TARGETED FINANCIAL SANCTIONS

TYPOLOGIES OF PROLIFERATION FINANCING
- MARCH 2023 -

CONTENTS

Contents 2
Introduction 3
Scope of Typology Paper 3
Contact details 3
Proliferation Financing 4
What is Proliferation? 4
What is Proliferation Financing? 4
Difficulties in Detecting Proliferation Financing 5
Proliferation Financing – Case Studies 6
(Mis)use of the Banking Sector 6
(Mis)use of Legal Entities and Arrangements 7
Selling of Goods 8
Cyberattacks 9
PF-related Red Flags 10

INTRODUCTION

1. The Principality of Monaco (Monaco), being an international financial center, is committed to protecting its financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs) from abuse by illicit actors engaging in proliferation financing (PF) and other proliferation efforts. It is of great importance that the entire population of natural and legal persons in Monaco exercises caution and vigilance to ensure that individuals or organizations which are subject to United Nations Security Council (UNSC) proliferation-related sanctions are in no way supported.[1]

2. PF facilitates the movement and development of proliferation-sensitive goods and weapons of mass destruction (WMD) programs and has the potential to contribute to global instability and loss of life. As such, preventing PF is an important part of combatting proliferation. It is essential to disrupt the financial flows available to proliferators and to obstruct and complicate the procurement of illicit goods, services and technology needed for the development of WMD and their means of delivery.

3. This PF-related typology paper presents international cases and examples on how designated persons (natural and legal), groups, or entities have received financing and support despite being listed on United Nations Security Council Resolutions (UNSCRs). The aim of the paper is to highlight methods and trends sanctioned persons use to circumvent the restrictions imposed on them by the UNSC. Particular focus is given to UNSCRs targeting the Democratic People's Republic of Korea (UNSCR 1718 (2006)) and the Islamic Republic of Iran (UNSCR 2231 (2015)).

4. This document also includes a list of red-flag indicators that can aid FIs and DNFBPs to detect any suspicious transactions related to PF.

Scope of Typology Paper

5. This typology paper has been issued by the Advisory Committee on the Freezing of Funds and Economic Resources (the Advisory Committee) to assist reporting entities with the implementation of targeted financial sanctions (TFS)-related obligations. The information contained in this paper does not in any way whatsoever constitute legal advice, and should be read in conjunction with relevant national legislation, international standards, and guidelines issued by the Advisory Committee or other competent agencies (e.g. SICCFIN, DSP).

Contact details

6. For all enquiries, reports and requests associated with the implementation of counter proliferation financing controls and targeted financial sanctions please email the Advisory Committee on the Freezing of Funds and Economic Resources.

Email: dbt.geldefonds@gouv.mc

Website: https://geldefonds.gouv.mc/en

[1] The PF-related UNSC Resolutions are UNSCR 1718 (2006) related to the Democratic People's Republic of Korea (DPRK) and UNSCR 2231 (2015) related to the Islamic Republic of Iran, and their successor resolutions.

PROLIFERATION FINANCING

What is Proliferation?

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

8. The UN, in its UNSCR 1540 (2004), defines proliferation as the transfer and export of WMD; their means of delivery and related materials. This could include, inter alia, technology, goods, software, services or expertise. It further defines 'means of delivery' as missiles, rockets and other unmanned systems capable of delivering WMD that are specially designed for such use and 'related materials' as materials, equipment and technology covered by relevant multilateral treaties and arrangements, or included on national control lists, which could be used for the design, development, production or use of WMD and their means of delivery.

What is Proliferation Financing?

9. Following the definition above, PF is defined by the FATF as the *provision of funds or financial services* used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of WMD 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.

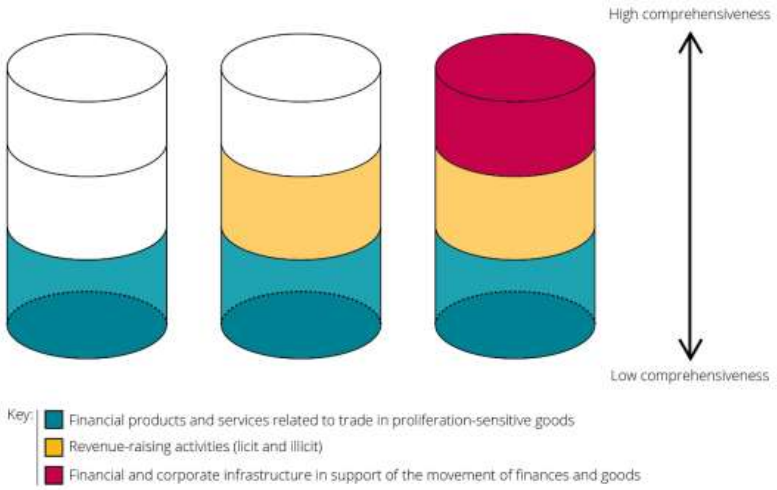
10. In other words, PF is about providing financial services to programs related to the transfer and export of WMD, their means of delivery, and related materials. It also involves the financing of trade in sensitive goods needed to support or maintain said programs, even if those goods are not related to any WMD (so called dual-use goods), for example: oil, coal, steel or military communication equipment (see Table 1, below, for more examples). Additionally, PF includes the financial support to individuals or entities engaged in proliferation, even if they perform other activities that are not related to such programs (e.g. diplomats, shipping companies, fisheries, trade in commodities companies).

Table 1. Examples of general dual-use goods

Nuclear	Chemical	Biological	Missile & Delivery
Centrifuges	Scrubbers	Fermenters	Aluminum alloys
High-speed cameras	Reactors	Spray dryers	Oxidants
Composites	Coolers	Tanks	Machine tools
Maraging steel	Elevators	Mills	Isostatic presses
Vacuum pumps	Heat exchanges	Bacterial strains	Composites
Pressure gauges	Mixing vessels	Filters	Gyroscopes

11. With PF being a mix of 1) the payment and financial services in direct support of the procurement of goods and development of WMD, 2) the raising of funds and revenue-generating activities to fund proliferation efforts, and 3) the financial and corporate networks and services that sustain these activities, the Royal United Services Institute[2] suggests thinking of PF as three categories of activities that should be considered as part of counter-proliferation financing (CPF) efforts.

[2] 'Guide to Conducting a National Proliferation Financing Risk Assessment', Royal United Services Institute, 2019



12. Designees under UNSCRs related to PF are prone to using complex networks of front companies and diversion techniques that mimic money laundering typologies to circumvent CPF sanctions measures and gain access to the global financial system. Nonetheless, there are distinct differences between money laundering and sanctions evasion, with the former being a circular process deployed by criminals to conceal the illicit origin of the proceeds of crime and the latter being about the individuals to whom funds are made available (designees) or the purposes for which they are being used (proliferation).

13. Due to their differences, FIs and DNFBPs should consider PF as a separate type of financial crime that also requires a different type of sanctions compliance. The next section will shed light on real-life cases of PF that occurred in different sectors, with the goal to increase awareness about these sanctions and the importance of their implementation.

Difficulties in Detecting Proliferation Financing

14. There are a number of difficulties associated with identifying proliferation financing:

- A growing trend in the purchase and sale of elementary components, as opposed to whole manufactured systems. The individual elementary components may also have legitimate uses (dual-use goods), making their identification for illegitimate purposes even more problematic.
- Dual-use goods are difficult to identify, requiring specialist knowledge and can be described in common terms with many uses such as 'pumps'.
- Networks through which proliferation-sensitive goods may be obtained tend to be complex. This, combined with the use of false documentation, allows 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 are often used to cover up the ultimate end-user.
- Risk of proliferation financing is more likely to be present in cases where the source of funds is legal and the end-user of a type of goods involved is obscured, making identification of such activities difficult.

15. Ultimately, as an FI or a DNFBP, it is of utmost important to properly understand the PF risk you are exposed to to be able to decide what measures to take to mitigate them. The above-listed trade-related indicators can aid in the identification and classification of potential threats and vulnerabilities. Each FI and DNFBP should have its own policy regarding risk assessments. In addition, PF should be included as a specific financial crime risk when providing training or conducting exercises to enhance staff awareness.

16. As stated above, identifying PF is difficult because most transactions occur within normal business transaction pathways, and can be masked with all legitimate transactions. Depending on the business model one could incorporate the trade-related indicators into Know Your Customer (KYC) procedures, transaction screening procedures, transaction monitoring systems and suspicious activity investigations, regulatory reporting procedures, and due diligence connected to trade finance operations.

PROLIFERATION FINANCING – CASE STUDIES

17. The following section will shed light on real-life cases of PF that occurred in different sectors, with the goal to increase awareness about these sanctions and the importance of their implementation.

(Mis)use of the Banking Sector

Case Study 1: Access to a legitimate business bank account[3]

18. In July 2013, Panama Cana authorities detained a North Korean vessel, the Chong Chon Gang (CCG), while it was transiting from Cuba to North Korea. Canal authorities found a shipment of arms and related materials concealed under other cargo. The CCG was operated and managed by Ocean Maritime Management Company Ltd (OMM), one of the largest North Korean shipping companies. Costs connected with the voyage of the CCG were paid by Chinpo Shipping Company (Private) Limited, based in Singapore.

19. The North Korean Embassy in Singapore used the business as a postal address. Chinpo hosted OMM staff at its offices and used its bank account to manage funds on behalf of OMM. Monies due to OMM (for example, freight charges) were paid into the account. Monies were remitted from the account at OMM's request, for example to North Korean vessel owners (who were not able to set up their own bank accounts because of sanctions), or on their behalf for supplies, port charges or other disbursements, or from one North Korean ship owner to another. Over three years, 605 remittances took place, totaling more than $40 million, all related to North Korean vessels. Chinpo was effectively operating as a remittance business, although it had no license to do so from Singapore authorities. Once a year, a North Korean diplomat with access to the Chinpo account would withdraw up to $500,000 in bank notes to carry out of the country. Chinpo tried to hide its involvement with North Korean companies by removing the names of North Korean vessels and other identifying details from remittance forms and email correspondence, and payments from Chinpo's account took place in the absence of invoices or other details.

Case Study 2: Maintaining representative offices and agents abroad

20. In February 2017 information was obtained by the UN Panel of Experts showing that two sanctioned banks, Daedong Credit Bank (DCB) and Korea Daesong Bank (KDB), were both operating on Chinese territory, through representative offices in Dalian, Dandong and Shenyang. A director of these offices simultaneously served as a director of a designated company, DCB Finance Ltd., registered in the British Virgin Islands. DCB Finance shared several officers with DCB, and when the DCB correspondent accounts were closed in 2005, DCB Finance was set up to undertake wire transfers and business transactions on its behalf .

21. The representative in Dalian of DCB and DCB Finance undertook transactions in US Dollars, with single transactions occasionally exceeding the $1 million mark. He also facilitated payments and loans between companies linked to DCB and exchanged large quantities of bulk cash transferred to China from the DPRK into US Dollar notes of higher denomination. Additionally, the representative also undertook foreign exchanges between US Dollars and Euros, transferring balances between DCB and its shareholder (mainly Korea Daesong Bank). When DCB established representative offices in Shenyang in late 2012, and Dandong in 2014, the three offices cooperated in managing the activities of foreign exchanges, transfers, bulk cash exchanges and loans.

Case Study 3: Buying dual-use goods through financial transactions[4]

22. A broker was involved who was an Iranian and EU national, with a residence in an EU member state and a bank account in the EU member state. The broker was registered in the British Virgin Islands (BVI) and operated through a front company. This front company could be linked by the Authorities to at least one Iranian company. The front company held an account at a domestic bank in Dubai and also had a bank account in a Balkan state, an EU member.

23. An Iranian bank was the source of funds. Payment was initiated by a branch of this bank in Dubai in the form of a wire transfer to the account of the front company in Dubai. Funds were transferred from this account to suppliers in Luxembourg and also to private persons in several EU member states.

[3] 'Countering Proliferation Finance: An Introductory Guide for Financial Institutions', Royal United Services Institute, 2017
[4] 'Study of Typologies of Financing of WMD Proliferation: Final Report', Jonathan Brewer, 2017

24. Investigators found no evidence that dual-use goods were involved in any of the financial transactions, but they suspected that the mechanism could be used for proliferation finance.

25. Iranian customers holding bank accounts in Luxembourg also wired money to the European account of the BVI-based broker. The channels were used more than once in some cases (when European suppliers were involved) and sometimes only once (when private persons were involved).

(Mis)use of Legal Entities and Arrangements

Case Study 1: Purchasing goods through 3rd parties

26. The United Arab Emirates' (UAE') Financial Intelligence Unit (FIU) received a suspicious transaction report from a bank in which Person X owned two companies, one of which was suspected of purchasing aircraft equipment from companies in another country. The equipment was shipped to a company based in the UAE that worked on behalf of an entity listed on the OFAC list that might support the Iranian nuclear program.

27. The UAE authorities confirmed that Person X and his companies had a business relationship with a listed entity, and the company was used to cover the ultimate beneficiary of the purchased equipment to avoid sanctions. Following this finding, a freezing order was issued on Person X's personal and corporate bank accounts.

28. The UAE Prosecution confirmed that it had reasonable grounds to suspect a sanctions breach based on the investigation reports, and ordered an arrest of Person X and the freezing of funds and other assets worth AED 4,800,000 (roughly € 1,200,000).

Case Study 2: Establishing joint ventures to generate revenue

29. An investigation into Korea General Corporation for External Construction (GENCO/KOGEN) by the UN Panel of Experts that showed that the company had a large reach and extensive network in several countries in the Middle East, Africa and Eurasia, where it utilized workers, prohibited cooperative entities and joint ventures of the DPRK to earn significant revenue. One country claimed that GENCO/KOGEN "has worked to supply North Korean laborers in the Middle East for the purpose of earning hard currency for North Korea". Evidence suggested that a joint venture between GENCO/KOGEN and a UAE company supported the company's activities.

30. Corporate registration documents showed that GENCO/KOGEN was the partial owner of a construction cooperative entity/joint venture company in Russia, with majority ownership belonging to a Russian national. This legal entity maintained an account with a Russian bank. Furthermore, the Russian company was found to have the same addresses, contact information and shareholders as three other companies, all of which engaged in construction-related activities. In addition, corporate registry documents showed that GENCO/KOGEN operated two official representative offices in Russian that together formally employed 17 DPRK nationals.

31. In addition to the Russian presence, GENCO/KOGEN was present in Nigeria, the Ivory Coast and Equatorial Guinea. In Nigeria, it was registered as "Korea General Company for External Construction GENCO (Nigeria)" and in the Ivory Coast as "Korea General Construction SL (KOGEN GE SL)". Furthermore, the African Union Inter-African Bureau for Animal Resources listed KOGEN GE S.L. on its website, stating that the company was an implementing partner for a project funded by Equatorial Guinea. GENCO/KOGEN was separately reported as a contractor for the Rebola Municipal Stadium, where earnings estimates were approximately US$ 30,500,000.

Case Study 3: Issuing unauthorized insurances

32. DGS Marine was a Liechtenstein-registered offshore business company located at a fiduciary's office in Vaduz until mid-2012. Media reports surfaced, where DGS's director, David Skinner, had issued insurance certificates for Iranian owned oil tankers transporting oil from Syria allegedly in contravention of European Union sanctions. Following the reports, the Liechtenstein Financial Authority issued a warning notice stating that DGS Marine was not licensed to issue insurances in Liechtenstein. Following the warning notice, the director registered DGS Marine as a British Virgin Island (BVI) business company one month later, though the UN Panel of Experts was also able to confirm shortly after that DGS Marine was not licensed or authorized to issue insurances in the BVI either.

33. Prior to 2012, the company's annual report were found to contain false information regarding the identity of DSG's independent auditor, calling into question the certification of DGS Marine's annual financial statements. DGS Marine did

not respond to the UN Panel of Experts' inquiries. Following the investigation, media reports indicated that DGS Marine was an elaborate insurance scam that, while maintaining offices in the United Kingdom, Cyprus, Denmark, Vietnam, India, China, and the UAE, did not possess the millions of pounds in securities alleged in its annual reports.

Selling of Goods

Case Study 1: Ship-to-Ship transfers

34. Ship-to-Ship transfers have become a frequent means of sanctions evasion, with frequency and value seeing unprecedented increases since 2018. The UN Panel of Experts' investigation of petroleum transfers showcased a very sophisticated example of DPRK-related vessel identity fraud, highlighting new sanction evasion techniques that defeated the due diligence efforts of the region's leading commodity trader, as well as the United States and Singaporean banks that facilitated the fuel payments and a leading United Kingdom insurer that provided protection and indemnity cover to one of the vessels involved. The same case underlines the extremely poor reporting, oversight, monitoring, and control over the vessels exercised by the flag-of-convenience States under whose jurisdiction they apparently sail and also the lack of implementation of freezing sanctions.

35. In 2018, four ships were found to be in violation of UNSCR 2375 (2017), with their activities being primarily based in Taiwan Province of China, while their companies being registered in multiple jurisdictions, including the BVI, Hong Kong, the Marshall Islands, Samoa and Seychelles, and ships flagged in the Dominican Republic, Hong Kong, Panama and Sierra Leone.

36. Two of the four tankers (Hong Kong-flagged Lighthouse Winmore and the Panama-flagged Billions No. 18) transferred marine diesel to DPRK-flagged tankers. Sailing from South Korea, the tankers switched off their Automatic Identification System a few days before and after the transfers occurred. Further suspicion arose when both tankers returned to the port of departure, as opposed to sailing to the intended port of arrival which was in Taiwan. The Republic of Korea detained the Lighthouse Winmore for investigation on 24 November 2017.

37. Investigations into the Lighthouse Winmore highlighted that the tanker was chartered shortly before the ship-to-ship transfer by Oceanic Enterprise Ltd, a Marshall Islands company, via a Singapore-based broker. The company's sole director and shareholder was Shih-Hsien Chen, a national of Taiwan.

38. Two of Mr. Chen's tankers, the Lighthouse Winmore and the Golden Rich, were found to be utilizing the same document of compliance holder and international safety management manager. The bills of lading for the petroleum products embarked by both the Lighthouse Winmore and the Billions No. 18 prior to the transfer show the multinational company, Trafigura Pte. Ltd, as the shipper, Global Commodities Consultants Ltd. as the consignee and the port of Taichung as the destination. Global Commodities is registered in Hong Kong, but the registered address matches that of the Singaporean company, Global SGP Pte Ltd. Both companies share the same director and sole shareholder.

39. Oceanic Enterprise prepaid Global SGP Pte Ltd. for the two shipments delivered to the vessels (totalling about US$ 13,000,000) through bank transfers to the supplier, with which it had a contract. In addition to these two transfers by the Billions No. 18 and the Lighthouse Winmore, Oceanic had planned another nine shipments with an estimated value of about US$65,000,000.

Case Study 2: Selling dual-use goods

40. In collaboration with the UAE, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) designated 11 entities and individuals involved in procurement on behalf of Iran's ballistic missile program. OFAC sanctioned Mabrooka Trading Co LLC (Mabrooka Trading) – based in the UAE – and a UAE-based network involved in procuring goods for Iran's ballistic missile program.

41. Said network obscured the end user of sensitive goods for missile proliferation by using front companies in third countries to deceive foreign suppliers. It had also designated five Iranian individuals who have worked to procure ballistic missile components for Iran. Hossein Pournaghshband and his company, Mabrooka Trading, were providing or attempting to provide financial, material, technological, or other support to Navid Composite Material Company (Navid Composite), an entity also sanctioned by the US in connection with Iran's ballistic missile program.

42. At the time of its designation, Navid Composite was contracting with Asia-based entities to procure a carbon fiber production line in order to produce carbon fiber suitable for use in ballistic missile components. Since at least early 2015, Pournaghshband used Mabrooka Trading to procure materials and other equipment for Navid Composite's carbon fiber production plan. Pournaghshband is also designated for having provided or attempting to provide financial, material, technological, or other support to Mabrooka Trading.

Cyberattacks

Case Study 1: Attack on cryptocurrency exchange bureaus

43. Cyber actors from the DPRK shifted focus to targeting cryptocurrency exchanges in 2019. Some cryptocurrency exchanges have reported multiple attacks, in particular those registered in South Korea. Bithumb was reportedly attacked by DPRK cyber actors at least four times. The first two attacks, in February and July 2017, resulted in losses of approximately US$ 7,000,000 each, with subsequent attacks in June 2018 and March 2019 resulting in the loss of US$ 51,000,000. Similarly, Youbit (formerly Yapizon) suffered multiple attacks involving a $4.8 million loss in April 2017 and then 17 per cent of its overall assets in December 2017, forcing the exchange to close.

Case Study 2: Attack on financial institutions

44. Investigations found evidence supporting DPRK-led cyberattacks stealing funds from FIs in different countries, allowing the DPRK to evade financial sanctions and generate income in ways that are harder to trace and subject to less government oversight and regulation. During 2019, there were investigations of at least 35 reported instances of DPRK actors being involved in attacking financial institutions with the goal of obtaining foreign currency from, among others, Malta, Kuwait, South Africa, Vietnam, Poland, Slovenia, and Chile.

45. According to the UN Panel of Expert, such targeted attacks have significantly increased in their scope and sophistication, with estimates of illegally acquired funds by the DPRK reaching up to US$ 2,000,000,000.

PF-RELATED RED FLAGS

46. The following list provides a non-exhaustive list of potential red flag indicators for PF that can aid FIs and DNFBPs to detect any suspicious transactions related to PF[5]:

- Transaction involves person or entity in foreign country of proliferation concern.
- Transaction involves person or entity in foreign country of diversion concern.
- The customer or counterparty or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.
- A freight-forwarding firm is listed as the product's final destination.
- Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
- Transaction involves possible shell companies (e.g., companies do not have a high level of capitalization or displays other shell company indicators).
- Transaction demonstrates links between representatives of companies exchanging goods i.e., same owners or management.
- Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
- Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g., does the country involved normally export/import the good(s) involved).
- Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
- Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
- Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
- Involvement of items controlled under WMD export control regimes or national control regimes.
- Involvement of a person connected with a country of proliferation concern (e.g., a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.
- Customers or counterparties to transactions are linked (e.g., they share a common physical address, IP address or telephone number, or their activities may be coordinated).
- Involvement of a university in a country of proliferation concern.
- Description of goods on trade or financial documentation is nonspecific, innocuous or misleading.
- Evidence that documents or other representations (e.g., relating to shipping, customs, or payment) are fake or fraudulent.
- Use of personal account to purchase industrial items.

[5] '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 Report on Proliferation Financing', FATF, 2018