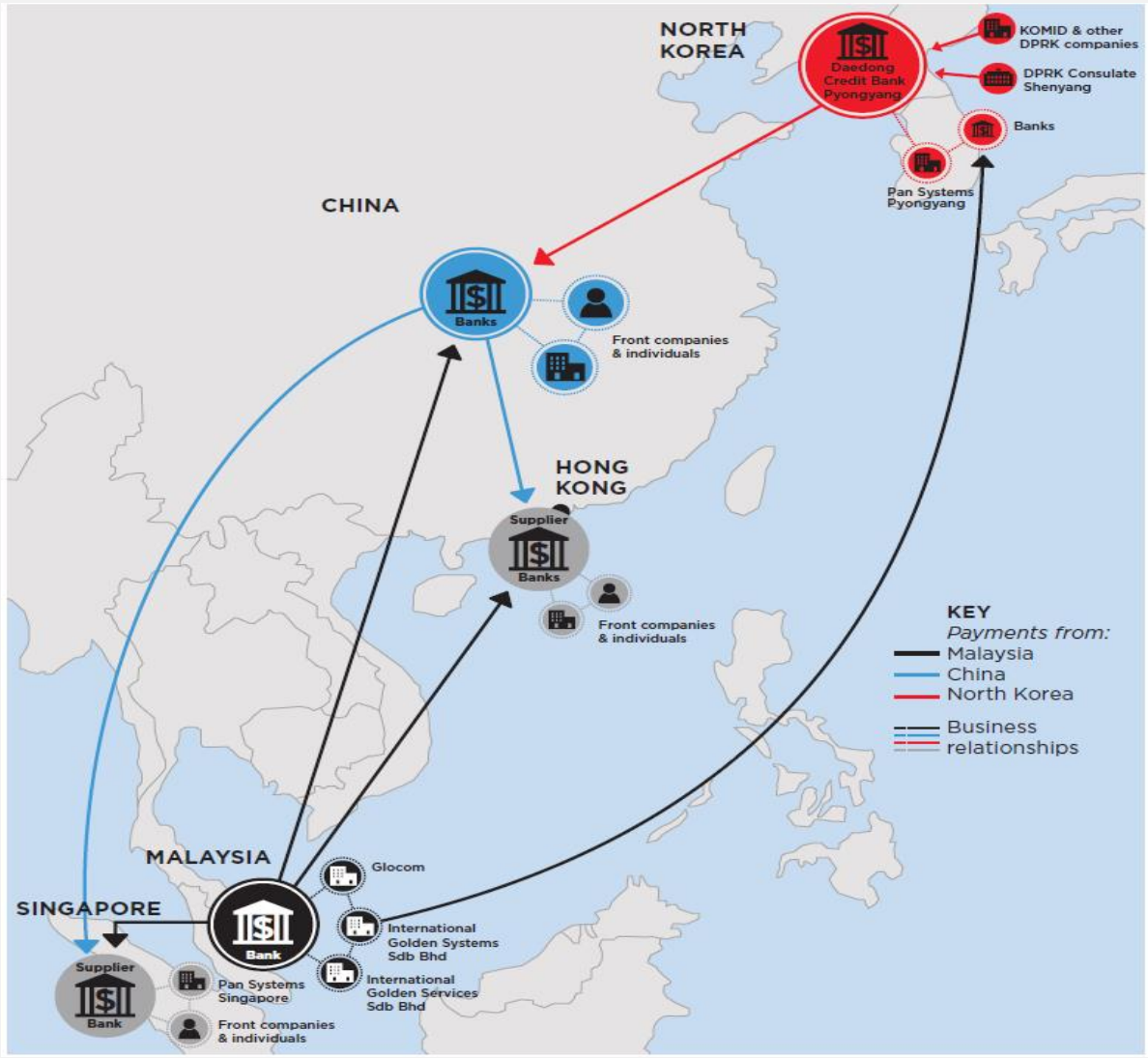
14 Annex F – RUSI's DPRK Reports Database



DPRK Reports (dprk-reports.org)

15 Annex G - North Korea's Procurement Networks[30]

A simplified illustration of North Korea's sophisticated procurement networks, based in multiple countries. In this case, Pan Systems Pyongyang and its front companies carry out financial activity in multiple jurisdictions, which benefits, among others, the Korea Mining and Development Trading Corporation (KOMID), which is widely considered to be North Korea's primary arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons. Pan Systems Pyongyang's involvement in Middle East business is referenced without details (not shown).



[30] Based on Project Alpha Report on Typologies of Financing of Proliferation, October 2017, which is based on the 2017 Final Report of the U.N. Panel of Experts on DPRK. This figure is reprinted from Jonathan Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation," (Center for a New American Security, January 2018), 9.