FATF

FATF Report

Complex Proliferation Financing and Sanctions Evasion Schemes

June 2025

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2025), *Complex Proliferation Financing and Sanctions Evasion Schemes,* FATF, Paris, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/complex-proliferation-financing-sanctions-evasion-schemes.html

Photocredit coverphoto: Sergey Nivens/Shutterstock.com

Abbreviations and Acronyms

AML/CFT Anti-Money Laundering/Countering the Financing of Terrorism
AECs Anonymity Enhancing Cryptocurrencies
AIS Automated Identification System
APT38 Advanced Persistent Threat 38
UBOI Ultimate Beneficial Ownership Information
CBDC Central Bank Digital Currency
CDD Customer Due Diligence
CPF Counter Proliferation Financing
CVC Convertible Virtual Currency
DeFi Decentralised Finance
DNFBP Designated Non-financial Business and Profession
DPRK Democratic People's Republic of Korea
EDD Enhanced Due Diligence
FIs Financial Institutions
FTB Foreign Trade Bank
FTZs Free Trade Zones
GECC Global Export Control Coalition
IMO International Maritime Organisation
INR Interpretive Note to Recommendation
IRGC Islamic Revolutionary Guard Corps
ML/TF Money Laundering/Terrorist Financing
MVTS Money or Value Transfer Service
NRA National Risk Assessment
OTC Over-the-counter
PF Proliferation Financing
PoE Panel of Experts
P2P Peer to Peer
PPPs Public-private partnerships
RGB Reconnaissance General Bureau
SARs/STRs Suspicious Activity/Transaction Report
SRB Self-Regulatory Body
TCSP Trust and Company Service Provider
TFS Targeted Financial Sanctions

UN United Nations

UNSC United Nations Security Council

UNSCR United Nations Security Council Resolution

VASP Virtual Asset Service Provider

WMD Weapons of Mass Destruction

1. Executive Summary

The proliferation of weapons of mass destruction (WMD) and related financing represents a significant threat to global security and the integrity of the international financial system. If technical compliance and effectiveness are not bolstered by the public and private sectors, sophisticated state and non-state actors will continue to take advantage of weaknesses in Counter Proliferation Financing (CPF) controls. The potentially catastrophic impact of WMD makes it vital to prevent and combat financing of this illicit activity.

Complex proliferation financing (PF) and sanctions evasion schemes are major threats to the international financial system. Consistent with the FATF mandate, this report highlights relevant methods and trends and supports national, regional, and global threat and risk assessments. The study details the techniques used by those evading the PF-related targeted financial sanctions (TFS) detailed in Recommendation 7, which is required by the FATF Standards, as well as techniques to evade other sanctions regimes (such as national and supranational sanctions) that are not covered under Recommendation 7 of the FATF Standards.

This comprehensive approach aims to provide an up-to-date understanding of threats and vulnerabilities, including the common challenges between relevant typologies. The study also strives to identify notable enforcement challenges and good practices, which helps to inform countries' PF risk assessments and risk mitigation processes. The broader framing of sanctions evasion is not intended to redefine the requirements of Recommendation 7, and it does not entail and/or promote the endorsement of national or supranational sanctions regimes.[1]

The FATF assesses that evolving **threats and vulnerabilities** relevant to PF and sanctions evasion represent enormous challenges for the public and private sectors. The current risk environment is characterized by state- and non-state actors acquiring and/or sourcing dual-use goods, technology, and knowledge through the use of procurement networks. Based on the current global PF threat, the FATF Global Network recognised the Democratic People's Republic of Korea (DPRK) as the most significant actor. The DPRK is subject to UN sanctions and the FATF Standards.

While there is no universally agreed upon estimate of the total funds generated or moved to support PF, the DPRK diversified its efforts to access the financial system and raise revenue for its WMD programme in recent years. For example, the DPRK generated billions of dollars through cyberattacks on virtual asset-related companies, such as the theft of $1.5 billion from ByBit in February 2025. Also, the DPRK is generating revenue through IT workers, a variety of other sectors, and illicit activity to benefit its WMD programme.

Many countries also identified relevant examples of sanctions evasion schemes involving Iran and the Russian Federation, which are not subject to UN proliferation-related sanctions or covered under the FATF's definition of PF risk. Given varying levels of risk understanding, threat actors are successfully exploiting national- and sectoral-level vulnerabilities to evade sanctions relevant to PF (see Section I).

1 The broader framing of sanctions evasion does not create any new obligations related to Recommendation 1 or any other part of the FATF Standards. Instead, FATF typologies reports aim to support the public and private sector to assess and mitigate risk based on their unique context.

Illicit actors are employing sophisticated schemes to evade sanctions and circumvent export controls relevant to PF. Based on the information submitted by the FATF Global Network, this report spotlights **four major typologies**: enlisting intermediaries to evade sanctions; obscuring beneficial ownership information (BOI) to access the financial system; using virtual assets and other technologies; and exploiting the maritime and shipping sectors (see Section II). To address complex PF and sanctions evasion schemes, the report profiles **challenges and good practices** for: detecting PF and sanctions evasion; investigation and prosecution; domestic coordination and collaboration; and international cooperation (see Section III).

This study contributes to the FATF Global Network's understanding of complex PF and sanctions evasion schemes, including through relevant **risk indicators** for competent authorities and the private sector (see Annex A: Risk Indicators). However, this study also shows the need to further improve the FATF Global Network's collective understanding of risk related to PF and sanctions evasion. In the coming years, threat actors will continue to probe for weaknesses in CPF controls, such as jurisdictional differences in the approach to PF and sanctions evasion and exploit new technologies and shifts in the geopolitical landscape.

To prevent and combat complex PF and sanctions evasion schemes, the FATF Global Network should consider (see Recommendations section):

1) **Updating the understanding of threats, vulnerabilities, and typologies on a periodic basis**, since the public and private sectors are at varying stages of understanding relevant risks;
2) **Encouraging more substantive information sharing to strengthen the public and private sector's ability to detect PF and/or sanctions evasion**, given the reliance on SARs/STRs to initiate relevant investigations;
3) **Adding an official definition for WMD PF** to the FATF General Glossary, within five years, to overcome jurisdictional differences that undermine international cooperation; and
4) **Conducting a horizontal review of the FATF Global Network's PF risk assessments**, within three years, to help identify good practices after countries have had more time to assess PF risk.

2. Background

Overview of FATF Standards and Work on PF

1. In October 2020, the FATF adopted amendments to Recommendations 1 and 2 (R.1 and R.2) and their Interpretive Notes (INR.1 and INR.2) to require countries, financial institutions, designated non-financial businesses and professions (DNFBPs) and virtual asset service providers (VASPs) to identify, assess, and understand their proliferation financing risks i.e., the risk of potential breaches, non-implementation or evasion of the targeted financial sanctions (TFS) detailed in R.7, and to take effective mitigation measures which are commensurate with the identified risks. The revised Recommendations also mandate countries to enhance national cooperation and coordination, and information sharing mechanisms related to PF risks.

2. To assist public and private sector stakeholders to effectively implement obligations under the revised Recommendations, the FATF published the Guidance on Proliferation Financing Risk Assessment and Mitigation in 2021[2] which provides guidance on:

1) how public and private sectors should conduct risk assessments to identify, assess, and understand PF risks;
2) how to implement the FATF requirements to mitigate identified PF risks;
3) how supervisors or self-regulatory bodies should supervise and monitor FIs, DNFBPs, and VASPs to ensure they properly assess and mitigate PF risks.

3. The 2021 Guidance complements the 2018 Guidance on Counter Proliferation Financing[3] which primarily aims to facilitate both public and private sector stakeholders in understanding and implementing the obligations under R.7 pursuant to the UNSCRs as well as preventing sanctions evasion. This is preceded by the 2013 Guidance on the Implementation of Financial Provisions of UNSCRs to Counter Proliferation of Weapons of Mass Destruction[4].

4. Prior to these guidance documents, the FATF identified and analysed the existing PF risks and CPF measures and published the findings in the 2008 PF Typologies Report[5] to further global understanding of these developments. The 2010 Combatting Proliferation Financing: A Status Report on Policy Development and Consultation[6] builds on the 2008 report by setting out policy options to be considered in implementing CPF measures pursuant to the UNSCRs, particularly regarding i) legal systems, ii) information sharing and awareness-raising between the public and private sectors, iii) preventive measures, and iv) investigation and prosecution.

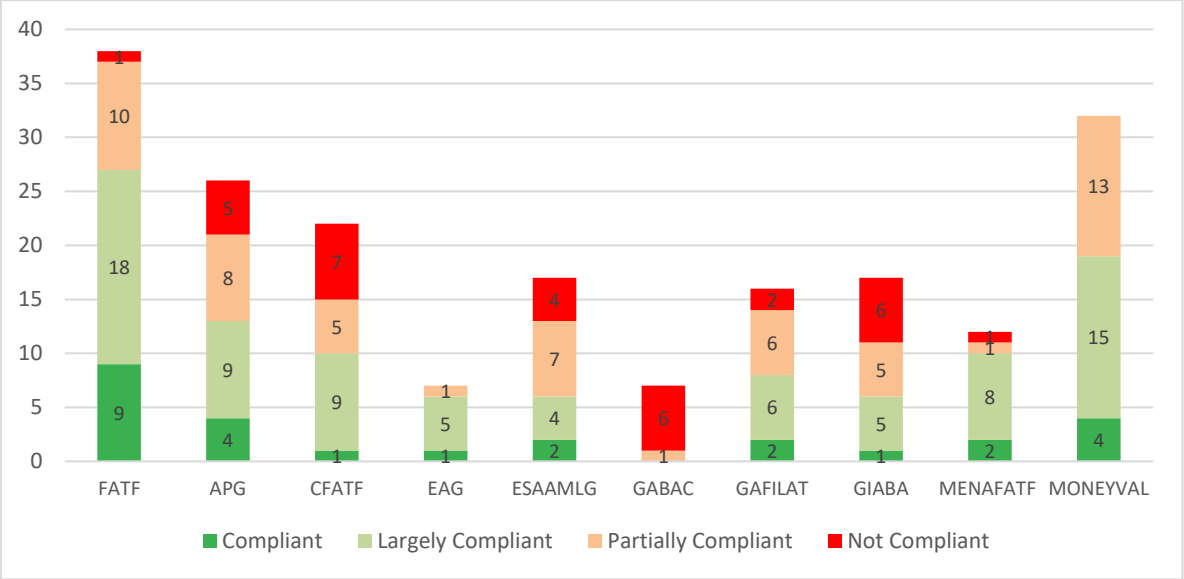
Current Implementation Status of the FATF Standards

5. The assessment results of the 4th round of Mutual Evaluation (ME) indicate that countries continue to struggle with R.7 and implementing and enforcing TFS in compliance with the UNSCRs on proliferation. As of April 2025[7], out of 194 FATF and FSRB members

2 FATF (2021) Guidance on Proliferation Financing Risk Assessment and Mitigation.
3 FATF (2018) Guidance on Counter Proliferation Financing
4 FATF (2013) Guidance on the Implementation of Financial Provisions of UNSCRs to Counter Proliferation of Weapons of Mass Destruction
5 FATF (2008) Proliferation Financing Typologies Report
6 FATF (2010) Combatting Proliferation Financing: A Status Report on Policy Development and Consultation
7 FATF (2024) Consolidated Assessment Ratings

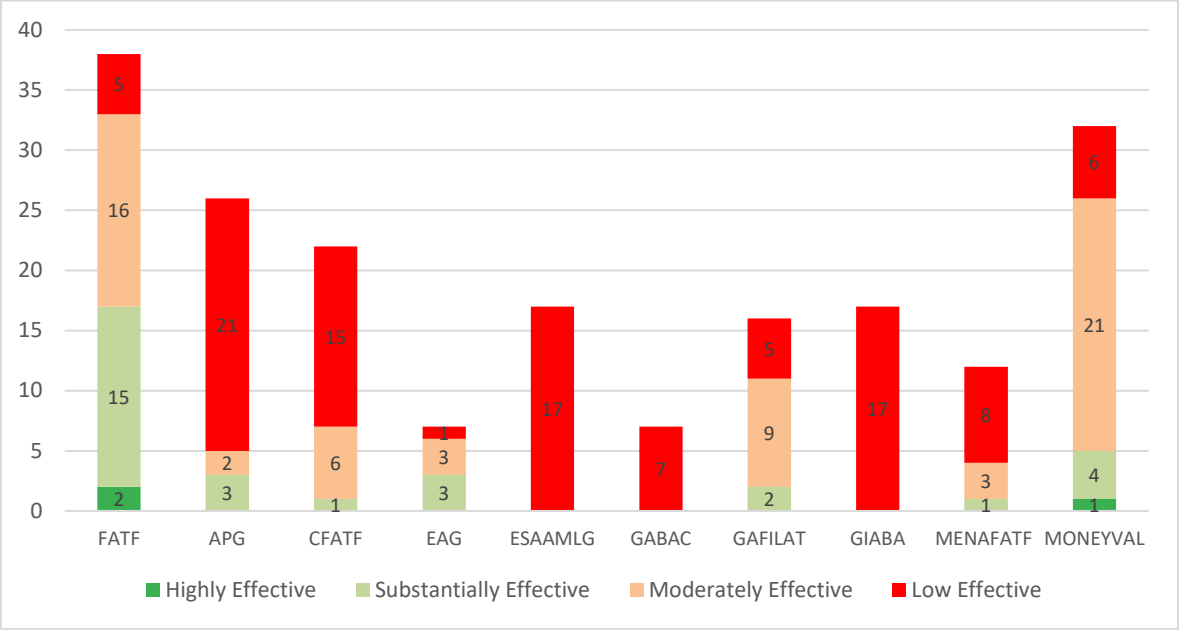
assessed during the 4th round of ME, only 13% (26 countries) are compliant with R.7 and nearly half (46%; 89 countries) are partially or not compliant.

Figure 1. Assessment Results: Technical Compliance with R.7 (as of April 2025)



6. Similarly, overall effectiveness remains low, with only 16% of assessed countries having demonstrated high/substantial effectiveness in IO.11 (TFS pursuant to the UNSCRs on proliferation). The effectiveness performance varies significantly across FATF and FSRB members (45% of 38 FATF members and 10% of 156 FSRB members assessed have obtained highly/substantially effective ratings).

Figure 2. Assessment Results: Immediate Outcome 11 – Effectiveness (as of April 2025)



Introduction

Overview of Focus

7. This report aims to build upon and update the two existing guidance reports 1) 2018 FATF Guidance on Counter Proliferation Financing – The implementation of Financial Provisions of the UNSCR 1718 to Counter PFWMD and 2) the 2021 Guidance on Proliferation Financing Risk Assessment and Mitigation. The study provides readers with a comprehensive understanding of current typologies in complex sanctions evasion schemes relevant to PF, and it identifies enforcement challenges and best practices, which help to inform countries' PF risk assessment and risk mitigation. The report uses the following key terms:

Box 1. Definitions of Key Terms

The report uses the broad working definitions used in the 2021 PF Guidance, which builds upon the 2010 Status Report:

Weapons of Mass Destruction (WMD) Proliferation

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 dual-use technologies and dual-use goods used for non-legitimate purposes).

Proliferation Financing (PF)

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 and related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes).[8]

The report reiterates that there is no standard, universal definition of WMD proliferation or PF shared by the relevant international regimes and fora and notes the potential implications and need for a standard definition in relevant sections.

PF risks

Except where noted otherwise, in line with the revised Recommendation 1 and its Interpretative Note (R.1 and INR.1), the report refers to PF risk strictly and only as the potential breach, non-implementation, or evasion of the TFS obligations referred to in Recommendation 7.

8. Building on the wide body of work from various national and international institutions, the report is designed to be used by the FATF Global Network members,

8 This working definition of PF builds upon the definition from the FATF's 2010 Status Report, which remains relevant for this study, especially for countries that take a broader approach to mitigating risks relevant to PF and sanctions evasion. The 2010 report defines PF as "the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations."

competent authorities, FIs, DNFBPs, VASPs, non-government organisations, and any other individuals or bodies in tackling sanctions evasions relevant to PF.

Objectives and Structure

9. This report is designed to provide a global view of trends and methods in sanctions evasions relevant to PF, with an aim of assisting countries in mitigating PF risks. The report provides indicators of complex sanctions evasion schemes, threats and vulnerabilities, and identifies good practices and challenges in detecting, investigating, and prosecuting cases of sanctions evasion relevant to PF. These objectives are delivered through four key parts:

- **Section One**: Sets out the project scope in line with the implementation plan. It also provides an overview of the current situation and identifies threats and vulnerabilities relevant to sanctions evasion and PF on the basis of case studies and literature analysis.
- **Section Two**: Provides an overview of typologies in complex sanctions evasion schemes relevant to PF.
- **Section Three**: Identifies challenges and good practices in detecting, reporting, investigating, and prosecuting linked to PF. It also outlines various mechanisms in domestic co-ordination and collaboration, and international cooperation relevant to the topic.
- **Conclusion and Priority Areas:** Summarises the overarching PF and sanctions evasion landscape and identifies areas where further work is needed.
- **Risk Indicators**: This annex is designed to enhance the ability of public and private sector entities to identify suspicious transactions and/or activity associated with relevant PF and sanctions evasion schemes.

Methodology

10. The methodology comprised a review and refinement of existing available materials on PF and PF risks, which included:

- A literature review to identify evolving trends in the nature and scope of sanctions evasions relevant to PF, including from recent UNSCR 1718 Panel of Experts (POE) reports. This review focused on threats, vulnerabilities, as well as emerging trends and methods.
- A request to the FATF Global Network members to provide inputs on sanctions evasion relevant to PF. This included a) material on strategic intelligence products or case studies that provided information on typologies and instances of sanctions evasion relevant to PF, b) threats and vulnerabilities identified in risk assessments and mitigation measures, c) detection, investigation, and information sharing mechanisms, and d) good practices and challenges.
- In addition to the risk indicators submitted by the FATF Global Network members, the following supplementary reports were also examined: i) PF risk assessment guidance by other organisations and institutions, ii) studies on PF typologies, and iii) TFS guidance published by countries.

- The private sector, civil society, and academia were encouraged to answer several questions in a public consultation to inform the report, especially related to challenges and good practices in domestic coordination and collaboration.

3. Section 1. Evasion of Sanctions Relevant to PF – Current Situation, Threats and Vulnerabilities

Scope

Framing the Report

11. As part of the risk assessment process, countries consider money laundering (ML), terrorist financing (TF), and PF risks that occur when a relevant threat successfully takes advantage of a vulnerability to produce a consequence.[9] According to the FATF Global Network, the most significant PF threat to the international financial system is posed by state-sponsored or -affiliated actors, including but not limited to those associated with sanctions evasion and PF activities related to the DPRK, the sole UN-sanctioned country.

12. In the framework of the revised FATF Recommendation 1, PF risk refers strictly and only to the potential breach, non-implementation, or evasion of the TFS obligations referred to in Recommendation 7, which focuses solely on that UN-sanctioned country, the DPRK. Based on this narrow definition of PF risk covered by the FATF Standards, the main threat actors identified by jurisdictions include the DPRK and the state actors, individuals, and entities supporting or working with the DPRK to evade UN sanctions.

13. As described in the FATF's 2021 PF Guidance[10], an understanding of the broader risk of WMD proliferation and its underlying financing may contribute to the understanding of risk related to the FATF's PF-TFS obligations. An enhanced understanding of PF risk can also assist in the implementation of risk-based measures and TFS. Many FATF members use a broader definition of PF to mitigate risk more broadly than the current FATF Standards. Consequently, the scope of jurisdictions' submissions reflected their understanding of the current global PF threat, including the DPRK (subject to UN sanctions and the FATF Standards), but also other state actors. Many countries identified Iran and the Russian Federation as current PF threats even though they are not subject to UN proliferation-related sanctions or covered under the FATF's definition of PF risk.

14. The scope of this report is to provide a current view of the complex sanctions evasion schemes being used by proliferation financiers and where relevant it also considers sanctions evasion schemes related to TF and PF more broadly regardless of the sanctions regime, in order to ensure sustainability and validity over time of the resulting typologies and address common challenges. Accordingly, this report covers all the actors most cited by jurisdictions in an effort to assist the FATF Global Network in identifying and mitigating its PF risk. [11]

The FATF Global Network's Experience in Assessing PF Risk

15. An effective way to evaluate relevant vulnerabilities is by conducting a PF risk assessment. While most countries across the FATF Global Network reported they have

9 FATF (2024) Money Laundering National Risk Assessment Guidance

10 FATF (2021) Guidance on Proliferation Financing Risk Assessment and Mitigation

11 As noted in the executive summary and elsewhere in the document, this report includes information on the techniques used to evade national and supranational sanctions regimes to provide an up-to-date understanding of threats and vulnerabilities, including the common challenges between relevant typologies that are not covered under Recommendation 7 of the FATF Standards. The broader framing of sanctions evasion is not intended to redefine the requirements of Recommendation 7.

assessed or are in the process of assessing PF risks as part of their national risk assessment process, there are indications that the extent of the assessment and/or understanding of PF vulnerabilities is in the early stages. For example, nearly half of countries responding to the questionnaire for this report did not verify whether they have PF vulnerabilities, while an additional six countries concluded they have no PF vulnerabilities.

16. In certain instances, countries indicated a low level of vulnerabilities to PF and sanctions evasion for several reasons, including geographic distance from sanctioned countries; no diplomatic or trade relations with sanctioned countries; underdeveloped financial sector with limited integration with the global financial market; robust national mechanism for implementation of TFS related to PF; and no identified PF cases in the jurisdiction.

17. Many of these are legitimate factors to lessen the potential that PF threat actors may exploit national or sectoral vulnerabilities. Still, it is important to consider that the global context has evolved enormously in recent years with the emergence of new technologies, including new payment systems, and a rise in geopolitical tensions. Also, the above factors do not consider broader weaknesses in AML/CFT/CPF controls for the public and private sectors or the prevalence of PF and sanctions evasion threat actors using various intermediaries in third countries to circumvent sanctions and export controls (see Typology 1). Because PF threat actors thrive on exploiting potential blind spots in the international financial system, more support and activities may be needed to identify and mitigate PF vulnerabilities and strengthen the collective effort to mitigate these vulnerabilities.

Current Situation

18. Despite comprehensive international, supranational and national sanctions regimes and export controls targeting WMD programmes, state-sponsored or -affiliated actors are successfully implementing complex procurement and revenue generation schemes to support PF actors and/or activities. In particular, the main threat actors are enlisting intermediaries in third countries, obscuring BOI, using new technologies, and exploiting the maritime and shipping sectors to evade sanctions, raise funds, and acquire dual-use goods (see section 2).

19. The FATF assesses the current threats and vulnerabilities as:

Current Situation – DPRK

20. The DPRK has been subject to significant international sanctions since the State conducted its first nuclear test in 2006. UNSCR 1718, passed in 2006, demanded that the DPRK cease nuclear testing, and it put in place TFS, amongst other countermeasures, on the DPRK broadly, but also specific to individuals and entities associated to the DPRK's WMD programme.

21. Despite being subject to UN sanctions for almost 20 years, the DPRK continues to progress its capabilities to deliver a nuclear device through its testing of intercontinental ballistic missiles. For example, on 31 October 2024, the DPRK launched an ICBM named Hwasong-19 that reached an altitude of approximately 7000 km while traveling a total distance of approximately 1000 km. This latest test is the 11th ICBM launch by the DPRK since announcing a new five-year military expansion plan in 2021.[12]

12 DPRK Korea's latest missile launch a 'grave threat' to regional stability | UN News

22. While the DPRK has continued such activities, the activities of the international community have not followed the pace or trajectory of the threat posed by the DPRK. There have been no additions to the UN's DPRK sanctions list in almost a decade. In addition, UNSCR 1718 Committees' Panel of Experts (POE) was dissolved in 2024. The dissolution of the UNSCR 1718 POE presents a major challenge for monitoring violations of sanctions relevant to the DPRK.[13] Many countries relied upon the biannual UNSCR 1718 POE reports to inform their national risk assessments on PF. As noted by the FATF Plenary in June 2024, "the ability to obtain reliable and credible information to support the assessment of PF risks relating to the DPRK is hampered by the recent termination of the 1718 Committee Panel of Experts mandate."[14]

23. In conducting this study, FATF delegations raised two main aggravating factors contributing to the DPRK's financing of its WMD programme: the DPRK's increasing financial connectivity and the diversity of the DPRK's revenue generation.

Increasing Financial Connectivity of the DPRK

24. While the FATF has continually reiterated since 2011 the need for all countries to robustly implement TFS consistent with UNSCRs and apply countermeasures to protect their financial system from illicit finance emanating from the DPRK, the jurisdiction has increased connectivity with the international financial system recently, which raises PF risks, as the FATF also noted in June 2024.[15]

25. In the DPRK-Russia Comprehensive Strategic Partnership Treaty[16] which came into force in late 2024, the two countries commit to strengthen cooperation, including by: creating favourable conditions for economic cooperation in custom finance and banking; working together to create favourable conditions for establishing direct ties between the DPRK and the Russian Federation; and promoting mutual understanding of the economic and investment potential of regions. Strengthening economic ties, particularly in re-establishing banking connections with DPRK financial institutions or entities that have been linked to PF, could introduce new vulnerabilities in the global financial system since several DPRK financial institutions and their overseas representatives are designated under UNSCR 1718.[17]

26. Since 2016, the number of countries hosting DPRK bankers has shrunk from 14 to four because of host-country sanctions enforcement and DPRK personnel withdrawals, most recently from Indonesia and Libya in late 2023. However, from 2023 to at least mid-2024, DPRK bankers in a neighbouring country and Russia facilitated transactions valued at hundreds of millions of dollars to support the DPRK's trade and revenue generation. As of mid-2024, more than 50 DPRK banking representatives were operating outside the country, despite UNSCR 2321 requiring host countries to expel them.[18] Also, UNSCR 2270 requires host countries to close existing representative offices and prohibits the DPRK from opening or operating new branches, subsidiaries, or representative offices in UN Member

13 Security Council Fails to Extend Mandate for Expert Panel Assisting Sanctions Committee on Democratic People's Republic of Korea | Meetings Coverage and Press Releases

14 High-Risk Countries subject to a Call for Action - June 2024

15 High-Risk Countries subject to a Call for Action - June 2024

16 http://en.kremlin.ru/acts/news/75534

17 Relevant UN-designated entities include Tanchon Commercial Bank (KPe.003), Bank of East Land (KPe.013), Amroggang Development Banking Corporation (KPe.009).

18 UNSCR 2321 requires host countries to take proactive steps, such as expelling DPRK banking representatives and prohibiting public and private financial support from within their territories or by persons or entities subject to their jurisdiction for trade with the DPRK.

States' territories.[19] One delegation noted that, in January 2024, a Russia-based banker enabled a deal to send DPRK construction workers to Russia where they earn foreign currency and enable DPRK to continue to circumvent UN sanctions.

The DPRK's Diversity of Revenue Generation Activities Benefit its WMD Programme

27. Many countries reported the criminal activities most associated with PF and sanctions evasion schemes involve forgery, fraud, (cyber)theft, and trafficking of arms, drugs, wildlife, smuggling and other items. DPRK-linked individuals and entities carry out these types of illicit activities and exploit legitimate businesses to raise revenue for the WMD programme, especially targeting countries or sectors with weak or no AML/CFT/CPF controls, such as new technologies and the maritime and shipping sectors (see Typologies 3 and 4). In addition to focusing on revenue generation through the use of IT workers in recent years, the DPRK is also known for targeting a diverse variety of sectors or illicit activities for generating revenue, including:

- **Wigs and false eyelashes sector**: Some countries are monitoring the DPRK's use of lucrative exports of wigs and false eyelashes to boost its finances and mitigate the impact of international sanctions designed to constrain its strategic weapons programme. Through the first half of 2024, the products accounted for nearly 60 percent of all DPRK exports to a neighbouring country. To produce these products, the DPRK imports raw materials from the same neighbouring country to make semifinished products, which the DPRK then sends back to firms for final processing and export to third countries. DPRK trading companies that produce wigs are subordinate to entities on the UNSCR 1718 List, which suggests that the wig revenue may be supporting the DPRK's strategic weapons programme. While UN sanctions do not prohibit companies from buying DPRK-origin wigs and false eyelashes, the companies involved in the production and purchase of the end products may not be aware of the link to UN-sanctioned entities.
- **Illegal wildlife trade:** Most of the sourcing of the illegal wildlife trade by the DPRK has taken place in Sub-Saharan African countries, given many of these countries' historic links with the DPRK. Illegal wildlife trade is a low-risk, high-reward means for the DPRK to source funds. With the DPRK diplomatic presence declining in Sub-Saharan Africa in recent years, this channel may become more difficult to exploit via diplomatic personnel. In addition, some countries agree with a RUSI assessment that DPRK citizens operating undercover as third-party nationals may play a greater role in sourcing and transporting these items in the coming years (for example, disguised as

[19] As described in the FATF's June 2024 statement on high-risk jurisdictions, "The FATF has continually reiterated since 2011 the need for all countries to robustly implement the targeted financial sanctions in accordance with UNSC Resolutions and apply the following countermeasures to protect their financial systems from the money laundering, terrorist financing, and proliferation financing threat emanating from DPRK: Terminate correspondent relationships with DPRK banks; Close any subsidiaries or branches of DPRK banks in their countries; and Limit business relationships & financial transactions with DPRK persons. Despite these calls, DPRK has increased connectivity with the international financial system, which raises proliferation financing (PF) risks, as the FATF noted in February 2024. This requires greater vigilance and renewed implementation and enforcement of these countermeasures against the DPRK. As set out in UNSCR 2270, DPRK frequently uses front companies, shell companies, joint ventures and complex, opaque ownership structures for the purpose of violating sanctions. As such, FATF encourages its members and all countries to apply enhanced due diligence to the DPRK and its ability to facilitate transactions on its behalf."

individuals from known wildlife trafficking transit and destination countries).[20]

Current Situation – Iran

28. Iran was originally sanctioned by the UN pursuant to UNSCR 1737 after the country refused to comply with UNSCR 1696, which required that Iran cease its uranium enrichment programme. This UNSCR was the first of a number to impose TFS on Iranian individuals and entities related to their nuclear programme.

29. Through UNSCR 2231, the UN Security Council endorsed the Joint Comprehensive Plan of Action, where Iran agreed to limit their nuclear programme in return for sanctions relief and other provisions. In accordance with UNSCR 2231, the TFS imposed on individuals and entities related to Iran's nuclear programme were sunset in October 2023 and no longer apply to FATF Recommendation 7. However, a number of countries use national sanctions programmes to implement TFS on Iran due to the threat posed by Iran and affiliated individuals and entities.

30. Iran has relied on militarised proxies in the Middle East as well as an array of transnational criminal organisations (TCOs) based within Iran and abroad to mitigate the impact of economic sanctions. Well-connected overseas businesspersons have aided in Iranian oil smuggling efforts, while banks, gold traders, and foreign exchange houses can serve as important conduits for money laundering and complex sanctions evasion. As described in various case studies, Iran's evasion of sanctions and export controls can support the development of missiles, weapons, military aerial equipment, and the WMD programme.

31. Iran's proxies have benefited from access to criminalised markets—particularly foreign exchange houses—that had previously served as conduits for ISIS and al-Qaeda financing. Hezbollah has played a particularly important role in this regard due to its extensive smuggling operations, global network of licit and illicit businesses, and dominant role in global money laundering through foreign exchange houses. Hezbollah has been linked to the smuggling of oil, weapons, and a range of sanctioned goods.[21]

32. Also, Hezbollah has penetrated financial institutions in numerous countries around the world and has carried out laundering schemes that straddle multiple continents and commercial sectors. Hezbollah operatives have even sought access to weapons and equipment in contravention of sanctions on Iran's behalf, a high-risk endeavour. These relationships show that the criminal markets that underpin Iran's foreign operations serve as catalysts for a range of threats.

Current Situation – Russia

33. As a result of the international sanctions pressure put forth onto the Russian economy because of the military invasion of Ukraine, the Russian Federation had to take steps to sustain its economy and military position. As described earlier in this section, one such move includes the signing of the Comprehensive Strategic Partnership Treaty with

20 UN investigating claims of rampant North Korean wildlife trafficking in Africa | NK News

21 As noted in the executive summary and elsewhere in the document, this report includes information on the techniques used to evade national and supranational sanctions regimes to provide an up-to-date understanding of threats and vulnerabilities, including the common challenges between relevant typologies that are not covered under Recommendation 7 of the FATF Standards. The broader framing of sanctions evasion is not intended to redefine the requirements of Recommendation 7.

DPRK.[22] This treaty creates economic and military linkages between the two countries, including provisions to: enhance strategic and tactical cooperation; provide military assistance; and take joint measures to strengthen defence capabilities (see para 26 for information on the economic coordination).

34. In April 2025, the DPRK confirmed the deployment of North Korean soldiers in the Russia-Ukraine conflict under the bilateral treaty, while Russian officials confirmed the activities of DPRK soldiers in the Kursk region.[23] [24] Previously, the March 2024 UN 1718 POE report cited UN efforts to investigate the presence of DPRK-sourced munitions in Ukraine.[25] As a result of the economic and military connectivity between Russia and the DPRK, the primary PF threat actor sanctioned by the UN for two decades, many countries view Russia as a PF threat by extension.

Other Threats

35. Additionally, many countries remain concerned about the efforts of non-state actors, such as terrorist groups and criminal organisations, to acquire and/or source goods, knowledge, and technology related to WMD, including biological, chemical, and nuclear capabilities. In November 2022, the UN Security Council renewed the mandate for UNSCR 1540, focusing on preventing the proliferation of WMD, knowledge, or precursor material to non-state actors.[26] As noted in the FATF's 2021 PF Guidance, UNSCR 1540 obligations exist separately and apart from the obligations set forth in Recommendation 7 and its interpretative note.[27] While there are few examples of non-state actors exploiting the financial system to support PF actors or activities, many countries view the potential impact of this activity makes it important to monitor on an ongoing basis. Also, there may be typologies from these activities that are relevant for understanding and mitigating overarching PF and sanctions evasion risks. As a result, some non-state actor case studies appear in this report.

Vulnerabilities

36. As described in the FATF's 2021 PF Guidance, vulnerability refers to factors that can be exploited by the relevant threat or threat actors that may support or facilitate the breach, non-implementation, or evasion of PF-TFS. Under the existing FATF Standards, this is applicable to the threat posed by the DPRK and the associated actors supporting the DPRK to evade UN sanctions. For those countries that view PF risk through a wider lens, this would apply to vulnerabilities exploited by all PF actors seeking to exploit the weaknesses of the public and private sectors.

37. Countries should consider vulnerabilities at the national (including structural) and sectoral levels. A national or structural vulnerability can include weaknesses in the legal and regulatory framework for AML/CFT/CPF. Other national-level vulnerabilities may include inherent factors in the jurisdiction, such as size and complexity of the economy, the extent to which the economy is informal/cash based, or the diversity of legal persons and arrangements.[28] For exposure to PF-related vulnerabilities particularly, many countries

22 http://kcna.kp/en/article/q/6a4ae9a744af8ecdfa6678c5f1eda29c.kcmsf
23 http://www.rodong.rep.kp/en/index.php?MTJAMjAyNS0wNC0yOS0wMDFAMTVAMUBAMEAxQA==
24 http://en.kremlin.ru/events/president/news/76805
25 https://docs.un.org/en/S/2024/215
26 Security Council Extends Mandate of Committee Monitoring Nuclear, Biological, Chemical Weapons for 10 Years, Unanimously Adopting Resolution 2663 (2022) | Meetings Coverage and Press Releases
27 Guidance on Proliferation Financing Risk Assessment and Mitigation
28 Money-Laundering-National-Risk-Assessment-Guidance-2024.pdf.coredownload.inline.pdf

noted the importance of their geographic location. This contextual factor is identified as significant in potential connection to DPRK's sanctions evasion schemes.

38. A sectoral vulnerability pertains to characteristics specific to a sector that can be abused by a person or entity to implement complex proliferation financing and sanctions evasion schemes. For example, the contextual feature of the delivery channel in a sector such as the prevalence of intermediaries and agents may impede the tracing of financial flows or asset movement.

National-level Vulnerabilities for PF and Sanctions Evasion

39. Some of the most common national-level vulnerabilities facilitating complex proliferation financing and sanctions evasion schemes that have been identified by the FATF Global Network are:

Economic and Trade Factors

40. Many countries noted that PF and sanctions evasion threat actors target countries that act as international financial centres, given their importance to global financial flows and transport (see Typology 1). The vulnerability for PF arises from the vast range of products and services offered by international financial hubs serving a broad and diverse customer base. Moreover, the openness (including the presence of Special Economic Zones) and sophistication of those established financial systems and economies facilitating cross-border transactions make them particularly vulnerable to misuse by illicit proliferation networks. Countries with strategic ports equipped with shipping and logistics infrastructure are also prone to be misused to circumvent sanctions and export controls related to dual-use goods.

41. Also, many countries cited vulnerabilities related to maintaining economic and trade relations with sanctioned countries [29], which increases the exposure to potential PF and sanctions evasion schemes. Geopolitical alignment, dependencies, or historical linkages may create opportunities for PF threat actors to target these countries without the knowledge of the country to circumvent sanctions and access financial systems and resources.

42. Most countries spotlighted the importance of customs agencies to prevent and detect complex sanctions evasion schemes relevant to PF. Customs agencies play a key role collecting and exchanging information domestically, regionally, and internationally (see Section 3).

Regulatory Factors

43. While countries have made progress in putting AML/CFT regulation in place, the global implementation of CPF-related measures is still lagging (see Figures 1 and 2). In the absence of a robust regulatory, legislative, and operational framework, some countries are not able to apply the required sanctions obligations and export controls to deter and

[29] In practice, many countries seek to address vulnerabilities relevant to evasion of UN, national, and supranational sanctions regimes. However, the FATF's Recommendation 7 only applies to the DPRK, which is the sole UN-sanctioned country. As noted in the executive summary and elsewhere in the document, this report includes information on the techniques used to evade national and supranational sanctions regimes to provide an up-to-date understanding of threats and vulnerabilities, including the common challenges between relevant typologies that are not covered under Recommendation 7 of the FATF Standards. The broader framing of sanctions evasion is not intended to redefine the requirements of Recommendation 7.

counter proliferation networks. Moreover, complex PF and sanctions evasion schemes employ a variety of obfuscation techniques, which are even harder to detect in unregulated sectors or sectors with inadequate oversight, such as VASPs. Further, the PF vulnerability deepens for countries with weak national laws on transparency of beneficial ownership for legal entities. Difficulty accessing BO information impedes cross-border investigations by authorities seeking to identify and trace the PF path, especially when multiple countries with inconsistent legal frameworks are involved.

Geographical and Demographic Factors

44. Some countries reported on vulnerabilities related to their geographical proximity to countries subject to UN, national, and supranational sanctions regimes, which may create opportunities for illicit networks to move assets and resources across borders. Strategically located countries offer vital shipping lanes and trade routes that raise the inherent vulnerability of neighbouring countries. For example, trade-based sanctions evasion schemes involving smuggling of illegal goods are more likely to occur between countries in proximity to a sanctioned jurisdiction (see Typology 4). As demonstrated in case studies, countries in East Asia may be exposed to the DPRK facilitating circuitous financial transactions and shipments, while countries in the Middle East may create illicit financial pathways for Iran's WMD programme. Also, some countries reported on vulnerabilities associated with the presence of diplomatic personnel and other relevant actors from jurisdictions subject to UN sanctions regimes.

Other National-level Factors

45. Another vulnerability is the large volumes of widely used foreign currencies like the US dollars in the global financial system. Countries should have regard to the cross-border transactions being affected in those foreign currencies given the vulnerability of the use of those currencies or accounts denominated in those currencies for illicit procurement or sanctions evasion.

46. Also, proliferation networks seek to exploit industrial and technological factors to illicitly acquire goods. Thus, countries that are producers of proliferation sensitive technology and goods are inherently vulnerable to PF and breaches of dual-use good restrictions. Countries with large defence sectors require a significant number of organisations to provide materials, products, and services. This provides opportunities for PF networks to take advantage of complex supply chains.

47. Finally, UNSCR 1718 POE reports highlighted the DPRK's reliance on organised or transnational criminal networks, leveraging their transport corridors and intermediaries, to support proliferation activities.

Sectoral-level Vulnerabilities for PF and Sanctions Evasion

48. Based on submissions by the FATF Global Network and results of the public consultation, the sectors most vulnerable to complex PF and sanctions evasion schemes include:

Banking and Other Financial Sectors

49. Many countries identified banking and other financial sectors, such as insurance, as vulnerable to PF and sanctions evasion threat actors. After financial transactions are conducted within countries and across borders, the funds supporting PF actors or activities may be generated from or moved through licit or illicit activity. Techniques often used to

blur the nature of these transactions include the use of several accounts and falsified documents, including related to trade finance.

50. Correspondent banks are vulnerable to sanctions evasion since they often do not have a pre-existing relationship with the customer of the respondent bank.[30] Several private sector entities identified various complex account types and transactions vulnerable to PF and sanctions evasion risk, which are especially relevant to correspondent banking relationships involving linkages to countries with higher risk exposure to PF and/or ineffective CPF controls. For example, trade conducted through open account transactions are vulnerable, because it lacks information on the goods being transported. Additionally, wire transfers allow for rapid movement of funds, but they typically contain limited information on transactional purpose or supporting documentation.

51. Some countries identified several other relevant factors, including financial systems with extensive nationwide networks, quick and easy access to banking services, increase in outstanding amount of investment assets, and an abundance of financial assets held by individuals.

Virtual Assets and Virtual Asset Service Providers

52. Many countries are concerned about the increasing use of virtual assets to make payments and transfers across borders. PF networks often seek to exploit the lack of effective implementation of AML/CFT/CPF measures for VASPs across countries, given lagging implementation of Recommendation 15 (see Typology 3). There are also instances of VASPs in countries with AML/CFT/CPF requirements failing to comply with applicable obligations. Countries are particularly concerned about associated PF risks to pseudonymously raise and move funds. Many illicit actors seek to increase anonymity in virtual asset transactions by using virtual asset mixing services and anonymity enhancing cryptocurrencies (AECs) including in the process of laundering proceeds of large-scale virtual asset heists that support the WMD proliferation. The use of mixing and other obfuscation techniques can make it difficult for third parties to trace or attribute transactions. Also, countries noted the role of virtual assets in revenue generation efforts by the DPRK.

New and Alternative Payment Infrastructure

53. Some state and non-state actors are exploring new payment channels and alternatives to the SWIFT payment system to avoid financial touchpoints linked to national, supranational, and/or international sanctions regimes. For example, in certain instances, state and non-state actors could utilise emerging digital payment systems like peer-to-peer payment services or digital remittance providers.[31]

---

30 Correspondent banking, especially those offered to known diversion/ conduit jurisdictions, or those with ineffective AML/CFT/CPF controls can pose heightened risks. However, correspondent banking risk is not uniformly high for proliferation financing. Risk assessment of correspondent relationships should be done on a case-by- case basis and should always take account of the internal controls and risk mitigation measures applied by the respondent bank. See the FATF's *2021 PF Guidance* for more information on correspondent banking relationships.

31 While there are potential risk management concerns regarding alternatives to the SWIFT payment messaging system, the use of Central Bank Digital Currencies (CBDCs) to evade sanctions is theoretical right now. On the other hand, some countries view CBDCs as a way to allow competent authorities to trace more easily the flow of funds and reduce illicit finance risks.

Other Sectoral-level Vulnerabilities

54. As noted in UNSCR 1718 POE reports and the FATF's 2021 Guidance on PF Risk Assessment and Mitigation, countries should be aware of additional sectors with higher exposure to the potential breach, non-implementation or evasion of PF-TFS, including, but not limited to: trust and company service providers (TCSPs) and dealers in precious metals and stones.[32]

55. Also, countries identified several other sectors vulnerable to the exploitation of PF and sanctions evasion actors, including aeronautics, information technology (IT), maritime, nuclear power, and shipbuilding.

32. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf

4. Section 2. Evasion of Sanctions Relevant to PF – Typologies

Current Trends and Methods

56. In this report, case studies are separated into two distinct categories:

a. **Evasion of PF-TFS related to the DPRK**, which is covered under Recommendation 7 of the FATF Standards

b. **Evasion of other sanctions regimes (such as national and supranational sanctions)**, which are not covered under Recommendation 7 of the FATF Standards

57. This section aims to provide a non-exhaustive list of typologies used in complex PF and sanctions evasion schemes, based on the information submitted by the FATF Global Network. These typologies have resulted in a list of indicators of financial transactions that could be indicative of PF (see Annex A: Risk Indicators).

Table 1. Overview of Typologies

Typology	Case Study Sub-Topics	Pages
1. Enlisting Intermediaries to Evade Sanctions	Front and Shell Companies Transit through Third Countries Bank Accounts and Financing	25-33
2. Obscuring BOI to Access the Financial System	Third-party Facilitators Supporting Financial Access Networks of Unlicensed Financial Facilitators Using Different Types of Legal Persons Exploitation of Credit and Debit Cards by the DPRK	33-40
3. Using Virtual Assets and Other Technologies	Regulatory Challenges Using Virtual Assets to Move Funds Virtual Assets and Generation of Funds Foreign Entities and Individuals Supporting DPRK IT Workers	40-47
4. Exploiting the Maritime and Shipping Sectors	Altering Vessel ID Ship-to-ship Transfers Disabling AIS Broadcast Falsifying Documents	47-52

Typology 1: Enlisting Intermediaries to Evade Sanctions

58. Countries report that to conceal the real end-users, procurement networks of goods destined for proliferating or sanctioned countries are using complex schemes involving several intermediaries. These tactics make it difficult to detect and investigate PF and sanctions evasion cases. Those intermediaries can involve shell and front companies, financial facilitators, bank accounts (including correspondent banking relationships), and transshipment through third countries. The use of those intermediaries plays a crucial role in masking the origin, destination, and purpose of funds. By exploiting vulnerabilities in different financial systems and regulatory frameworks, intermediaries enable proliferation

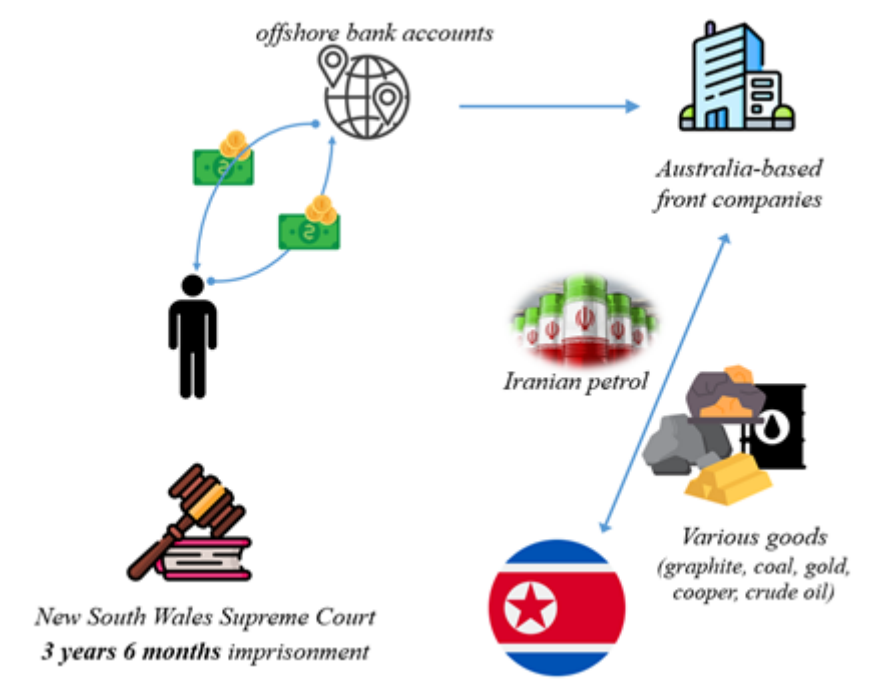
networks to evade detection and sanctions (see Vulnerabilities section for more information).

Use of Front and Shell Companies

59. Many countries reported that PF and sanctions evasion networks can set up or partner with local businesses in third countries to act as intermediaries and front companies. These entities can be shell companies with no activity or conduct legitimate-appearing transactions to access financial systems, facilitate payments and contracts, import or export goods under false pretences (such as declaring dual-use goods as solely for civilian purposes), and obscure the connection to sanctioned entities by operating under different names, ownership structures, or countries. The illicit actors operate in sectors relevant to the smuggled dual-use goods or items, such as electronics, chemicals, or industrial equipment, or other goods subject to sanctions or export control regulations.

Box 2. Case Study: Use of Australia-based corporate structure to evade sanctions

On 23 July 2021, the New South Wales Supreme Court sentenced a South Korean-born Australian citizen to a term of three years and six months imprisonment for contravening Australian sanctions law relating to the DPRK. The individual used offshore bank accounts and a series of Australia-based front companies to broker trade with the DPRK in a variety of goods, including coal, graphite, copper ore, gold, crude oil (including purchasing Iranian petrol on behalf of the DPRK), missiles and missile-related technology. This was the first time charges were laid in Australia for breaches of sanctions in relation to the DPRK.



Source: Australia

60. Intermediaries can also involve the support of lawyers and accountants who help to set up complex structures to avoid detection, or freight forwarders and shipping agents who aid in creating complex supply chains and providing advice on exploiting loopholes in sanctions regimes and ensuring that prohibited goods are mis-declared and shipped under false pretences.

61. Front companies are a common vehicle to obscure the path of dual-use goods with an application in military weaponry or the defence sector. Illicit actors employ these types of complex vehicles to slow the momentum of investigations to uncover the potential evasion of sanctions or circumvention of export controls involving sensitive goods. The two case studies below describe complex schemes to hide the final destination for such dual-use goods.

Box 3. Case Study: Sanctions evasion scheme to smuggle U.S.-origin electronic components to Iranian military entities

In January 2024, four Chinese nationals were charged in an indictment in the District of Columbia with various federal crimes related to a years-long conspiracy to unlawfully export and smuggle U.S.-origin electronic components from the United States to Iran. The defendants allegedly unlawfully exported and smuggled U.S. export-controlled items through China and Hong Kong for the benefit of entities affiliated with the Islamic Revolutionary Guard Corps (IRGC) and Ministry of Defense and Armed Forces Logistics (MODAFL) that supervise Iran's development and production of missiles, weapons, and military aerial equipment to include Unmanned Aerial Vehicles (UAVs).

Beginning as early as May 2007 and continuing until at least July 2020, the individuals utilised front companies in China to funnel dual-use U.S.-origin items, including electronics and components that could be used in the production of UAVs, ballistic missile systems, and other military end uses, to sanctioned entities with ties to the IRGC and MODAFL such as Shiraz Electronics Industries (SEI), Rayan Roshd Afzar, and their affiliates.

Throughout the course of the conspiracy, the defendants concealed the fact that the goods were destined for Iran and Iranian entities and made material misrepresentations to U.S. companies regarding end destination and end users. These deceptive practices caused the U.S. companies to export dual-use goods to the front companies under false pretences and under the guise that the ultimate destination of these products was China as opposed to Iran in violation of U.S. sanctions and export control laws and regulations. The charges related to this complex sanctions evasion scheme were coordinated through a multiagency strike force co-led by the Departments of Justice and Commerce.

Source: United States

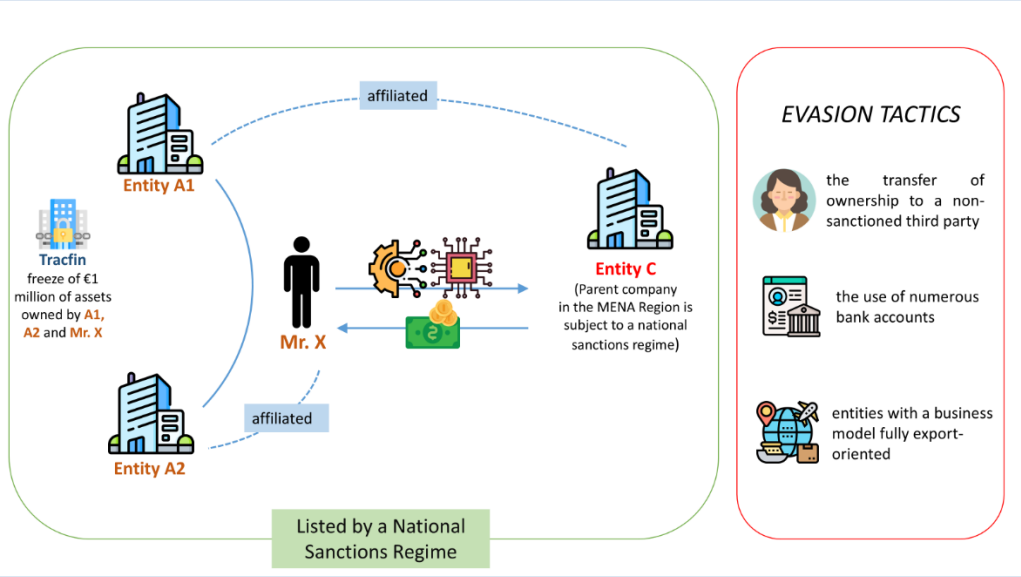
Box 4. Case Study: Export of dual-use goods to Russian entity using intermediaries

French companies A1 and A2, acted as an intermediaries to purchase foreign electronic components that were re-sold to another intermediary entity in the MENA region (Entity B). After the intermediaries purchase the dual-use goods, they supplied the electronic components to a Russian U.S.-sanctioned parent company (Entity C). This proliferating scheme allowed the Russian defence sector to be provided with prohibited items and enhanced its overall capabilities.

The French FIU, TracFin, led an interagency effort to halt this scheme with the freeze of €1 million of assets owned by A1, A2, and Mr.X (UBO of A1 and A2). While U.S. Treasury's OFAC sanctioned A1, A2, and Mr. X, the individual and entities are not subject to EU or French restrictive measures for now. Subsequently, TracFin worked along with French banks to restrict their funds under the control criteria[33], since there was suspicion that Entity C still holds control over Company A1 despite having sold its shares to a foreign investor. Entity A2 is fully owned by Mr. X.

This complex sanctions evasion scheme involved the use of many common evasion tactics, including the transfer of ownership to a non-sanctioned third party (the individual's wife), the use of numerous bank accounts, and entities with a business model fully export-oriented, which nonetheless were acting as pass-by entities.

The major challenge was the discrepancy between sanction regimes,[34] which could lead to capital flight. Concerted designation processes would be beneficial to ensure sanctions are efficient, and to ensure there is a legal basis for asset freezing across countries.



Source: France

Use of Transit in Third Countries to Leverage Globalised Supply Chains and International Trade

62. Countries described proliferation networks using globalised supply chains and international trade to obscure procurement activities of goods and technology. They may

source components from multiple suppliers to make the nature of the end-use less apparent, and transfer goods through free trade zones (FTZs), which often have less stringent oversight and allow repackaging and re-exporting under new labels. Goods can be shipped through multiple ports or countries to hide the true origin or destination, using false documentation, falsified shipping documents, end-user certificates, or bills of lading to misrepresent the nature of the cargo or the final recipient. For example, a prohibited shipment of missile components might be disguised as industrial machinery with altered documentations. The two case studies below describe complex transit routes to make it more difficult to detect the circumvention of export control regulations and sanctions.

Box 5. Case Study: Use of intermediaries to circumvent export control regulations

Several cases, tending to illustrate a recurring typology, highlight circumvention schemes where third-country companies, sometimes based in another EU jurisdiction, managed or controlled by Iranians, purchasing dual-use goods from French suppliers, which are then re-exported to Iran.

An Iranian company supplying Iran's ballistic missiles programme tried to obtain composite materials from a French supplier. The Iranian head of the company used a company in a third country run by another Iranian national, who would then re-export the composite materials to Iran.

In 2020, a machine tool was exported consecutively to European countries A, B, and C before leaving the EU territory. This complex trade pattern and changes in documentation were intended to camouflage the rest of the journey, which included arrival in a jurisdiction in the Middle East before the machine tool reached its final destination in Iran.

Source: France

Box 6. Case Study: Detection of EU Sanctions' evasion through the use of intermediaries through international cooperation

In 2022, a Portuguese company attempted to export motors with application in UAVs via an intermediary in the UAE with an alleged final destination to a Kazakhstan-based company. These goods were covered under the scope of the 12th Package of EU Restrictive Measures for Russia and there were strong indicators that the goods final destination would be The Russian Federation. During the investigations, the company dropped the export of the goods after questions were raised about the destination.

The company tried to circumvent the sanctions using two different intermediaries: a freight forwarder in UAE and a retailer in Kazakhstan. It also concealed the final end user. The Kazakh company had strong commercial ties with Russian companies and the

33 In EU law, control criteria help determine if funds or an entity are controlled by a sanctioned entity or person. For example, if the sanctioned person or entity holds influence or can take decision over the funds or entity, this can help to determine there is control.

34 Such discrepancy is one of the key factors in challenges in detecting, investigating, and prosecuting sanctions evasion relevant to PF, as noted in Section 3 (see para 105-106) and in conclusion (see para 146 and priority areas).

risk of diversion was high. Payments were conducted through bank transfers.

Afterwards, the Portuguese authorities monitored the company and discovered that this company exported later in 2023 other goods in the field of security and defense, likely to Russia, through intermediaries in Serbia and Hong Kong. Both intermediaries were companies with strong commercial relations with the Russian Federation.

The case involved the cooperation of the Security Intelligence Service and the Customs Authority. The case was detected through intelligence collection and investigated with the help of international cooperation and customs investigations.

This example illustrates the ability of the procurement networks to adapt to new circumstances and different challenges. Only effective cooperation between countries with fluid communication can help to mitigate this kind of threat.

Source: Portugal

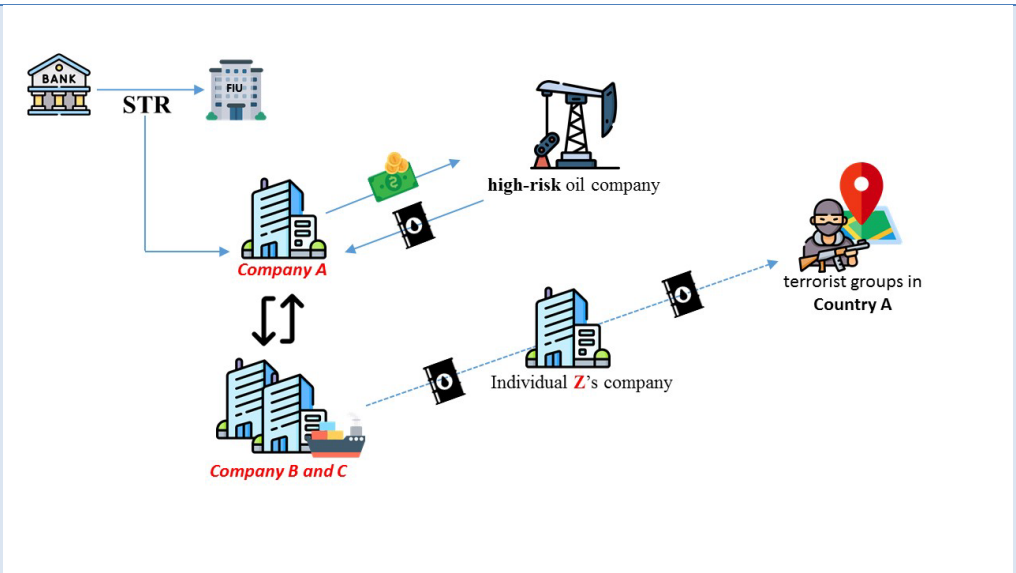
63. Additionally, regional transit hubs in close proximity to sanctioned countries or entities are targeted by sanction evaders seeking to move funds and commodities. In particular, PF and sanctions networks seek to mask their activity in international financial centres, where they hope the vast scale of commercial, financial, and trade activity can help to mask their illicit activities.

Box 7. Case Study: Using shipping companies to sell oil for sanctioned entity

In September 2022, LEAs received a UAEFIU dissemination regarding a SAR/STR from a bank. The SAR/STR highlighted that a wire transfer from Company A to a high-risk oil company suspected of being used to support WMD proliferation. LEAs and the UAEFIU conducted a criminal and financial investigation on Company A, and its financial/commercial activities.

The investigations identified that Company A was established by a foreign national, connected to two UAE shipping companies (Companies B and C). It also revealed that Companies B and C belonged to individuals supporting terrorist groups in Country A. Both companies used Individual Z's company as an intermediary to prepare shipping contracts for moving oil from high-risk country to Companies B & C, which were later to be shipped to the terrorist group.

The investigation also revealed that Companies B & C sold oil to the terrorist group using forged documents to conceal the oil's source and origin. Proceeds of oil sales were transferred to Company A, which sent them to the high-risk oil company – a suspected front used by the sanctioned entity to support proliferation. Investigations identified that the total funds transferred were USD $70 million. LEAs arrested all suspects, including Person Z, who confessed their involvement in assisting Iran to evade PF sanctions and suspended the companies' business activities.



Source: United Arab Emirates

Use of Bank Accounts and Financing Through Third Countries

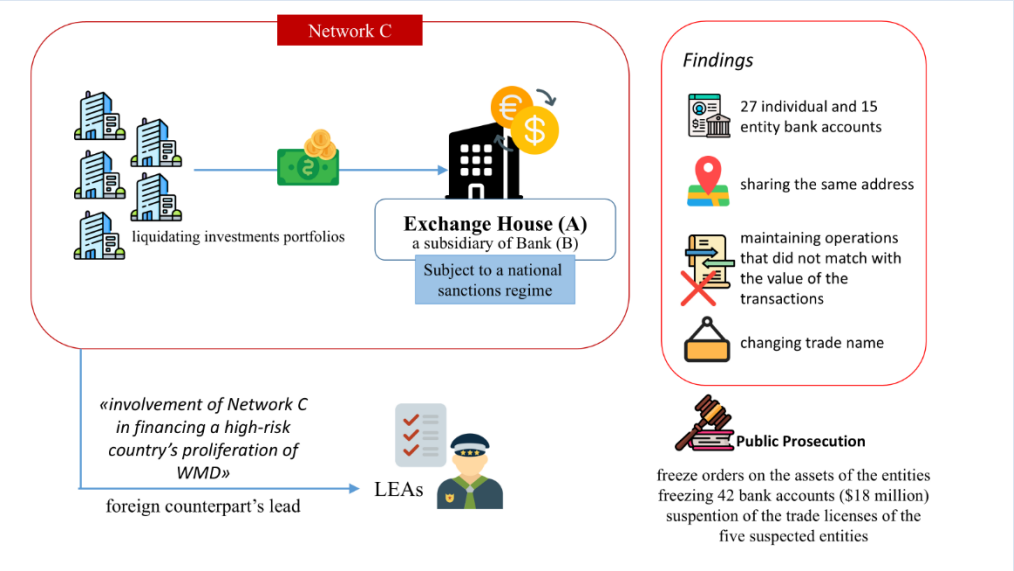
64. PF and sanctions evasion actors often use multiple layers of financial transactions to conceal the origin, destination, or purpose of funds, which is a classic money laundering technique. They often route payments through multiple financial institutions across several countries to hinder tracing efforts, with front business or shell companies registered in countries with regulatory loopholes.

Box 8. Case Study: Misusing the financial system and oil shipments to support PF

LEAs identified, through confidential sources, multiple high-value inward/outward transactions conducted by five UAE companies with high-risk Exchange House (A), a subsidiary of Bank (B). Both Exchange House A and Bank B are part of "Network C" and are designated by U.S. Treasury's OFAC. Two of the five suspected companies were obtaining funds by liquidating investments portfolios and transferring the funds to Exchange House A, which in turn transferred the funds to Bank B to support a sanctioned entity. LEAs commenced an investigation with the relevant stakeholders (UAEFIU, CBUAE, Local Registrars, and customs).

CBUAE identified 27 individual and 15 entity bank accounts linked to the network. Local Registers also provided LEAs with on-site inspection reports; these reports revealed that the suspected entities shared the same address, tended to change their trade name prior to the onsite visit, and maintained operations that did not match with the value of the transactions. In parallel, LEAs received a lead from a foreign counterpart that confirms the involvement of Network C in financing a high-risk country's proliferation of WMD.

Based on these findings, the Public Prosecution, in coordination with the UAEFIU and CBUAE, issued freeze orders on the assets of the entities, freezing 42 bank accounts with a total balance of approximately $18 million (63,725,065 AED). In addition, the Local Registrars suspended the trade licenses of the five suspected entities.



Source: United Arab Emirates

65. PF networks target financial institutions in third countries where they are seeking to take advantage of jurisdictional differences in the implementation of international and national sanctions regimes. The illicit actors use banks to open accounts, and to facilitate international wire transfers without raising red flags using correspondent banking relationships to access international financial markets indirectly. The illicit networks can also use informal financial systems that are less likely to detect suspicious transactions and rely on countries with less stringent reporting requirements or enforcement for cross-border transactions.

Box 9. Case Study: Entities and individuals sanctioned for constituting a "shadow banking" network used by the IRGC to generate revenues

In June 2024, OFAC sanctioned nearly 50 entities and individuals that constitute multiple branches of a sprawling "shadow banking" network used by MODAFL and the IRGC to generate revenue to, among other activities, illicitly procure the U.S.-origin electronic components to develop advanced weapons, such as UAVs, and support Yemen's Houthis and Russia's war in Ukraine.

To gain access to the international financial system, MODAFL uses exchange houses in Iran that manage numerous front companies in Hong Kong, the UAE, and elsewhere to launder revenue generated through foreign commercial activity, including oil sales, into clean foreign currency. The same front companies use the laundered foreign currency to procure weapons components on the international market.

Source: United States

Box 10. Case Study: Use of intermediaries to circumvent TFS and transfer revenue raised from real estate

In 2015, a DPRK diplomat, posted in France, bought an apartment in Paris and rented it, before being designated by the UN in 2017. After being sanctioned, he continued to receive revenue generated by the rental of the flat. The individual developed a scheme involving various intermediaries with bank accounts in several third countries, which hid his status as the end beneficiary. After the alert was raised by a European bank in 2019, the revenues were then placed in an escrow account.

Source: France

Typology 2: Obscuring BOI to Evade Sanctions and Access the Financial System

66. Complex PF and sanctions evasion often involve the falsification of BOI, obfuscating end-user/end-use and ultimate destination, which is challenging to detect for both the public and private sector. Also, a lot of these obfuscation techniques are being applied to the digital realm, which can pose an additional challenge to detection. Because TFS applies to designated individuals and entities, and the funds that are controlled or owned by these designated persons, identifying beneficial owners can help to mitigate risks associated with sanctions evasion.

Third-party Facilitators Supporting the DPRK's Access to Financial System

67. The DPRK routinely employs deceptive practices, including obscuring BOI, to circumvent UN and national sanctions regimes and access the formal financial system. The DPRK continues to use foreign-based front and shell companies, covert overseas representatives, and third-party facilitators to obfuscate the true originator, beneficiary,

and purpose of transactions, enabling billions of dollars of DPRK illicit financial activity to flow through the international financial system. State actors supporting the DPRK's complex schemes to access the financial system make it difficult to disrupt sanctions evasion.

Box 11. Case Study: DPRK and Russian financial entities orchestrated complex sanctions evasion scheme

In September 2024, U.S. Treasury's OFAC designated a network of five entities and one individual – based in Russia and in the Russia-occupied Georgian region of South Ossetia—that used illicit financial schemes to enable the DPRK to access the international financial system in violation of TFS required under UNSCR 1718.35 Also, the entities and individual violated a ban on correspondent relationships with DPRK banks under UNSCR 2270.

This action targeted complex schemes orchestrated by two DPRK state-run organisations, Foreign Trade Bank (FTB) and Korea Kwangson Banking Corporation (KKBC), both of which are designated entities on the UNSCR 1718 Sanctions List.36 FTB serves as the DPRK's primary foreign currency exchange bank and is vital to the illicit financial networks the DPRK uses to finance its WMD and ballistic missile programmes. FTB and KKBC have continued to expand the DPRK's access to illicit financial networks with the assistance of the Russian Federation.

In a scheme orchestrated by the Central Bank of Russia, MRB Bank (MRB), based in Georgia's South Ossetia region, acted as a cut-out for a Russian bank, TSMR Bank, OOO (TSMR Bank), to establish a secret banking relationship with the FTB. A senior official at TSMR Bank facilitated cash deposits from FTB through TSMR Bank to MRB. The senior official at TSMR Bank organised the opening of correspondent accounts for FTB and KKBC at MRB and coordinated with DPRK representatives to ensure the delivery of millions of dollars and rubles in banknotes to FTB and KKBC accounts at MRB. At least some of the DPRK accounts at MRB were used to pay for fuel exports from Russia to the DPRK.

As a part of a separate scheme in late 2023, the Russian Financial Corporation Bank JSC (RFC), worked with FTB to establish a Moscow-based company, Stroytreyd LLC (Stroytreyd), to receive frozen DPRK funds held in defunct Russian banks. As a part of this effort to repatriate frozen assets to the DPRK, RFC-owned Timer Bank, AO (Timer Bank) transferred funds worth millions of dollars to Stroytreyd that were for the ultimate benefit of FTB. DPRK government officials worked with the RFC to increase high-level economic exchanges between the DPRK and Russia and to enhance financial collaboration between the two countries. FTB has also worked with RFC toward opening accounts for other DPRK banks, including DPRK-based Agricultural Development Bank.[37]

Source: United States

35 https://home.treasury.gov/news/press-releases/jy2590

36 On the UNSCR 1718 List, FTB is designated as KPe.047 and KKBC is KPe.025

37 On January 10, 2025, Japan designated four individuals and five entities (MRB Bank, Russian Financial Cooperation, Stroytreyd LLC, TsMRBank, and Timer Bank AO) for facilitating DPRK-Russia cooperation.

68. As cited by many countries, the DPRK also relies upon its citizens, including diplomatic personnel, to facilitate the provision of financial services or transfer of assets or resources, including transporting bulk cash. These tactics are challenging to detect, and diplomatic protocols make it even harder to take timely action to intercept or disrupt such activities.

Box 12. Case Study: Spouse of DPRK diplomat moving funds with insurance company

Nigeria-based insurance companies were suspected of working with the spouse of a sanctioned country's diplomat to help the DPRK's national insurance corporation, the Korea National Insurance Company (KNIC), in debt recovery, business development, money collection, financial transfers, and acting as agents or representatives to circumvent United Nations sanctions. KNIC was designated under the UNSCR 1718 Sanctions Regime in 2017 (KPe.048). Money received through KNIC is diverted to the WMD programmes of the DPRK.

A SAR/STR filed by a financial institution helped Nigerian authorities to detect financial activities involving unreasonable amounts of money. The estimated total value of transactions exceeded €616,000. After the suspicious activity was identified, financial institutions froze relevant accounts and reported back to Nigeria authorities. Also, Nigeria is considering additional counter measures.

The vulnerability targeted in the insurance sector was the way in which insurance companies purchase international insurance or reinsurance for state infrastructure through third-party companies. Also, insurance customers and transactions were employed towards sanctions evasion schemes, which demonstrates the need to strengthen risk controls for relevant entities.

Source: Nigeria

69. Many countries are aware of the DPRK utilizing foreign nationals and front companies registered by these same individuals to obfuscate BOI to access and move funds through the formal financial system. For example, FTB and KKBC obscured financial ties to the DPRK by establishing networks of front companies in the name of Chinese nationals who hold accounts at China-based banks, to move funds through the international financial system.

Box 13. Case Study: DPRK banking and financial Services – Foreign Trade Bank

In May 2020, U.S. authorities unsealed criminal charges against more than 30 individuals who worked in various capacities to allegedly provide services and effect prohibited U.S. dollar transactions for UN-designated FTB. The indictment outlined specific payments made to U.S. companies ultimately on behalf of the DPRK government. Other payments between FTB front companies and other third-party companies cleared through U.S. correspondent banks.

The individuals listed in the indictment caused correspondent banks to process at least $2.5 billion in illegal payments, via over 250 front companies, that transited through the United States during the period of the conspiracy. These companies were established in Austria, China, Kuwait, Libya, the Marshall Islands, Russia, and Thailand. Many individuals indicted were stationed in these countries, operating covert "branches" of the FTB, with multiple significant activity concentrated in Chinese cities.

The individuals worked with third-party financial facilitators to create front companies that could make payments to purchase commodities and other goods on behalf of the DPRK, including payments related to the trade in refined petroleum and coal. Other payments were made to metals, electronics, and telecommunications companies. The defendants created new front companies once counterparties deemed the old ones suspicious. They used coded payment references in communications between FTB agents so FTB headquarters could direct purchases and keep an accurate appraisal of the flow of funds from their front companies to payees. Finally, when it came to shipping actual goods, the defendants labelled contracts and invoices with false end destinations and end-users.

Source: United States

Networks of Unlicensed Financial Facilitators Support Sanctions Evasion

70. Also, a number of countries identified Iran's use of complex sanctions evasion schemes, including the obfuscation of BOI, to source dual-use goods for their WMD programme. Often, Iran is observed to use front companies registered in key financial centres to move funds from money exchanges that are under the control of the Iranian government.

Box 14. Case Study: Use of illegal TCSPs to trade dual-use goods

Iranian citizens set up multiple legal entities in the Netherlands that were or are active in the technology sector. This includes the use of a recognised reference company[38] (RRC) to purportedly make it easier for highly skilled migrants to obtain a Dutch residence permit. The RRC is also part of or directly related to an illegal TCSP, which provides a variety of services like the registration of a company, opening of a bank account, and verifying at least half of the company directors are Dutch nationals (to benefit Dutch tax advantages and tax treaties).

While legal TCSPs are under the supervision of the Dutch Central Bank, illegal TCSPs divide up the services they provide and places them within multiple legal entities. By doing this, these services are cheaper, and it becomes more difficult to recognise such trust services. Therefore, it is difficult for the Dutch Central Bank to supervise the entities. In this case, money allegedly coming in from Iran via prominent financial centres, is being unlawfully transferred to the Dutch legal entities, that were set up by the illegal TCSP. Then, the money is transferred within this structure and eventually flows to the highly skilled migrants.

In this case, bank statements show multiple transactions that form risks for the supply of dual-use goods for Iran. These goods are also applicable for proliferation purposes. These transactions are also seen in relation to the tech companies controlled by the Iranian highly skilled migrants. Therefore, it can be concluded that these companies are acting as front companies. By making use of TCSPs, especially illegal ones, and setting up a web of companies, it makes detection extremely difficult to recognise in these financial transactions.

Source: The Netherlands

71. Unlicensed MSBs are also utilized to move money for individuals acting on behalf of domestic-designated and UN-designated terrorist groups. In the below case, UAE authorities uncovered a complex scheme to use a front company as a hawaladar[39] to move millions of dollars. While this is an example of individuals evading TF-TFS on behalf of non-state actors, it could be relevant to the types of complex schemes used to evade PF-related sanctions as well.

38 A recognised reference is a company, school or organisation who benefit of the arrival of foreigners.
39 Hawaladar is a money transmitter that provides Hawala services.

Box 15. Case Study: Unlicensed MSB used to evade sanctions for terrorist group on the UN 1267 List

In Q1 2022, a local Exchange House filed a SAR/STR to the UAEFIU regarding wire transfers from a high-risk jurisdiction, received by a foreign resident of the UAE. All parties engaged in the transfers were subjects of financial intelligence information obtained by the UAEFIU.

According the UAEFIU's investigation and analysis, the main suspect received seven wire transfers totaling $3.5M USD and had established a front company in the UAE to function as a hawaladar for the transfer of funds to high-risk countries to support members of the Daesh (ISIL) and Jabhat Al Nusra. Both groups are designated on the UAE National List and UN Consolidated List - UNSCR 1267/1989.

The UAEFIU provided State Security with a case dissemination that detailed information on the suspect and his front company. The State Security in collaboration with the UAEFIU and Central Bank investigated the suspects financial activities. Accordingly, State Security issued an order to freeze the suspect's funds and other assets totalling of $500,000 USD and 4 KG of gold. The front company's business activity was also suspended. Throughout the investigation, the suspect confessed to providing funds to Daesh (ISIL) and Jabhat Al Nusra to acquire military equipment, including guns and ammunition.

Source: United Arab Emirates

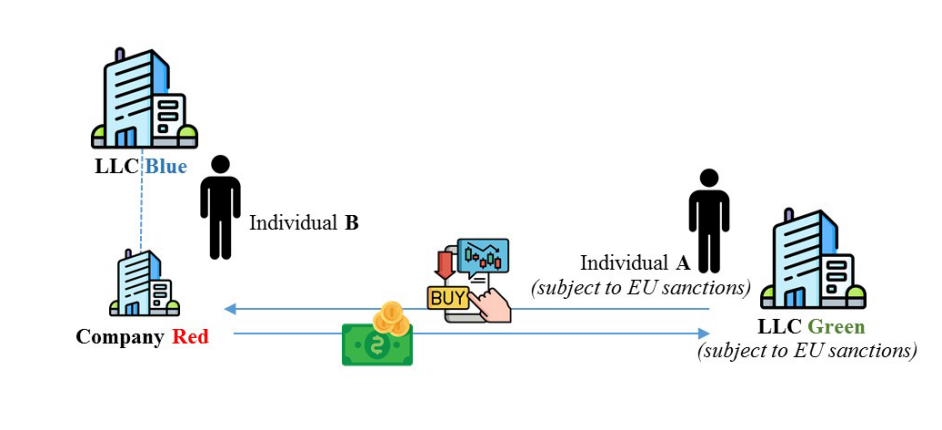
Using Different Types of Legal Persons to Evade Sanctions

72. Some countries reported on the use of subsidiaries and other legal persons to cloud true beneficial owner information. The common tactic included examples of complex schemes to evade sanctions and more straightforward approaches to target sectors without strong AML/CFT/CPF controls.

Box 16. Case Study: Complex scheme to evade EU Sanctions

Individual A, who is subject to EU sanctions, coordinated a complex scheme with Individual B to facilitate the evasion of sanctions. First, Individual B, owner of Limited Liability Company (LLC) Blue, established a subsidiary called Company Red. Second, Individual B used Company Red to acquire Individual A's share in LLC Green. Although LLC Green owns 28.5 million shares in a European company, those shares were frozen because LLC Green was controlled by Individual A. Thus, when Company Red acquired Individual A's share of LLC Green, it also acquired the frozen shares of the European company. In exchange for the sale of LLC Green, Individual A received an equivalent economic benefit.

Individual B facilitated the evasion of sanctions because he and the Russia-based companies (LLC Blue, Company Red, and LLC Green) used this scheme to sell a non-EU company controlled by a listed individual and owning frozen shares of an EU company with the sole purpose to lift the freezing of those shares in the European Union.



Source: European Commission

Box 17. Case Study: Complex ownership structure used to disguise true owner of vehicles

Various shell companies were used to hide the true owner of several luxury vehicles worth several hundred thousand euros. The last company in the chain, an LLC registered in Germany, owned the luxury vehicles. While the LLC's official task was to manage these vehicles, extensive investigations by the Central Office of Sanctions Enforcement were able to prove that the company served exclusively to conceal the vehicles' true ownership.

In fact, the company and thus the vehicles were controlled by a person listed by the EU under the Russian Sanctions Regime. After the investigation uncovered this link between the listed individual and the LLC, the vehicles had to be frozen. Further investigations were able to attribute further assets to the listed person.

Source: Germany

Box 18. Case Study: Use of subsidiary to mask link to UN-designated DPRK entity

Company BETA operates in the construction and public works sector, which includes the supply of heavy machinery, fixed cranes, mobile cranes, excavators, loaders, and lorries to other companies. BETA's main customers are Company GAMMA and several small and medium-sized companies operating in the same sector. The beneficial owner of BETA, Mr. X, and the manager, Mr. Y, are both nationals of DPRK, a country subject to UN sanctions.

Company GAMMA, which operates in the agri-food sector, purchased agri-food machinery from Company BETA. After Company BETA cashed an unusual number of checks exceeding €300,000 (200,000,000 CFA Francs), a financial institution in Senegal conducted customer due diligence investigations, which revealed that the parent company of BETA, based in Pyongyang in DPRK, is on the United Nations 1718 Sanctions List.

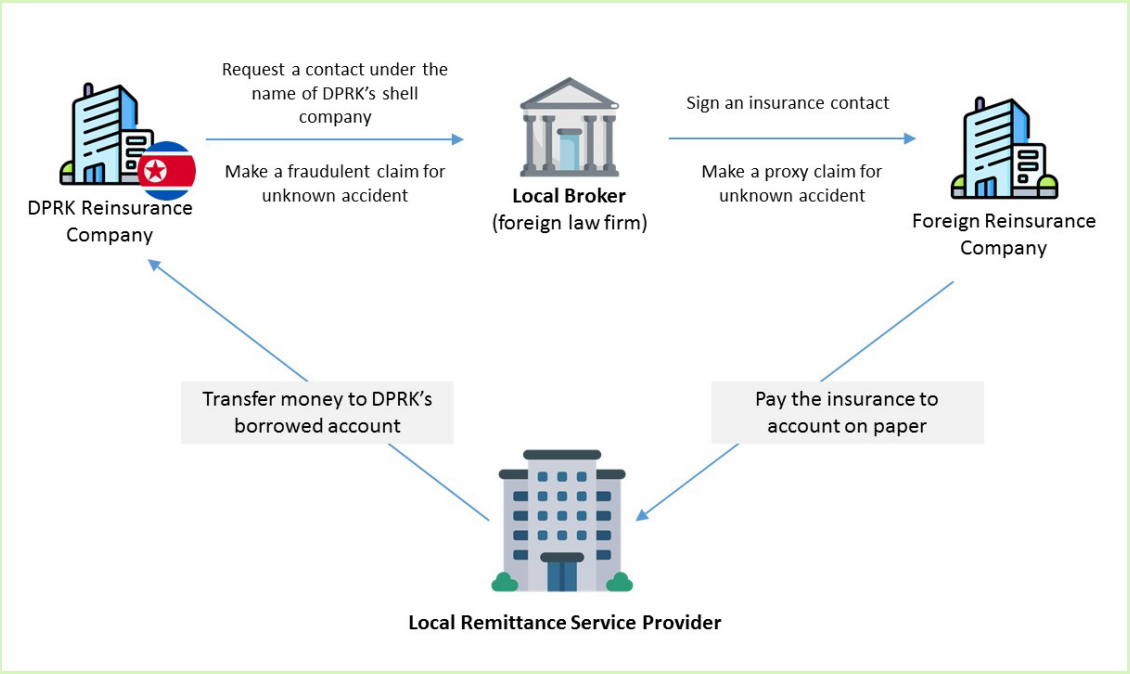
After the link to the sanctioned entity was verified, the financial institution filed a STR with the Senegalese FIU (CENTIF) and Company BETA's assets were frozen. The STR enabled CENTIF to conduct investigations, which did not reveal GAMMA's witting involvement in the sanctions evasion scheme.

Source: Senegal

73. The DPRK has earned millions of dollars annually by fabricating accidents and defrauding the international insurance market. Because there is no way to verify claims in North Korea, DPRK reinsurance companies purchase international insurance or reinsurance for all state infrastructure such as bridges and factories, and then forge

documents to collect insurance money. The DPRK mobilizes shell companies or borrowed accounts in order to sign reinsurance contracts and receive insurance money.[40]

Box 19. Illustrative Example: The DPRK's use of opaque corporate vehicles to commit insurance fraud



Exploitation of Credit and Debit Cards by the DPRK

74. Multiple countries are aware of DPRK-associated individuals increasingly obfuscating their financial profiles using illegally-obtained accounts in the names of Chinese nationals and exploiting virtual assets to make payments and access local currency, enabling DPRK to continue to circumvent UN sanctions.

75. It is suspected that DPRK bankers are fraudulently managing numerous illegally-obtained UnionPay debit cards issued by major China-based commercial banks, in the names of hundreds of domestic account holders to conduct local currency payments. There is an indication this is an attempt to circumvent sanctions by obscuring transactions, links to DPRK while sidestepping countries implementing robust DPRK sanctions regimes to receive profits and purchase proscribed items.

76. The seemingly decentralised nature of these financial networks also reduces the impact of any individual disruption, as well as making it much more difficult for government authorities to identify all of the DPRK's accounts. There are indications that the DPRK is using illegally-obtained UnionPay debit cards to receive deposits of fiat currency derived from stolen cryptocurrencies, as well as coordinating transactions for a range of WMD-related entities.

40 Insurance or/and reinsurance for the DPRK is in violation of Articles 33 and 36 of UNSCR 2270, which prohibits States from providing bulk cash, gold, and insurance service which could contribute to the DPRK's nuclear or ballistic missile programs.

Typology 3: Using Virtual Assets and Other Technologies

77. There has been an increasing trend in the exploitation of the digital economy by sanctioned actors. Virtual assets and other new technologies are being utilised to circumvent international, supranational, and national sanctions regimes and finance WMD actors and activities.[41] Virtual assets are being used to facilitate financial flows:

a) directly to sanctioned countries; and

b) indirectly through intermediary third-party countries that do not apply the sanction measures. Consequently, most countries identify the use of virtual assets and other new technologies by illicit actors as key PF threats/vulnerabilities.

78. More broadly, countries have also identified the sanctions evasion challenges arising from other emerging technologies such as artificial intelligence. However, evidence and trends in this area are too nascent to draw conclusions and few case studies are present.

Regulatory Challenges

79. Notwithstanding efforts to tackle emerging risks related to virtual assets and other technologies, VASPs in many countries lack AML/CFT requirements. As of April 2024, three quarters of FATF Global Network countries were evaluated to be non-compliant or partially compliant with international standards on virtual assets and VASPs.[42] Shortcomings in the regulation and supervision internationally have left the sector vulnerable to abuse by PF networks. As long as there are gaps in implementation of the FATF Standards for virtual assets and VASPs across jurisdictions, PF networks can use VASPs in jurisdictions with weak or non-existent frameworks without detection or disruption. As indicated by the case below, there are also instances of VASPs that are subject to AML/CFT frameworks, failing to comply with applicable requirements.

Box 20. Case Study: Binance Enforcement Action

In November 2023, Binance Holdings Limited ("Binance") pleaded guilty and agreed to pay more than $4 billion to resolve the U.S. Department of Justice's investigation into violations related to multiple sanctions programmes, including failure to register as a money transmitting business, and violations of the International Emergency Economic Powers Act (IEEPA). Binance's founder and chief executive officer pleaded guilty to failing to maintain an effective AML programme, in violation of the Bank Secrecy Act (BSA).

Due in part to Binance's failure to implement an effective AML programme, illicit actors used Binance's exchange in various ways, including conducting transactions that obfuscated the source and ownership of virtual assets; transferring illicit proceeds from ransomware variants; and moving proceeds of darknet market transactions, exchange hacks, and various internet-related scams.

41 During the March 2025 Private Sector Consultative Forum in India, participants emphasised the heightened risks associated with emerging financial technologies, particularly the use of virtual assets in cyber-enabled thefts by state actors, including the DPRK, which uses increasingly more complex and sophisticated methods.

42 https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

Binance users effected transactions with virtual asset exchanges in U.S.-sanctioned countries like Iran without filing SARs/STRs. Binance user wallets effected a significant volume of direct transactions with various Iranian virtual asset exchanges, each worth more than $2,000, and in the aggregate worth the equivalent of over half a billion dollars. This total also includes several transactions with virtual asset wallets associated with sanctioned entities and individuals.

Source: United States

Using Virtual Assets to Move Funds

80. Virtual assets are being used to conceal the movement of funds flowing to sanctioned countries and affiliated actors. Virtual assets can afford a higher level of anonymity to users when paired with certain techniques and are capable of being transferred across borders instantaneously. Additionally, the international nature of virtual assets can present challenges related to verifying jurisdictions in which foreign VASPs are based, time and resources necessary for international cooperation, and differences between regulatory frameworks and sanctions regimes across jurisdictions. In particular, examples presented by countries showed the common use of virtual asset wallets and exchange platforms for potential sanctions evasion.

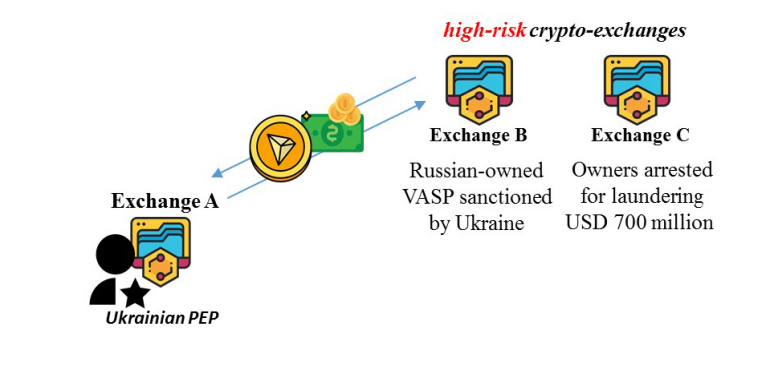
Box 21. Case Study: Funds transferred to nationally sanctioned VASP

As part of a wider study on the use of new technology for money laundering and sanctions evasion, the FIU of Ukraine uncovered the suspicious movement of funds between crypto exchanges, including a domestically-sanctioned VASP.

The FIU found that a crypto-exchange (Exchange A), consisting of companies registered across Europe and other countries (including BVI, Hong Kong, UK, and Estonia), was a recipient of virtual assets from two other high-risk crypto-exchanges (Exchanges B and C). Although, the owner of exchange A was registered as an Estonian national, this case was of interest to the Ukrainian FIU as the owner was considered to be a Ukrainian PEP and son of a Ukrainian politician.

Exchange A was receiving large amounts of funds from exchanges B and C. Exchange B was identified as a Russian-owned VASP sanctioned by Ukraine under its domestic sanctions regime in 2023. Exchange C was identified as a high-risk exchange, whose owners were arrested under suspicion of laundering USD 700 million. The FIU of Ukraine notes that Exchanges B and C transferred virtual assets through the Tron blockchain to Crypto Exchange A to disguise the origin and movement of the funds.

The FIU's findings are currently being considered as part of a pre-trial investigation.



Source: Ukraine

Box 22. Case Study: Using various methods to move funds to the DPRK

In December 2024, South Korea sanctioned one entity and 15 individuals, including Kim Chol Min and Kim Ryu Song, both general managers of the 313 General Bureau located in a neighbouring country, for generating funds, launching cyberattacks, and stealing virtual assets on behalf of the DPRK.[43] With the help of facilitators in the neighbouring country, the DPRK used virtual wallets, banks, e-finance platforms, and other fiat currency accounts to move funds. After converting some of the illicit proceeds to fiat currency, the DPRK sent a large sum of money to Pyongyang and used the fiat currency proceeds from the converted virtual assets for purchasing sanctioned supplies and financing the regime's WMD Programme.

The 313 General Bureau controls the DPRK's research and development and products of weapons and other military equipment. Also, the 313 General Bureau is involved in deploying the DPRK's IT workforce in neighbouring countries and around the world.

Source: South Korea

81. PF and sanctions evasion-related actors are using increasingly sophisticated methods to launder illicit proceeds via virtual assets and obfuscate sources of funds. Countries such as the DPRK are carrying out this activity through anonymity-enhancing technologies, like mixers, purportedly decentralised finance (DeFi) arrangements, cross-chain bridges, as well as VASPs without AML/CFT controls. After laundering funds, the sanctions evasion actors will often convert virtual assets into fiat currency at over-the-counter (OTC) brokers concentrated in certain jurisdictions.[44] In some instances, the DPRK directs OTC brokers to send converted funds to bank accounts held by front companies, which purchase goods on behalf of the DPRK. As noted above, in some instances the DPRK uses illegally-obtained UnionPay debit cards to receive deposits of fiat currency derived from stolen virtual assets.

Box 23. Case Study: Sanction designation of mixers used to launder funds

In November 2023, OFAC designated mixers involved in laundering funds for DPRK, including Sinbad.io (Sinbad).45 Sinbad served as a key money-laundering tool for the Lazarus Group, a DPRK-sponsored hacking group. Sinbad processed millions of dollars' worth of virtual assets that the Lazarus Group had stolen, including through the high-profile heists from Horizon Bridge, Axie Infinity, and Atomic Wallet. Similar to Blender.io, Sinbad operated on the Bitcoin blockchain and indiscriminately facilitated illegal transactions by obfuscating their origin, destination, and counterparties.

Source: United States

43 https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=375771

44 https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

Box 24. Case Study: DPRK criminal prosecution and related enforcement action

In April 2023, the DOJ unsealed two indictments charging a DPRK FTB representative for his role in money laundering conspiracies designed to generate revenue for the DPRK using virtual assets. The individual allegedly conspired with two over-the-counter traders to launder stolen virtual assets and used funds to purchase goods on behalf of the DPRK government in U.S. dollars via Hong Kong-based front companies.

Also, OFAC designated the individual who received tens of millions of dollars in virtual assets in part derived from the DPRK individuals unknowingly hired by U.S.-based companies to provide IT development work. When the IT workers obtain employment, they are known to request to be paid in virtual assets and send most of their salaries through a complicated laundering pattern to funnel these illegally-obtained funds back to the DPRK. After apparently receiving money from IT development workers, the FTB representative directed the OTC virtual asset traders to send payments to front companies, so that those front companies can make payments in fiat currency for goods, such as tobacco and communications devices, on behalf of the DPRK regime. This action is the result of OFAC's ongoing collaboration with the Department of Justice and Federal Bureau of Investigation. The action was also closely coordinated with the Republic of Korea, which designated the same individual for his illicit activities.

Source: United States

VAs and the Generation of Funds

82. Some countries identified that the theft of virtual assets and cyberattacks are used by DPRK to raise funds globally, including for its WMD and ballistic missiles programmes. When carrying out this activity, the DPRK and associated actors commonly target organisations in the blockchain technology and virtual asset industry, including VASPs, DeFi services, blockchain bridge developers, virtual asset trading companies, and venture capital funds investing in virtual assets.

83. In 2024, a UN Panel of Experts report on the DPRK highlighted global cyberactivity on behalf of the DPRK regime, where they were investigating a total of 58 suspected cyberattacks by the DPRK on virtual asset-related companies between 2017 and 2023, valued at approximately $3 billion.[46] According to Chainalysis, DPRK-linked hackers stole approximately $428.8 million from DeFi platforms in 2023, and also targeted centralised services ($150.0 million stolen), exchanges ($330.9 million), and wallet providers ($127.0 million).[47] Countries also highlighted the DPRK's fraudulent deployment of IT service workers to generate funds (in some cases receiving payment in virtual assets) and evade sanctions. DPRK actors use the methods described in the above section to launder proceeds generated in virtual assets.

46 S/2024/215

47 Chainalysis 2024 Crypto Crime Report (Page 44-46) Case Study DPRK's Atomic Wallet exploit.

Box 25. Case Study: Cyber-enabled theft and fraud

In February 2021, the Department of Justice charged three DPRK computer programmers with participating in a wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks, to steal and extort more than $1.3 billion of money and cryptocurrency from financial institutions and companies, to create and deploy multiple malicious cryptocurrency applications, and to develop and fraudulently market a blockchain platform.

The indictment alleges that the three defendants were members of units of the Reconnaissance General Bureau (RGB), a military intelligence agency of the DPRK, which engaged in criminal hacking[48]. These DPRK military hacking units are known by multiple names in the cybersecurity community, including Lazarus Group and Advanced Persistent Threat 38 (APT38).

The indictment alleges a broad array of criminal cyber activities undertaken by the conspiracy, in the United States and abroad, for revenge or financial gain. The schemes alleged include creation and deployment of malicious cryptocurrency applications; targeting of cryptocurrency companies and theft of cryptocurrency; spear-phishing campaigns; and marine chain token and initial coin offering.

According to the allegations contained in the indictment, the three defendants were members of units of the RGB who were at times stationed by the DPRK government in other countries, including China and Russia. While these defendants were part of the RGB units that have been referred to by cybersecurity researchers as Lazarus Group and APT 38, the indictment alleges that these groups engaged in a single conspiracy to cause damage, steal data and money, and otherwise further the strategic and financial interests of the DPRK.

The Departments of the Treasury and Justice also acted against two Chinese nationals who were charged with laundering over $100 million in cryptocurrency from a hack of a cryptocurrency exchange. According to the pleadings, in 2018, DPRK co-conspirators hacked into a virtual currency exchange and stole nearly $250 million worth of virtual currency. The funds were then laundered through hundreds of automated cryptocurrency transactions aimed at preventing law enforcement from tracing the funds. The pleadings further allege that between December 2017 and April 2019, the two defendants laundered over $100 million worth of virtual currency, which primarily came from virtual currency exchange hacks. OFAC designated the two individuals for having provided material support to the Lazarus Group.

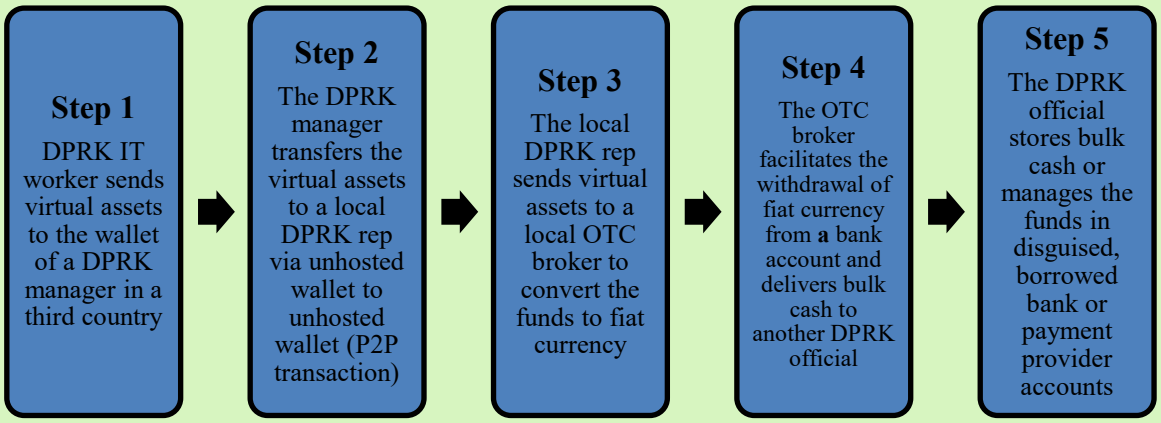
Source: United States

84. Additionally, the DPRK has dispatched thousands of highly skilled IT workers around the world to generate revenue, which contributes to its WMD and ballistic missile programmes. These IT workers take advantage of existing demands for specific IT skills, such as software and mobile application development, to obtain freelance employment contracts from clients around the world, including in Asia, Europe, and North America. In many cases, DPRK IT workers represent themselves as internationally based and/or non-DPRK teleworkers. The DPRK IT workers who obtain the projects using the facilitator's

48 On the UNSCR 1718 List, RGB is designated as KPe.031.

identity may further obfuscate their identities and/or location by subcontracting the projects. The money is sent back to the DPRK using various methods to evade sanctions, including through the use of intermediaries and by obscuring BOI (see Typologies 1 and 2). Virtual assets are also used to remit the funds to the DPRK.

Box 26. Illustrative Example: Process for moving DPRK IT worker's illicit funds



Foreign Entities and Individuals Committing Fraud to Hide Lucrative Business with DPRK IT Workers

85. Additionally, DPRK IT workers also coopt foreign individuals and companies to further mask their involvement in sanctions evasion schemes to make money. In one of the below case studies, Japanese companies were targeted by the DPRK-associated IT workers to raise and move funds. In the other case study, a U.S. national participated in a scheme that included money laundering and identity theft to support DPRK IT workers.

Box 27. Case Study: Fraud schemes to mask lucrative business relationships with DPRK IT Workers

In March 2024, a South Korean national who was the president of an IT-related company and a former employee were arrested for fraud and other crimes. During the investigation, it was found that the suspects had falsified records and asked DPRK IT workers believed to be located in China to develop applications ordered by a Japanese company through an online platform. This alleged activity was suspected to be in support of a scheme to evade sanctions, as those funds could be used for the DPRK's WMD programme, which violates UNSCR 1718.

In September 2024, two Japanese individuals were arrested for conspiring with an alleged DPRK IT worker to use a prohibited "automatic trading system" to conduct FX transactions, and for illegally registering in the customer database and opening accounts. The suspects are suspected of remitting funds obtained through these illegal FX transactions to North Korea.

Source: Japan

Box 28: U.S. Justice Department disrupts DPRK remote IT worker fraud schemes through charges and arrest of Nashville facilitator

In August 2024, DOJ unsealed an indictment charging a U.S. national with conspiracy to launder monetary instruments and several other crimes to generate revenue for the DPRK illicit weapons programme, which includes WMD. According to court documents, the defendant participated in a scheme to assist overseas IT workers to obtain remote IT work at U.S. companies, which believed that they were hiring U.S.-based personnel. The IT workers, who were DPRK nationals, used the stolen identity of a U.S. citizen to obtain this remote IT work.

According to court documents, the defendant ran a "laptop farm" at his Nashville residences between approximately July 2022 and August 2023. The victim companies shipped laptops addressed to "Andrew M." to the defendant's residences. Following receipt of the laptops, the defendant downloaded and installed unauthorised remote desktop applications, and accessed the victim companies' networks, causing damage to the computers. The remote desktop applications enabled the DPRK IT workers to work from locations in China, while appearing to the victim companies that "Andrew M." was working from the defendant's residences in Nashville.

The overseas IT workers associated with the defendant's laptop farm were paid over $250,000 for their work between approximately July 2022 and August 2023, much of which was falsely reported to the U.S. Internal Revenue Service and the Social Security Administration in the name of the actual U.S. person whose identity was stolen. The defendant and his conspirators' actions also caused the victim companies more than $500,000 in costs associated with auditing and remediating their devices, systems, and networks. The defendant and others conspired to commit money laundering by conducting financial transactions to receive payments from the victim companies, transfer those funds to the defendant and to accounts outside of the United States, in an attempt both to promote their unlawful activity and to hide that transferred funds were the proceeds of it. The non-U.S. accounts include accounts associated with DPRK and Chinese actors.

Source: United States

Typology 4: Exploiting the Maritime and Shipping Sectors

86. As defined by the International Maritime Organisation (IMO), the *shadow fleet* or *the dark fleet* refers to "[…] ships engaging in illegal operations for the purposes of circumventing sanctions or engaging in other illegal activities […]."[49] The maritime sector has become a primary target used by illicit actors, leveraging its complexity, international reach, anonymity, and limited AML/CFT/CPF controls. The maritime industry involves a vast network of vessels, ports, logistics, and international regulations that illicit actors can exploit to evade sanctions and generate revenue that can contribute to PF. While the FATF Standards do not cover the maritime sector, a number of countries identified the use of this sector as a key vulnerability in their national PF risk assessment. To this end, various aspects and activities of the maritime sector are potentially exposed to sanctions evasion

[49] International Maritime Organisation, "Urging Member States and All Relevant Stakeholders to Promote Actions to Prevent Illegal Operations in the Maritime Sector by the "Dark Fleet" or "Shadow Fleet," (Dec. 6, 2023). A 1192 33

and PF risks, including maritime insurance arrangements, maritime companies, open registries, commodity traders, and dual-use goods manufacturers.[50]

87. Illicit actors can employ a range of deceptive shipping tactics to disguise the vessel, its origins or designation, obscure the true nature of their activities, and evade detection. While there is overlap in techniques, tactics can be divided into four main categories: vessel identification, ship-to-ship transfers, disabling or disguising AIS broadcasts, and falsifying documents. However, it is important to note that illicit actors attempting to conduct PF and sanctions evasion schemes can employ more than one tactic to achieve their goals.

Altering Vessel Identification

88. As discussed in Typology 2, illicit actors can obscure beneficial ownership information to circumvent sanctions regimes and access the formal financial system. In the maritime sector, illicit actors can physically alter merchant vessels to pass as different vehicles and obscure their identity to conceal their true ownership and activities. For example, a vessel's physical identity can be tampered by painting over vessel names, using alias flags, and altering its unique IMO ship identification number. By physically altering merchant vessels and obscuring their identity, illicit actors acquire anonymity, and they can mask a ship's history of illegal activities. The case study below highlights an example of a vessel altering its identification to circumvent United Nations Security Council resolutions on the DPRK.

50 To assist members' preparation for mutual evaluations and to respond to emerging regional risks, the APG Secretariat, with support from the United Nations Office on Drugs and Crime, published a Shipping Registries and PF Risk Factsheet: Asia / Pacific Group On Money Laundering

Box 29. Case Study: Revenue generation through illicit coal in the maritime sector

In 2022, Indonesian authorities patrolling Indonesian waters detained Petrel 8. In 2017, Petrel 8, a bulk carrier under the flag of Comoros, was added to the UN Sanctions List for transporting illicit coal to the DPRK. The case involved the coordination of Indonesian authorities with the UN 1718 Sanction Committee. The Indonesian Ministry of Foreign Affairs (MOFA) requested information from the Indonesia FIU (PPATK), which led to the detection of the case through international cooperation.

The investigation revealed that PT Lintas Bahari Nusantara, an Indonesian shipping corporation, had purchased the vessel from a Japanese company, UYO Co. Ltd, for an estimated 500,000 Yen, with financing providing by Bank BCA. Although the initial investigation did not identify any direct financial links to DPRK, the vessel's detention was a result of its involvement in ongoing sanctions evasion for the DPRK. Methods such as tampering with the vessel's identity and using alias flags were utilised to evade detection. The vessel was purchased for approximately Rp61 Billion (USD 4 million) and it was used for transporting coal to DPRK. The acquisition of the Petrel 8 entailed the transfer of funds from an Indonesian company to a Japanese firm.

The case highlighted vulnerabilities in the surveillance of vessel ownership changes and illicit trade practices, emphasizing the need for enhanced international cooperation to prevent sanctions evasion. Following discussions with the UN 1718 Sanctions Committee in 2023, the decision to scrap the Petrel 8 was deemed the most effective solution to prevent further sanctions evasion activities.

Source: Indonesia

Ship-to-Ship Transfers

89. The process of ship-to-ship transfers occurs when goods are moved between vessels in open waters. While ship-to-ship transfers can be a legitimate practice, the practice is identified as high-risk for sanctions evasion as illicit actors can employ the method with the intent of disguising the origin or destination of shipments. This makes it harder for governmental authorities to track sanctioned goods and identify violations of international sanctions. Further, the lack of transparency may cause maritime insurers to unwittingly provide shipping insurance to vessels involved in illicit ship-to-ship transfer activities.

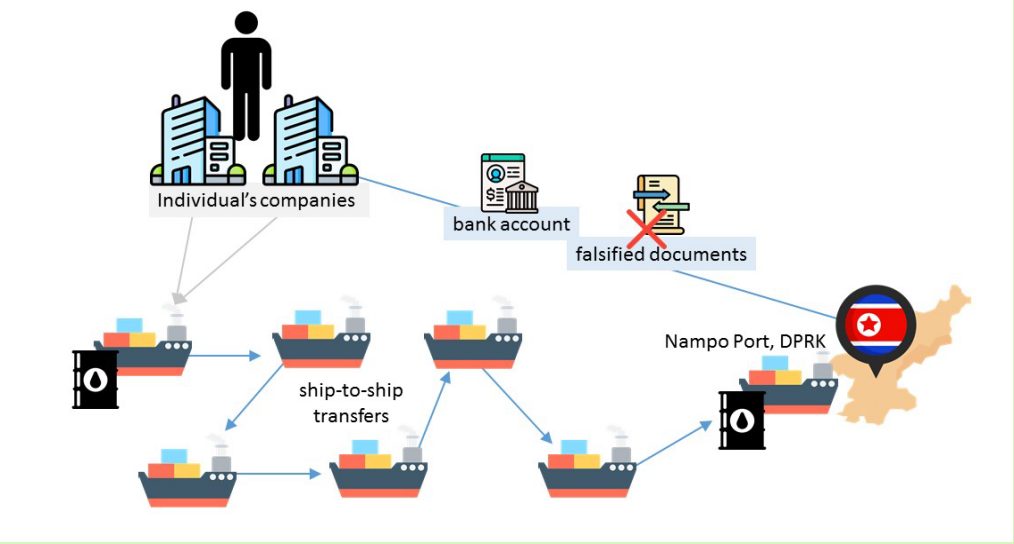
90. As reported by one jurisdiction, the DPRK operates a fleet of a minimum 28 tankers capable of engaging in ship-to-ship transfers of refined petroleum products, and at least 33 ships that are capable of transporting coal. Ship-to-ship transfers conducted by the DPRK are often cash transactions that do not occur through financial institutions, highlighting an additional vulnerability relevant to PF and sanctions evasion risk. The case studies below detail how illicit actors can employ ship-to-ship transfers to move prohibited items, circumvent sanctions, and mask the true origin or destination to avoid detection.

Box 30. Case Study: Exploiting maritime sector to supply gasoil to the DPRK

In late 2019, an individual allegedly conspired with five other individuals abroad to supply approximately 12,260 metric tons of gasoil to the DPRK using the vessel, MT Courageous, on seven occasions. The supplies were facilitated through ship-to-ship transfers on the first six occasions, with the final transfer occurring at the Nampo Port in the DPRK. The alleged actions are in violation of Singapore's UN DPRK Regulations and the UNSCR 1718 Sanctions Regime.

To facilitate payments for the purchase and supply of gasoil to the DPRK, the individual is accused of utilizing the bank account of a company, of which he was a director, on four occasions. The individual also allegedly falsified documents belonging to the company on two occasions, and allegedly utilised the bank account of another company under his control to receive payments for the prohibited supply of gasoil to the DPRK, on five occasions. Furthermore, the accused allegedly lied to the investigation officer, disposed of evidence, and failed to inform police about the supply of gasoil to the DPRK by another vessel in February 2019.

Consequently, the accused faces multiple charges, including supplying prohibited items to the DPRK, falsifying accounts, acquiring benefits from criminal conduct, obstructing justice, and failing to disclose a prohibited transaction. Additionally, the first company of which the accused was a director has been charged with four counts of transferring financial assets that may contribute to a prohibited activity in contravention of Singapore's UN DPRK Regulations and the second company faces five counts of acquiring benefits from criminal conduct. Court proceedings are ongoing.



Source: Singapore

Box 31. Case Study: Transfer of oil to DPRK ships on the high seas

From January 2017 to October 2022, Chinese Taipei prosecutors investigated 11 cases involving violations of sanctions by DPRK.[51] The most common typology involving PF is the transfer of oil to DPRK ships on the high seas from third-jurisdiction ships controlled by Chinese Taipei oil companies, or transfer of oil to ships owned by third-party jurisdictions who resell it to DPRK ships.

Petroleum products are still the most common commodity traded by Chinese Taipei individuals in breach of UN sanctions. Under local law, it is legal to transact oil trade on the high seas. Representatives or beneficial owners of shipping companies, including foreign nationals, other intermediaries and involving complex business structures, broker ostensibly legal trades to disguise illicit transfer of oil via ship-to-ship transfers at sea. False export information is also utilised and offshore companies and accounts used to frustrate funds tracing.[52]

Source: Chinese Taipei

Disabling and Manipulating Automated Identification System Broadcasts

91. The Automated Identification System (AIS) is a coastal tracking system used on vessels to provide identification and position information, allowing authorities to track movement.[53] Illicit actors can manipulate data transmitted via AIS broadcasts, which can include altering vessel names, IMO numbers, or other unique identifying information, to help conceal a vessel's voyage. Further, shadow fleets often disable the AIS broadcast, effectively "going dark" and suspending the tracking of movement.[54]

92. As reported by countries, and reflected in UNSCR 2397 (2017), DPRK-flagged, controlled, chartered, or operated vessels are intentionally disabling or manipulating AIS transponders to evade UN sanctions, and generate revenue that has historically contributed to the country's WMD and ballistic missile programmes[55]. The case study below details two separate incidents of the detection, seizure, and confiscation of DPRK-origin coal found on civilian vessels, in violation of UNSCRs related to the DPRK.

51 Five cases resulted in convictions, three were found not guilty, and three did not proceed to prosecution.

52 The subjective element of Article 9, Paragraph 1, Subparagraph 1 of the Counter-Terrorism Financing Act requires a suspect to "knowingly" trade with the sanctioned target, and the intervention of intermediaries has made this element difficult to prove.

53 International Maritime Organisation, "REVISED GUIDELINES FOR THE ONBOARD OPERATIONAL USE OF SHIPBORNE AUTOMATIC IDENTIFICATION SYSTEMS (AIS)," (Dec. 2, 2015). A 1106 29

54 The IMO mandates AIS usage for all vessels over 300 gross tones that are engaged in international voyages, as well as all passenger ships, regardless of size.

55 UNSCR 2397

Box 32. Case Study: The detection, seizures, and confiscation of DPRK-origin coal on vessels

In two separate incidents, Cambodia uncovered the DPRK using civilian vessels to assist in the export of coal, in violation of UNSCRs 2397 and 2375, which prohibit such activities. In both cases, the vessels and their cargo were confiscated, and individuals were found guilty of (1) illegally entering Cambodia and (2) attempting to smuggle goods in the custom area of Cambodia.

In accordance with UN obligations, Cambodia routinely investigates and examines properties and vessels entering from the high seas for potential violations of UN sanctions related to the DPRK. Sometimes, vessels use obfuscation techniques to disguise the origin of their cargoes, such as turning of their Automatic Identification System (AIS) to obscure the goods onboard, spoofing their location, or conducting ship-to-ship transfers. Two recent vessels seizures display the tactics used by DPRK vessels to mask the origin of its illicit cargo.

In the first case, a motor vessel (M/V) HJL was seized by Cambodian authorities in February 2024. After the foreign-registered vessel approached DPRK waters, the vessel turned off the AIS broadcast. The next day, the vessel's AIS broadcasted a position that indicated the HJL was anchored, even though the vessel was still underway under a false name. After HJL entered Cambodian territorial waters, Cambodian authorities seized the vessel with assistance from another jurisdiction sharing information on a suspicious vessel. This international cooperation led to the seizure of the HJL, which was carrying 12,000 tons of coal ore originating from the DPRK. The ship entered Cambodian territorial waters to anchor purportedly where it would meet its buyers. Following Standing Orders and due to the content onboard, the Prosecution Office froze the vessel and its cargo for further investigation and trial.

In the second case, in May 2024, Cambodian Authorities seized M/V CNI after the vessel conducted a ship-to-ship transfer with a DPRK vessel in DPRK waters involving UN-prohibited cargo, including 4,800 tons of coal ore. Further investigations found that the shipment was arranged by a logistics company in a third country, and that the company arranged to import DPRK-origin coal ores but conceal its origin through falsified documents.

Source: Cambodia

93. The vulnerabilities demonstrated by the two cases above highlight the need for countries to consider increasing surveillance frequencies and patrolling force presence, and enhancing tracking systems in territorial waters, specifically those with geographic proximity to international waters.

Falsifying Documents

94. Additional tactics to obscure the origin or destination of cargo is the use of false documentation when transporting commodities originating from or destined to the DPRK, especially for exports of dual-use goods. In this case, illicit actors alter transport documents for a shipment after departure, thereby concealing the actual final destination of goods. This practice generally involves a shell company in a third country, controlled more or less directly by the proliferating entity. In appearance for the customs authorities and the shipper, the shell company is the official consignee of the cargo. However, once the goods

are shipped, the sponsor makes a change to the transport documentation, enabling the shipment to be redirected to a PF-associated high-risk jurisdiction.

95. In addition to the practice of falsifying documenting involving the DPRK, this is a common tactic to evade sanctions and export controls elsewhere. The case studies below highlight how illicit actors can manipulate transport documents early in the shipping process to disguises the export of dual-use goods.

Box 33. Case Study: Forging Bills and False Declarations of Dual-use Shipments

During the permit-approval process in 2021, Federal Authority for Nuclear Regulation (FANR) identified a suspicious shipment that contained a dual-use goods. Company X, based in a UAE free zone, had submitted three permits to export inverters valued at approximately US$25,000 (95,040 AED). The inverters were listed in the UAE Export Control List and classified as a dual-use goods. The documents submitted by Company X included a bill of lading and a bill of sales and purchase (BSP), which had conflicting information on the seller's information and the origin country of the shipment. The documents specified that these items were destined for a high-risk country.

LEAs investigations identified that Company X submitted a forged bill of lading, which declared itself as the shipper, while the BSP identified the seller as another company located in Country T. LEAs also determined, following additional investigations, that the purported seller primarily trades in nuts and thus that its business was not consistent with the trade transaction. Further investigations uncovered that the items were in fact imported by the seller from Country H to the UAE. Company X also provided forged documents of having multiple branches in Country U to mislead the authorities and evade sanctions imposed on the Iran nuclear programme.

LEAs conducted a criminal and financial investigation in cooperation with the UAEFIU, CBUAE, EOCN, Federal Customs Authority & FANR. A physical inspection of Company X's premises determined that it was operating as a front for the buyer of the inverters, located in a high-risk country. The UAEFIU and CBUAE identified and froze three bank accounts with a total balance of 34,000 AED (USD 9500) related to Company X. Furthermore, Customs provided LEAs with all identified forged documents related to sub-contracted import / export parties attempting to obscure BO.

FANR has prepared a technical report about the shipment and provided LEAs confirmation that the item is a dual use goods listed in the UAE Export Control List. Customs authorities seized the shipment and LEAs ordered a freeze on the shipment (95,040 AED (USD 26000)).

Source: United Arab Emirates

Box 34. Case Study: Non-declaration of dual use goods under the prescribed export laws of the exporting country

In 2020, Indian custom authorities seized an Asian-flagged ship bound for Pakistan. During an investigation, Indian authorities confirmed that documents mis-declared the shipment's dual-use items. Indian investigators certified the items for shipment to be 'Autoclaves', which are used for sensitive high energy materials and for insulation and chemical coating of missile motors. The sensitive items are included in dual-use export control lists of the Missile Technology Control Regime, India, and other jurisdictions.[56]

The Bill of Lading of the seized cargo provided evidence of the link between the importer and the National Development Complex, which is involved in the development of long-range ballistic missiles.

Source: India

[56] Export of such equipment without formal approval from various authorities is a violation of existing law and covenants.

5. Section 3. Challenges and Good Practices in Mitigating Risks Relevant to PF

Detection Through SARs/STRs and Sanctions Screening

96. To detect PF and sanctions evasion methods, countries rely heavily on SARs/STRs obligations and robust sanctions screening matches. To complement these techniques and effectively identify and address illicit activity on a global scale, other detection methods include sharing cross-border intelligence, interagency coordination, international cooperation, and monitoring tools including open-source intelligence and blockchain analysis.

97. Many countries reported relying upon robust SARs/STRs obligations for the detection of PF and sanctions evasion schemes to identify and combat complex and evolving tactics. Varying domestic legal frameworks and reporting obligations may mandate reporting entities to submit SARs/STRs as it pertains to PF and sanctions evasion more broadly. Multiple countries note that the scope of reporting entities' obligations may include conducting thorough customer due diligence, complying with provisions of laws and regulations, monitoring of transactions involving high-risk countries, and fulfilling all SARs/STRs obligations when suspicious transactions are identified.

Good Practices for Detecting PF and Sanctions Evasion Through SARs/STRs and Sanctions Screening

98. In addition, several countries require reporting entities to integrate automated sanctions screening systems in reporting entity obligations, including related to internal policies and procedures, to improve the effectiveness of SARs/STRs. International and/or national sanctions lists are integrated into sanctions screening systems, whereby reporting entities can find matches to individuals or entities and use keywords as it pertains to high-risk transactions and sanctioned individuals, entities, or activities. In some countries, a positive match found during screening can trigger further obligations for reporting entities to submit SARs/STRs and inform authorities about frozen assets under sanctions or transactions tied to sanctioned entities. The below two case studies show how SARs/STRs were used to initiate investigations.

Box 35. Case Study: Negative news screening and SARs/STRs detect illicit purchase of dual-use goods

Two French companies acted as intermediary to purchase U.S.-origin dual-use electronic components, which were re-sold through a series of entities to a U.S.-sanctioned company in Russia.

The case was detected through French authorities working with the private sector, using the monitoring of negative news related to Russia and SARs/STRs from banks following TracFin's issuance of a "call for vigilance" targeting a relevant individual and entities (the UBO of the entities). TracFin's publication also pointed at the individual's wife, who was appointed manager of one of the entities less than a month before her husband was designated as an OFAC SDN.

The investigation required strong interagency cooperation and successful partnership with financial institutions, including a regular follow-up with involved banks to avoid any capital flight and ensure the existing funds were effectively unavailable during the investigation.

Source: France

99. Several countries have invested in training, outreach, specialised guidance, and monitoring mechanisms through public- private partnerships to bolster compliance and enhance detection capabilities. To this end, the publication of advisories, guidance, or nationally or internationally identified indicators can help reporting entities detect suspected sanctions evasion and PF activity and submit specific SARs/STRs to meet their obligations. Some countries have also enacted domestic legal frameworks that require regulated entities to file SARs/STRs based on these advisories or alerts, further enhancing detection capabilities.

Box 36. Case Study: Issuing detailed alerts to make it easier for FIs to file SARs/STRs

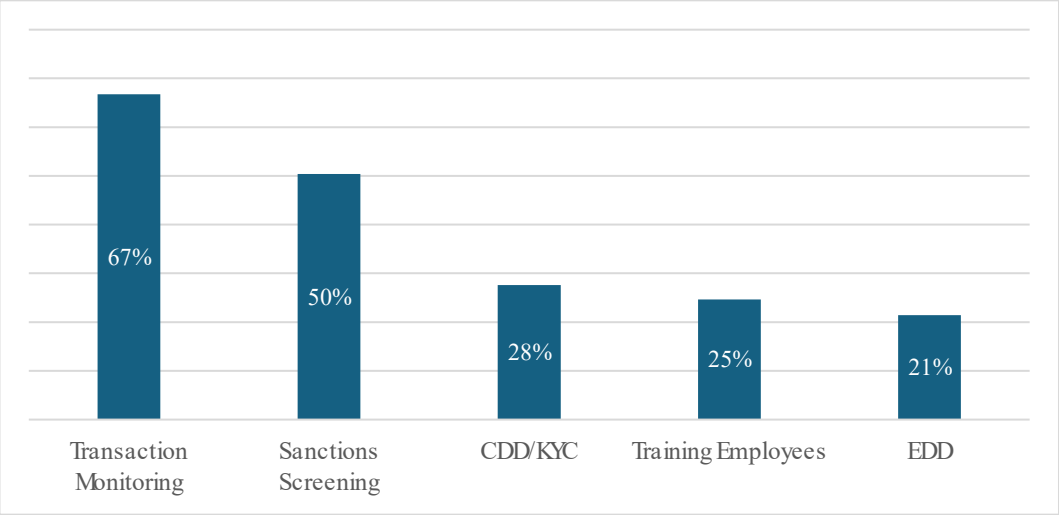
To make it easier for financial institutions to file SARs/STRs related to evasion of U.S. export controls related to Russia and Belarus, BIS and FinCEN issued a 2022 joint alert that provided financial institutions with an overview of BIS's current export restrictions; a list of commodities of concern for possible export control evasion; and select transactional and behavioural red flags to assist financial institutions in identifying suspicious transactions relating to possible export control evasion. The alert also requested FIs use the key term "FIN-2022-RUSSIABIS" when filing SARs/STRs.

Expanding on that alert, BIS and FinCEN issued a joint alert in November 2023 highlighting red flags relating to global evasion of export controls. This alert requested FIs use the key term "FIN-2023-GLOBALEXPORT" when filing SARs/STRs. FIs have submitted more SARs/STRs with the Russia-related key term than the global export key term, mainly because the export restrictions imposed on Russia and Belarus are broader and easier for FIs to identify potentially related financial transactions in the information they receive.

Source: United States

100. According to most private sector entities that responded to the FATF's public consultation, the best ways to mitigate risk related to sanctions evasion and PF are linked to key AML/CFT preventive measures like customer due diligence, comprehensive assessment of risks, sanctions screening tools, ongoing monitoring that may lead to the filing of SARs/STRs, training employees, policies and procedures, negative news screening, and enhanced due diligence (EDD) (see Figure 3 for good practices most cited by the private sector). Also, trade-based money laundering preventive measures, real-time alerts, and advanced technology solutions were cited as important. However, in the absence of robust information sharing mechanisms, it may be difficult for the private sector to detect complex PF and sanctions evasion schemes through standard risk management processes.

Figure 3. Good Practices for Detecting Sanctions Evasion



Challenges Detecting PF and Sanctions Evasion through SARs/STRs and Sanctions Screening

101. Nearly one-third of countries did not report the use of SARs/STRs as a method for detecting PF. Because a notable number of countries do not criminalise PF, this may explain why some countries do not rely on SARs/STRs to an extent. Countries that do not treat PF as a criminal offense may be less likely to require reporting entities to identify PF in SARs/STRs. In turn, reporting entities may file SARs/STRs involving PF actors, but the vital information linking them to PF activities may be absent without further guidance on the complex nature of detection for this illicit activity.

102. Also, integrating sanctions lists into national SARs/STRs frameworks and utilizing screening tools can play a central role in the detection of suspected PF and sanctions evasion. Some countries noted challenges with sanction screening matches as they experienced false positive matches to individuals/entities or irrelevant information based on generic keyword searches. Also, because multiple identifiers are required to be matched, including dates of birth, names, aliases, multiple versions of names, phonetic and spelling differences in names, and passport numbers, the matching algorithms can be prone to detection of false positives. However, mitigation measures can include EDD, utilizing open-source intelligence such as company registries or BOI, and corroborating information with other databases.

103. Countries reported another challenge regarding the low level of understanding and compliance with PF obligations among designated non-financial businesses and professionals (DNFBPs). Many of DNFBPs entities are unaware of their responsibilities in monitoring and reporting PF-related activities.[57] In some countries, this may make it difficult for authorities to detect PF activities in sectors outside of financial institutions. However, private sector entities across sectors reported a lack of public sector feedback on relevant SARs/STRs, which may make it harder to address this challenge.

[57] See Section Two, Mitigation of PF Risks, in the 2021 FATF PF Guidance for more information on risk mitigation measures by FIs, DNFBPs, and VASPs.

Other Detection Methods

104. To complement SARs/STRs and sanctions screening matches, other detection methods include cross-border intelligence, information sharing through interagency coordination and international cooperation, and monitoring tools. It is important to note that countries will often integrate multiple detection sources to form a comprehensive view of illicit finance and evasion schemes.

105. Many countries report that customs authorities and cross-border intelligence play a pivotal role in the detection and investigation of PF-related activities, especially the linkages to high-risk countries and trade routes. Customs agencies collaborate with regional and international bodies, and can exchange information on investigations, customs declarations, import/export data, and licensing applications to improve detection and investigate potential violations related to sanctions evasion from proliferation financers. This exchange improves detection capabilities and aids in investigating potential violations. In particular, key activities in this area include the analysis and monitoring of foreign trade operations and the movement of goods, including the flow of assets to high-risk countries, defence materials, and strategic and dual-use goods. Intelligence sharing, coupled with jurisdictional regulatory frameworks to ensure compliance, highlights the critical role customs authorities play in detecting potential violations related to PF and sanctions evasion.

Good Practices Detecting PF and Sanctions Evasion through other Detection Measures

Interagency Coordination

106. Most countries highlighted the importance of interagency coordination in the detection of PF and sanctions evasion. Specifically, LEA investigations and information exchanges with other competent authorities can result in case referrals from domestic agencies, joint investigations, and awareness-raising, which can help identify the financial flow of funds and/or assets of designated persons and entities. Intelligence gathering, complemented by investigative work, is a multi-disciplinary approach to identify and detect suspected cases of PF and sanctions evasion.

Box 37. Case Study: Interagency coordination on controlled dual-use goods exportation

In 2017, FINTRAC received voluntary information from Canadian law enforcement indicating that a Canadian electronics company was suspected of being involved in the shipping of controlled dual-use integrated circuits.

The SARs/STRs indicated that the company's transactional activity was consistent with some of the key attributes indicative of the Russian and Eastern European Laundromat Schemes. One SAR/STR indicated:

- Funds originated from high ranking individuals;
- Individuals located in countries like Russia, Azerbaijan, as well as other Eastern European countries;
- High ranking individuals opened shell companies for the purpose of laundering funds;
- Shell companies registered in tax haven countries;
- Funds remitted via shell companies in tax haven countries.
- That the company received electronic funds transfers from possible intermediary countries for the transshipment of dual-use goods or other illicit financial activity (including several European countries). In some instances, the country of origin did not match the listed address for the entities responsible for ordering the electronic funds transfers. Additionally, the company was the beneficiary of electronic funds transfers ordered by individuals and entities with addresses listed in Russia.

The SAR/STR noted that the company's funds were depleted through multiple outgoing cheques to shareholders, and through outgoing electronic funds transfers to an online payment processing company.

When asked about the impact of FINTRAC's intelligence disclosures pertaining to the company, Canadian law enforcement indicated that the disclosed information triggered a new investigation and provided them with additional and unknown subjects. They specified that FINTRAC's disclosures and collaboration were key factors in their understanding of the networks involved and of the overall enforcement success of their cases. They added that the information provided by FINTRAC contributed to the seeking of formal indictments in a partner country.

Source: Canada

107. In addition, some countries highlighted that the publication of guidance products, which may include trends, typologies, and indicators, is essential in the detection of suspicious activity (see section on domestic coordination and collaboration).

International Cooperation

108. Given the global nature of PF and sanctions evasion, international cooperation through intelligence and information sharing is a major instrument in detection and prevention. Effective detection measures require a coordinated approach between domestic authorities and international partners. For instance, FIUs can pursue information sharing through the Egmont Group, which plays a pivotal role in facilitating information sharing between FIUs, enhancing the detection of suspicious financial activity related to PF

or sanctions. In addition, international cooperation can assist countries in systematically analyses risks associated with the international trade movement, which can help strengthen national risk profiles.

Monitoring Tools

109. Monitoring tools also play an important role in the detection of PF and sanctions evasion. These tools leverage a variety of data sources including open-source intelligence, and sophisticated blockchain analysis techniques. Competent authorities can utilise open-source intelligence to access a wide range of information, which can include corporate registries, beneficial ownership information, satellite imagines, and geospatial data, which can unveil networks of illicit actors.

110. Several countries also noted blockchain analysis tools help to detect sanctions evasion and PF activity. The use of virtual assets can create an additional layer of complexity to detection, but transactions in virtual assets that operate on public blockchains can be traced. Blockchain analysis allows competent authorities to monitor and trace the flow of funds, identify suspicious activity, and mitigate some obfuscation efforts in virtual assets. For more information, please see Typology 3 (Using Virtual Assets and Other Technologies).

Challenges Detecting PF and Sanctions Evasion through other Detection Measures

111. Countries reported several challenges in detection, including jurisdictional differences in sanctions programmes and the related diverging lists of sanctioned entities, national legal requirements, and various enforcement regulations. Another key challenge is the DPRK's use of diplomatic personnel to facilitate the provision of financial services or transfer of sanctioned assets or resources, including transporting bulk cash. The DPRK relies on the use of diplomatic immunity to avoid controls and investigative measures. Many countries are concerned about inconsistent collection and/or availability of beneficial ownership information, which further complicates the detection of PF and sanctions evasion (see Typology 2 and the Vulnerabilities Section for more information).

Investigation and Prosecution

112. Since the publication of the FATF's report *Combating PF: A Status Report on Policy Development and Consultation* in 2010[58], legal frameworks for preventing and combating PF and sanctions evasion may have been strengthened considerably, but examples of effective investigations and prosecutions remain scarce in 2025. As described in the 2010 FATF report, the difficulty in prosecuting PF cases was attributed to several challenges, including: non-criminalisation of PF; gathering evidence in PF cases; the international nature of PF activities; the use of financial intermediaries to mask illicit activities; ineffective frameworks for export control; lack of a universally accepted definition of WMD PF; and differences in jurisdictional approaches to the topic, including international cooperation. Based on submissions from the FATF Global Network, many of the same core challenges appear to remain impediments to the successful investigation and prosecution of complex PF (and sanctions evasion) cases.

58 COMBATING PROLIFERATION FINANCING

Investigative Techniques and Mechanisms

Good Practices in PF Investigations

113. Many countries reported that effective PF and sanctions evasion investigations depend on the use of standard procedures for financial crime cases and collaborative work involving relevant interagency partners. SARs/STRs are a key input for identifying and understanding unusual patterns in financial activities. The use of SARs/STRs also assist in revealing the links between businesses and individuals involved in sanctions evasion and illicit activities.

114. Some countries reported that another important investigative tool is the tracking of virtual assets, which are sometimes used to avoid detection. Investigators can follow the money through blockchain analysis, even if the amounts are small, uncovering financial patterns and connections to relevant entities and individuals.

115. Advanced analytics play an important role in combating PF by finding patterns and unusual activities in financial data. These tools can help investigators discover links between entities and identify networks of people or businesses involved in sanctions evasion. For example, advanced analytics support link analysis, which connects accounts, transactions, and parties to show how illegal networks operate. Real-time monitoring tools make it possible for authorities to act quickly when suspicious activities are detected. Combining data from different sources, like financial institutions, customs records, and intelligence reports, also makes investigations more effective and complete. These tools can further identify unusual transaction patterns or detect when privacy enhancing technologies are used to hide the origin of funds. When this information is shared between agencies, the tools become even more effective in fighting PF.

116. A few countries reported on the importance of considering the same tactics as used in investigations of TCOs and drug traffickers, such as the use of undercover agents and confidential sources.

Box 38. Case Study: Use of undercover agents and confidential sources against trafficker of nuclear materials

On February 21, 2024, the United States Department of Justice (DOJ) and United States Drug Enforcement Administration (DEA) announced the issuance of a superseding indictment charging a defendant with conspiring with a network of associates to traffic nuclear materials from Myanmar to other countries. During this conspiracy, the defendant and his confederates showed samples of nuclear materials in Thailand to a DEA undercover agent ("UC-1"), who was posing as a narcotics and weapons trafficker. With the assistance of Thai authorities, the nuclear samples were seized and subsequently transferred to the custody of U.S. law enforcement. A U.S. nuclear forensic laboratory later analysed the samples and confirmed that the samples contain uranium and weapons-grade plutonium.

The defendant and his co-defendant were previously charged in April 2022 with international narcotics trafficking and firearms offenses, and both were ordered detained.

According to the allegations contained in the superseding indictment, beginning in early 2020, the defendant informed UC-1 and a DEA confidential source ("CS-1") that the defendant had access to a large quantity of nuclear materials that he wanted to sell. Later that year, the defendant sent UC-1 a series of photographs depicting rocky substances with Geiger counters measuring radiation, as well as pages of what the defendant represented to be lab analyses indicating the presence of thorium and uranium in the depicted substances. In response to the defendant's repeated inquiries, UC-1 agreed, as part of the DEA's investigation, to help the defendant broker the sale of his nuclear materials to UC-1's associate, who was posing as an Iranian general (the "General"), for use in a nuclear weapons programme. The defendant then offered to supply the General with "plutonium" that would be even "better" and more "powerful" than uranium for this purpose.

During their discussions regarding the defendant's access to nuclear materials, the defendant also engaged with UC-1 concerning his desire to purchase military-grade weapons. To that end, in May 2021, the defendant sent UC-1 a list of weapons, including surface-to-air missiles, that he wished to purchase from UC-1 on behalf of the leader of an ethnic insurgent group in Myanmar ("CC-1"). Together with two other co-conspirators ("CC-2" and "CC-3"), the defendant proposed to UC-1 that CC-1 sell uranium to the General, through the defendant, to fund CC-1's weapons purchase.

On January 8, 2025, the defendant pled guilty to conspiring to traffic nuclear materials, including uranium and weapons-grade plutonium, from Myanmar to other countries, as well as to international narcotics trafficking and weapons charges.

Source: United States

117. Finally, many countries highlighted the importance of interagency cooperation through regular meetings, including by establishing specialised taskforces and experts working groups. When financial institutions, customs authorities, and LEAs work together, they can enhance investigations and proactively lead to the freezing of assets and halting of shipments linked to PF and sanctions evasion.

Box 39. Jurisdiction Examples: Specialised taskforces and working groups to combat PF and sanctions evasion

- **France**: A specialised task force led by TracFin (the financial intelligence unit), investigated two companies (Entities A1 and A2) supplying electronic components to a sanctioned Russian entity. These companies acted as intermediaries, purchasing the components and transferring them to sanctioned groups through another company in a third country. The task force included TracFin, financial institutions, and law enforcement agencies. They analysed SARs/STRs submitted by banks, monitored the companies' financial flows, and tracked the involvement of beneficial owners. Their coordinated efforts resulted in freezing the companies' assets and stopping their operations.
- **Indonesia**: A working group investigated a bulk carrier vessel, Petrel 8, involved in transporting coal to the DPRK in violation of UN sanctions. The task force included the Ministry of Foreign Affairs, customs authorities, and the Financial Intelligence Unit (PPATK). They combined financial intelligence and shipping records to identify that the vessel was owned by an Indonesian company and had been previously sanctioned for similar activities. The task force coordinated with the UN Sanctions Committee, leading to the vessel's detention and eventual dismantling.

Sources: France and Indonesia

Challenges in Pursuing PF Investigation

118. In general, PF investigations are different from money laundering (ML) and terrorism financing (TF) investigations in many ways. PF focuses on funding activities that help support WMD programmes. It often involves powerful state actors or groups using front companies, trade, and complex ownership structures to avoid sanctions. Unlike ML, which hides the origins of illegal money, and TF, which funds terrorism, PF investigations rely more on intelligence related to potential violations of export controls and sanctions. PF can be more difficult to investigate because there is less awareness of its risks, and it often involves legal goods (including controlled goods) being used for illegal purposes. Investigators need stronger domestic and international cooperation, and advanced analytical tools to solve PF cases, which can be more complex than what is needed on a regular basis in ML or TF cases.

119. Many countries reported facing similar challenges, including PF schemes using front companies, multiple layers of ownership, and small but frequent transactions. These tactics make it very difficult for relevant stakeholders including LEAs, regulators, financial institutions, FIUs, and prosecutors, who rely on accurate data and strong collaboration to trace beneficial owners or organisations involved in complex schemes (see Typology 2).

120. Another challenge is the lack of awareness of PF risks, trends, and methods in financial institutions and other regulated entities, including insufficient training on PF risks to enhance the quality of SARs/STRs. As mentioned in this report's previous section, many countries do not criminalise PF. In part, this may explain deficiencies related to the number and quality of relevant SARs/STRs.

121. More broadly, limited resources amongst governmental authorities and private sector entities are also a challenge for many countries. Particularly, smaller countries may not have enough funding or expertise to handle complex cases. This could also be a prioritisation challenge that trickles down to the allocation of resources in the public and private sectors. While some countries may have established a primary offense that incudes PF or use ancillary offenses to prosecute acts of PF, the lack of countries with a consistent approach to criminalisation may disrupt international cooperation to investigate and prosecute PF-related cases.

122. Finally, cross-border cases require cooperation with other countries, but differences in legal systems, such as different rules for considering what is admissible evidence, varying definitions of financial crimes, and absence of dual criminality poses challenges in pursuing cross-border investigations. Without agreements between countries to share information, there may be significant delays or rejected information requests for investigations (see International Cooperation section).

Prosecution and other Methods

Good Practices in PF Prosecution

123. Many countries reported that prosecuting complex PF and sanctions evasion cases is even more complicated than investigating them. Successful prosecutions in PF and sanctions evasion cases require a strong legal framework, including clear laws that define PF and its related activities, along with the ability to collect and present evidence in court.

124. Coordinated efforts between investigation units and prosecutors are also essential for building strong cases. Learning from precedents and knowledge of typologies and new methods used by PF and sanctions evasion perpetrators can improve the chances of successful investigations and therefore successful prosecutions. Additionally, global partnerships can play an important role in PF prosecutions, highlighting the value of international cooperation in addressing these complex crimes. Lastly, serious confiscation and asset recovery regulations could lead to more prosecutions especially for funds flowing out of the country.

Challenges in Prosecuting PF Cases

125. Most countries reported that prosecuting complex PF and sanctions evasion cases is challenging. Some countries cited evidential difficulties in proving that controlled or prohibited goods were sent to a sanctioned jurisdiction. Where such evidentiary challenges are insurmountable, there are examples of prosecutors pursuing the offenders for other offences committed to conceal their PF offence, such as obstruction of justice or forgery offences. Others mentioned diplomatic immunity can limit the pursuit of certain PF or sanctions evasion cases.

126. Another challenge that countries face is proving that financial activities are directly linked to PF or sanctions evasion, especially when evidence is spread across different countries. This requires detailed documentation and strong international cooperation, which is not always easy to achieve in such complex cases.

127. Sharing information and intelligence between countries can help fill enforcement gaps and countries can tackle cross-border cases more effectively and prevent PF networks from exploiting weaknesses in the global financial system. However, many countries are lacking these mechanisms.

128. Training and awareness raising are also essential for successful prosecutions though many financial institutions, businesses, and even prosecutors lack understanding of the risks and complexities of PF. Providing proper training can help them recognise suspicious activities and understand how PF schemes work. This is important especially in countries with limited resources or expertise in handling PF cases.

Other Measures to Deter Violating Sanctions

129. As already outlined in this section, governmental authorities may consider criminal prosecution for breaches of TFS. Additionally, some countries consider other enforcement options to remedy breaches of TFS, including in relation to PF. Because many countries appear to face notable challenges in prosecuting complex PF and sanctions evasion cases, pursuing other measures may be worth considering under the appropriate circumstances.

Box 40. Jurisdiction Examples: Civil and criminal enforcement actions as a complement or alternative to criminal prosecution

- **European Commission**: EU Directive 2024/1226 of 24 April 2024 introduced new rules to establish common basic standards for criminal penalties for natural and criminal or non-criminal penalties for legal persons in all Member States, closing existing legal loopholes and increasing the deterrent effect of violating EU sanctions in the first place.[59]
- **United Kingdom**: A breach of financial sanctions may be a criminal offence, punishable upon conviction by up to seven years in prison. There are both civil and criminal enforcement options to remedy breaches of financial sanctions. Law enforcement agencies may consider prosecution for breaches of financial sanctions. The monetary penalties regime created by the 2017 Act provides an alternative to criminal prosecution for breaches of financial sanctions legislation. OFSI is the part of HM Treasury that imposes these monetary penalties.[60]
- **United States**: OFAC's investigative and enforcement authorities are exclusively civil in nature, as distinguished from the criminal sanctions enforcement authorities exercised by the DOJ, DHS, and Department of Commerce in this area. When appropriate, enforcement actions highlight the importance of robust and effective sanctions compliance programmes, particularly for companies involved in complex, international transactions to ensure measures are in place to prevent involvement in sanctions evasion schemes.
- In April 2023, British American Tobacco (BAT), a tobacco and cigarette manufacturer, agreed to pay $508,612,492 to settle its potential civil liability for apparent violations of OFAC's sanctions against the DPRK and WMD proliferators. In exporting tobacco and related products and receiving payment for those exports, BAT caused U.S. financial institutions to process wire transfers that contained the blocked property interests of sanctioned DPRK banks and to export financial services and facilitate the exportation of tobacco to the DPRK.61
- In April 2022, OFAC entered into a settlement agreement with Toll Holdings Limited ("Toll"), an Australian-headquartered international freight forwarding and logistics company for apparent violations of multiple sanctions programmes, including processing transactions involving the DPRK, Iran, and Syria. A key vulnerability was the lack of sufficient risk management and due diligence within Toll's compliance function.[62]

Sources: European Commission, United Kingdom, and United States

Domestic Coordination and Collaboration

Interagency Mechanisms

130. An effective interagency framework contributes to mitigating risks related to complex PF and sanctions evasion schemes. To develop effective interagency frameworks,

countries report the need for ongoing cooperation and coordination among relevant governmental authorities. For many countries, the relevant actors include AML/CFT/CPF officials, LEAs, supervisors, the judiciary, import and export controls and licensing authorities, customs, border control, and intelligence agencies. Countries report that close cooperation and coordination among many of these competent authorities facilitates exchange of relevant and timely information. Through this interagency process, governmental authorities are best positioned to help initiate and pursue investigations into potential violations of the TFS regime and other relevant PF activities.

Good Practices for the Interagency Cooperation

131. Based on submissions across the FATF Global Network, countries use interagency mechanisms to address PF and sanctions evasion under one of three overlapping categories: 1) general coordination on TFS, which includes PF-TFS; 2) a specialised focus on PF-TFS and export controls regulations; or 3) a specialised focus on PF-TFS and export controls regulations, as well as a wider scope of coordination to initiate complex PF and sanctions evasion investigations, prosecutions, and other measures.

132. Under the FATF Recommendation 7, the FATF Global Network is obligated to implement TFS without delay to comply with all UNSCRs relating to PF.[63] Most countries verified establishing a legal framework to implement PF-TFS, which often includes using existing interagency mechanisms on TFS. This type of interagency mechanism allows countries to fulfil their minimum rules-based requirements to address the potential breach, non-implementation, or evasion of TFS referred to in Recommendation 7.

---

59 The new rules aim to ensure that such violations can be criminally investigated and prosecuted in all Member States. They include a list of criminal offences related to the violation and circumvention of EU sanctions, such as for example: failing to freeze assets; breaching travel bans and arms embargoes; providing prohibited or restricted economic and financial services, transferring funds that should be frozen to a third party or providing false information to conceal funds that should be frozen. They also include enhanced rules on freezing and confiscation of proceeds, instrumentalities and assets subject to EU sanctions. Furthermore, the new rules aim to strengthen the cooperation and communication between the competent authorities in a Member State and among Member States and other relevant EU institution, bodies, offices and agencies.

60 Financial sanctions enforcement and monetary penalties guidance - GOV.UK

61 According to court documents, BAT Marketing Singapore (BATMS) pleaded guilty to a criminal information filed in the District of Columbia charging BAT and BATMS with conspiracy to commit bank fraud and conspiracy to violate IEEPA. BAT entered into a deferred prosecution agreement related to the same charges.

62 Toll facilitated nearly 3,000 payments in connection with sea, air, and rail shipments, originating from or received by its global units, through US financial institutions, benefiting individuals or entities that were either sanctioned by the US or located in UN or US-sanctioned countries. For more than half of the relevant period, Toll's compliance function failed to consider policies and controls commensurate with the complexity of its operations, which included almost 600 invoicing, data, payment, and other system applications spread across its various business units. The enforcement action revealed that after a bank raised concerns over Toll's compliance with US sanctions, Toll took steps to mitigate their risk exposure by ceasing all business with US-sanctioned countries in June 2016. However, Toll did not implement the compliance policies and procedures necessary to prevent payments involving sanctioned individuals or entities, nor did it test whether shipments involved persons located in UN or US-sanctioned jurisdiction.

63 This 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 United Nations Security Council under Chapter VII of the Charter of the United Nations, or persons and entities acting on their behalf, at their direction, or owned or controlled by them. Provided, those acting on behalf or under control of designated persons and entities or owned or controlled by them are not designated under national/supranational sanctions regimes.

Box 41. FSRB Secretariat Example: GAFILAT conducts TFS freezing mock exercises for member countries

GAFILAT is conducting mock exercises that allow member countries to test their interagency processes for implementing TFS in line with the FATF Standards. Based on a methodology and manual developed by GAFILAT, member countries respond to scenarios that are meant to test TFS capabilities and control mechanisms (including those in place for the public and private sectors).

Through the drills, GAFILAT is seeking to provide member countries with a practical tool to identify potential areas of weakness and strengthen their TFS systems. After the exercise, GAFILAT provides a non-public report with feedback and guidance for the country. Since 2024, GAFILAT conducted three mock exercises involving the TF-TFS processes for three member countries. Looking ahead, GAFILAT plans to conduct additional mock exercises, including sessions focused on PF-TFS processes for the rest of its member countries.

Source: GAFILAT

133. In the context of dual-use goods, export control authorities are responsible for regulating the export of most commercial items, often referred to as "dual-use" goods, which are those having both commercial and military or proliferation applications.[64] Many countries go beyond TFS requirements in line with UNSCR 1718 and prioritise the implementation of export control regulations as a broader risk management tool against PF and sanctions evasion.

Box 42. Jurisdiction Examples: Interagency mechanisms incorporating export control regulations

- **India:** Established multiple mechanisms for operational and policy coordination on PF, including the Inter-Ministerial Working Group (IMWG) on SCOMET (Special Chemicals, Organisms, Materials, Equipment and Technologies) Licensing, which discusses the licensing applications for export of dual-use goods and related matters. Also, the Multi-Agency Co-ordination Mechanism, constituted under India's WMD Act of 2005, is chaired by FIU-India and includes the participation of Regulators, Law Enforcement Agencies, and other relevant organisations.[65]

64 Dual use export licenses are required in certain situations involving national security, foreign policy, short-supply, nuclear non-proliferation, missile technology, chemical, and biological weapons, regional stability, crime control, or terrorist concerns. The license requirements are dependent upon an item's technical characteristics, the destination, the end-use, and the end-user, and other activities of the end-user. Even if a license is not required, there may be additional requirements to satisfy prior to exporting. The two examples below illustrate a specialised focus on export controls regulations relevant to PF and sanctions evasion.

65 Under the relevant provisions of the WMD Act, India's various Advisory Committees on WMD and their Delivery Systems, Nuclear and Nuclear related Items, Chemical Weapons and related Items, Biological

- **Singapore:** The Inter-Ministry Committee on Export Controls (IMC-EC), which oversees Singapore's export controls framework, including policy and operational issues relating to the proliferation of WMD and PF. The IMC-EC is chaired by the Ministry of Foreign Affairs and comprises relevant policy and law enforcement agencies. The IMC-EC also monitors Singapore's implementation of relevant UNSCRs and coordinates interagency follow-ups when Singapore receives information/intelligence relating to the proliferation of WMD and PF.

Sources: India and Singapore

134. As described earlier in this report, an understanding of this broader risk of WMD proliferation, and its underlying financing, may have a positive contribution to the understanding of the risk of the breach, non-implementation, or evasion of PF-TFS (i.e. the narrow definition of PF risks covered in the FATF Standards), and assist the implementation of risk-based measures and TFS. In this context, the examples below illustrate a wider scope of coordination to initiate complex PF and sanctions evasion investigations, prosecutions, and other measures.

Box 43. Jurisdiction Examples: Interagency mechanisms to address broader PF risk

- **Japan:** Under the Inter-Ministerial Council for AML, CFT, and CPF Policy, co-chaired by the National Police Agency and the Ministry of Finance, the Ministry of Finance and the Financial Services Agency conduct "joint inspections" where they jointly conduct the Ministry of Finance's foreign exchange inspections and the Financial Services Agency' AML inspections, from the perspective of sharing the inspection officials' knowledge and inspection information between the respective supervisory authorities and effectively and efficiently ensuring financial institutions' compliance with the related laws and regulations. In addition, when JMSDF (Japan Maritime Self Defence Force) ships or other assets detect activities that are suspected of illicit maritime activities including ship-to-ship transfers prohibited by the UNSCRs, the Ministry of Defence provides the information to relevant ministries and agencies.
- **Malaysia:** There are two main interagency groups that complement the multi-agency cooperation and coordination of Malaysia's CPF regime: the Strategic Trade Action Committee (STAC), chaired by the Strategic Trade Controller (STC) in the Ministry of Investment, Trade and Industry; and the National Coordination Committee to Counter Money Laundering (NCC), chaired by Bank Negara Malaysia. The STAC primarily focuses on the implementation of the Strategic Trade Act 2010 (STA 2010), which regulates exports, transit, transhipment and brokering of strategic items and technology, of which attended mostly by enforcement agencies and technical agencies related to PF

Weapons and related Items, and Export Control of Dual-Use Items, convene meetings periodically. The meetings include the participation of relevant Government of India organisations, in order to consider policy and related matters on the pertinent provisions of the WMD Act and other relevant Government of India Acts pertaining to WMD, their delivery systems and related dual-use goods and technologies.

matters. The NCC, which are represented by relevant AML/CFT/CPF ministries and agencies, formulate, implement, and monitor national strategies on combating ML/TF/PF.

- **United States:** Export Enforcement (within the Department of Commerce's Bureau of Industry and Security, BIS) has access to FinCEN's Banking Secrecy Act (BSA) data, works cooperatively with the export community and conducts investigations to support criminal and administrative penalties. Meanwhile, BIS administers and enforces export controls on dual-use, certain munitions, and commercial items through the Export Administration Regulations (EAR) under authority of the Export Control Reform Act of 2018 (ECRA). BIS works with the exporting community to prevent violations and conducts investigations to gather evidence supporting criminal and administrative penalties. BIS also works closely with FinCEN and OFAC, as well as U.S. law enforcement agencies to monitor for illicit procurement through PF, sanctions evasion, and circumvention of export control schemes.

Sources: Japan, Malaysia, and United States

Challenges for Interagency Coordination

135. Countries reported a variety of obstacles for successful domestic coordination, but many challenges were tied to a general lack of understanding and/or buy-in to address PF risks, especially in comparison to ML and TF. Because PF and sanctions evasion networks can often be backed by state actors, regular communication with the Intelligence Community is required and access to actionable information is vital to uncover sophisticated corporate structures and address sanctions evasion schemes.

136. However, some countries reported on the impediments to intelligence sharing, including when it involves foreign partners who place restricted access on the information. This challenge complicates the timely sharing of information and options to take immediate action against PF actors or activities. In one jurisdiction, the lack of understanding impacts prioritisation of PF, making it difficult to ensure relevant authorities are focused on the topic, sharing relevant information, and responding to intergovernmental referrals in a timely manner.[66]

137. Some countries reported a lack of relevant resources, knowledge, experience, and technology to address appropriately the risks associated with PF and sanctions evasion schemes. Although many countries in the FATF Global Network have dedicated resources to updating legal frameworks to address PF in line with the FATF Standards over the past decade, this has not led to a notable boost in the effective implementation of PF-related measures. As of April 2025, while more than half of 194 countries (54%; 105 countries) assessed during the 4th round of Mutual Evaluation are compliant (13%; 26 countries) or largely compliant with R.7 (41%; 79 countries), only 24% of these 105 countries (25 of 105) have achieved highly or substantially effective ratings on IO.11. In total, 17% of the assessed countries (32 of 194) have achieved highly or substantially effective ratings on IO.11 (See Figures 1 and 2).

66 For this project, some countries reported encountering their own interagency barriers that limited the sharing of relevant information and case studies. Given the nature of complex PF and sanctions evasion schemes, some countries reported not being able to declassify intelligence and/or share other sensitive information with the rest of the FATF Global Network.

138. However, in the context of Recommendation 1, the obligations to identify, assess, and understand PF-TFS risks referred to in Recommendation 7 is fuelling a global effort to evaluate PF risk, which may bolster effectiveness in the coming years. Over half of countries reported completing a PF risk assessment or PF chapter in the NRA within the last five years, while nearly one-fourth of countries are in the process of undertaking their first PF risk assessment and expect to complete the process by the end of 2025.

Information Sharing Between Public and Private Sector

139. Public-private partnerships (PPPs) can be valuable platforms for strengthening collaboration between stakeholders. These partnerships aim to allow governments to share useful information (e.g. typologies, evasion indicators, good practices, challenges) with private sector contacts. When actionable information is shared by the public sector, the private sector is better positioned to analyse their own customer and transaction records to identify current and historical potentially illicit activity, including the potential evasion of sanctions. Subsequently, this type of exchange bolsters the public sector's ability to identify and mitigate risks and issue targeted guidance aimed at the private sector entities, while preserving its responsibility to maintain customer privacy.

140. To support information sharing, many countries reported developing and monitoring risk indicators and red flags of PF and sanctions evasion schemes with a focus on transactions and trade patterns (see Annex A: Relevant to Proliferation Financing). In general, countries share the list of risk indicators with both public and private sector through periodic outreach and awareness-raising activities. However, nearly half of countries did not report developing or maintaining such risk indicators and red flags. This may indicate a lack of differentiation between PF risk indicators and other financial crimes, or a lack of prioritisation on complex PF and sanctions evasion in those countries. Because most countries rely upon SARs/STRs to detect PF and sanctions evasion activity, there is a possible information gap between the public and private sectors that undermines the effective implementation of preventive measures.

Good Practices for the Public Sector

141. Roughly one-third of countries reported concentrating their focus on private sector outreach through implementation of their TFS legal framework, including the receipt of SARs/STRs and implementation of TFS without delay. However, the same number of countries reported more robust public-private sector collaboration through various PPPs whose primary focus is not typically PF, though there are working groups or other mechanisms that allows for discussions on PF and sanctions evasion-related issues. Some countries also reported law enforcement and intelligence-led outreach to the private sector in addition to the participation of Ministries of Finance, FIUs, and regulators.

Box 44. Jurisdiction Examples: Public sector outreach to the private sector on PF and sanctions evasion

- **France**: 'Awareness-raising' mechanisms have been put in place to inform and exchange with the private sector, via the Banking and Insurance Supervisor, under the Central Bank, and the Treasury. In addition to financial institutions, public-private exchanges primarily target professionals in sectors deemed to be most exposed to risk, including DNFBPs and humanitarian non-profit

organisations (NPOs). The FIU organises specific occasional meetings with French financial entities (banks and credit institutions) among which some are targeted on proliferation financing. These reporting entities are the most critical to the Agency given that they accounted for 52.6% of the incoming SARs/STRs in 2023. There is a dual purpose behind these meetings: (i) raising awareness and (ii) addressing pain points and issues banks might be facing in the framework of countering PF. TRACFIN hosted a series of meetings with some of the major French banks to better understand compliance regarding PF, and to achieve feedback on the challenges they are facing in the detection of PF cases and the implementation of CPF mechanisms.

- **United States**: The Department of Commerce's BIS, which administers and enforces the Export Administrative Regulations (EAR), periodically publishes guidance and advisories for financial institutions, in coordination with FinCEN and other parts of the U.S. government. The publications include red flags and risk indicators to assist financial institutions in identifying transactions potentially tied to evasion of U.S. export controls. Recent publications focused on relevant PF threats posed by global evasion of sanctions and export controls, Iran's UAV-related activities, and the Ukraine-Russia Conflict.[67,68,69]

Sources: France and United States

Challenges for the Public Sector

142. Given the nature of PF and sanctions evasion, and the frequent involvement of state actors and intelligence collection, it often involves sensitive information that is difficult to share publicly. Many countries have established PPPs, but their main objectives are generally to improve the effective use of SARs/STRs, and there are few examples of partnerships focused specifically on PF or sanctions evasion issues. Approximately one-fourth of countries report the receipt of SARs/STRs as the extent of their outreach to the private sector on PF and sanctions evasion-related issues. However, Singapore and the UK use PPPs to overcome some public-private and private-private information sharing challenges on PF and/or sanctions evasion.

Box 45. Jurisdiction Examples: Overcoming information sharing barriers on PF and/or sanctions evasion

- **Singapore**: On April 1, 2024, the Monetary Authority of Singapore launched a digital platform, COSMIC, which stands for "Collaborative Sharing of Money Laundering/Terrorist Financing Information and Cases, with six major commercial banks in Singapore. COSMIC allows FIs to securely share with one another, information on customers who exhibit multiple "red flags" that may indicate potential financial crime concerns, if stipulated thresholds are met. This makes it easier for FIs to detect and thereby deter criminal activity. COSMIC

67 FinCEN & BIS Joint Notice, FIN-2023-NTC2, November 6, 2023
68 Microsoft Word - Iran UAV Industry Advisory - Final For Posting June 9 10AM (003)
69 FinCEN and Bis Joint Alert for OCC-OGC-FO

currently focuses on three key financial crime risks in commercial banking: misuse of legal persons, and misuse of trade finance for illicit purposes, and proliferation financing. COSMIC aims to help Fis to identify bad actors and take prompt action to disrupt illicit activities and network, while it also supports law enforcement and supervision of the financial system.

- **United Kingdom:** Joint Money Laundering Intelligence Taskforce (JMLIT) is used regularly by Law Enforcement Agencies (LEAs) to share intelligence with the private sector who in return share intelligence back to the LEAs. This enables the private sector to understand strategic typologies and tactical threats. The Office of Financial Sanctions Implementation (OFSI) have recently established a sanctions circumvention cell of JMLIT which is jointly chaired by a UK-based FI.

Sources: Singapore and United Kingdom

Good Practices for the Private Sector

143. Many private sector entities reported that PPPs are useful tools to promote public-private and private-private information sharing on sanctions evasion and PF issues. However, it is noteworthy that the private sector provided considerably more examples of challenges than good practices in regard to information sharing (see Challenges for the Private Sector below). Also, there were several suggestions for the public sector to improve and expand current PPP initiatives. For instance, private sector entities asked for more streamlined processes to share information with FIUs and law enforcement agencies; a consistent approach to timely intelligence sharing from the public sector; and clearer legal frameworks and/or guidance to encourage public-private information sharing in additional countries. Furthermore, some private sector entities stated that the effectiveness of information sharing is undermined by a lack of sharing across sectors. Still, several private sector entities believe that the FATF could play an instrumental role in advancing discussions and analysing risks on PF and sanctions evasion across sectors.

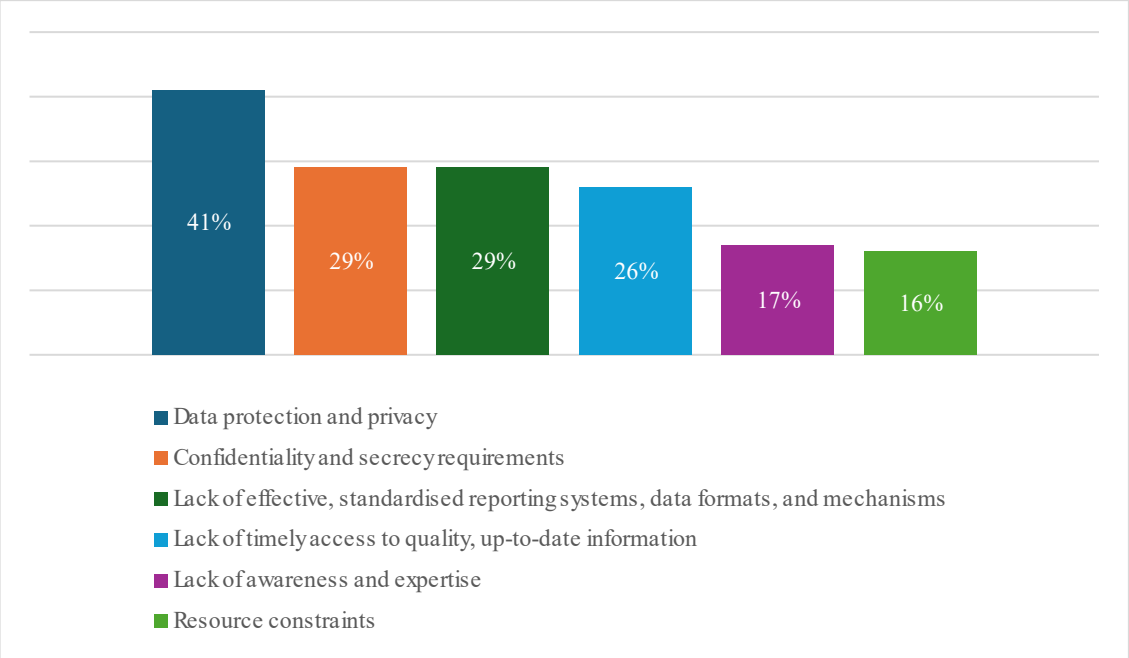
Challenges for the Private Sector

144. Financial institutions, DNFBPs, and VASPs are important actors in preventing and combating complex PF and sanctions evasion schemes. However, private sector entities typically have less understanding of PF than ML or TF. Accordingly, most examples of current PPPs focus mainly on the public sector raising awareness of PF and providing information on the filing of SARs/STRs, which may not provide an opportunity for the private sector to learn how to take concrete steps to identify and detect complex PF and sanctions evasion schemes. To detect and report these complex schemes, the private sector would likely benefit from more guidance on evaluating relevant activity, such as trade transactions and the exchange of large volumes of information between multiple parties. The relevant documents may be stored in various forms and media, which can make it difficult to cross-reference the data with international and national sanction lists.

145. Many private sector entities reported a number of other information sharing challenges, including the uneven implementation of data privacy provisions, other regulatory restrictions and jurisdictional differences, confidentiality and trust concerns, delays in dissemination of intelligence, inconsistent data formats, and resource constraints (see Figure 4). In particular, the private sector emphasized the difficulty of balancing data privacy and preventive measures obligations. Also, some non-bank financial institutions

and DNFBPs reported the need for sectoral guidance, since current outreach is more focused on the activities of large banks.

Figure 4. Top Challenges for Information Sharing



International Cooperation

146. To promote consistent enforcement and reduce opportunities for illicit actors to target countries or entities with weaker preventive controls, the public and private sector benefit from the aligned approach to legal frameworks on PF and sanctions evasion. The standards set by the FATF, such as implementing TFS, and adopted by countries, which can also include criminalizing PF and enhancing export controls in certain instances, create a shared framework for combating PF. For instance, countries enforcing similar measures against the misuse of financial institutions reduce the potential of weaker links in the international financial system. A push toward standardised export controls and end-user verification help prevent sensitive technologies from being diverted to prohibited uses and disrupt underlying proliferation financing.

147. International cooperation is also crucial to address emerging threats related to new financial technologies, such as virtual assets. In this context, as mentioned above, the FATF Virtual Asset Contact Group has been intensively discussing challenges and good practices for the effective implementation of AML/CFT/CPF measures on virtual assets, especially the growing risks of theft and misuse of virtual assets by the DPRK.

Good Practices for International Cooperation

148. Some countries reported that effective international cooperation relies on the exchange of intelligence between governments, financial institutions, and private sector actors. Sharing information about suspicious transactions, sanctioned entities, and high-risk activities helps identify and disrupt PF networks and sanctions evaders. For example, sharing SARs/STRs across borders helps uncover complex transaction chains linked to proliferation. FIUs of most countries reported signing treaties and memorandums of

understanding (MOUs) with other FIUs to enable the exchange of intelligence, including intelligence related to PF activities. For instance, the Egmont Group of FIUs facilitates secure communication and collaboration among over 160 countries, allowing sharing in real-time of actionable information.

Box 46. Case Study: International cooperation on controlled dual-use goods exportation

FINTRAC received a spontaneous dissemination from an FIU detailing SARs/STRs submitted by financial institutions in their jurisdiction, reporting 90 suspicious wire transfers, totalling approximately US$2.5 million. The spontaneous dissemination included wire transfers involving entities subject to the national sanctions regime of another jurisdiction due to the illicit procurement of dual-use goods for the Russian defence sector. The SARs/STRs identified several potential money laundering indicators, and identified several wire transfers from listed entities in the FIU's jurisdiction to entities in Canada, and entities in high-risk countries for illicit procurement activity.

FINTRAC assessed the spontaneous dissemination, and produced a disclosure detailing financial activity reported to FINTRAC by means of SARs/STRs and electronic funds transfer reports. The disclosure included financial transactions between a Canadian entity and related individuals/businesses that have been previously subjects of investigation due to suspected illegal export of dual-use/military goods to Russian end-users. Additionally, SARs/STRs described transactions consistent with a known money-laundering typology on "Russian and Eastern European laundromat scheme," and continued transactions with Russian entities post-Canadian sanctions.

The disclosure packages provided an overview of a suspected illegal procurement network. The disclosure was sent to multiple federal disclosure recipients and other FIUs.

Source: Canada

149. Cross-border cooperation in law enforcement enables countries to tackle the complex and transnational nature of PF and sanctions evasion. Multinational task forces bolster the resources and expertise of governmental authorities to investigate and dismantle networks. For instance, coordinated operations can uncover front companies, intermediaries, and complex routes involving several countries, used by proliferating networks for procurement and financing of WMD programmes.

Box 47. Case study: Spain's national police cooperating with EU counterparts to counter PF

Spain has encountered several recent cases that required international cooperation with other EU countries. In every case, intermediary companies were concealing the destination of the material. The entities involved were networks of companies, some with subsidiaries in different countries, and their managers. There was also a "facilitator" or an intermediary in the operations. The main risk indicator detected in the different cases was an unusual volume of sales, and the origin of the transfers and the different amounts detected, after the financial analysis was conducted.

In one case, the National Police were investigating the diversion of an estimated €5 million worth of defense material to Russia, specifically parts for military aircraft, through the use of front companies and intermediaries. The investigation revealed relevant payments and laundering of payments from the sales operations of the front companies. International cooperation, within the framework of EU countries, allowed the investigations of shipments that were made via complex road and air routes and passing through different countries.

In another case, the National Police were investigating the diversion of more than €800,000 worth of chemical substances to Russia, which is prohibited under European Union sanctions. Some of these substances were precursors of explosives and precursors of chemical weapons. The chemical substances were stored in a free zone at Spanish port before being exported. In Spain, a joint investigation between the National Police and Customs was conducted. As the transport was carried out by road, it required cooperation with agencies from other countries to investigate the routing of the material across European borders.

Source: Spain

Box 48. Case Study: United States and ROK sanction actors financing the DPRK WMD Programme[70]

In March 2024, in coordination with the Republic of Korea (ROK), OFAC designated six individuals and two entities based in Russia, China, and the United Arab Emirates, that generate revenue and facilitate financial transactions for the DPRK. Funds generated through these actors are ultimately funnelled to support the DPRK's WMD programmes in violation of TFS required under UNSCR 1718. The ROK jointly designated six of the same individuals and entities for their involvement in illicit financing and revenue generation through overseas DPRK IT workers.

This action targets agents of designated DPRK banks along with companies that employ DPRK IT workers abroad. DPRK banking representatives, IT workers, and the companies that employ them generate revenue and gain access to foreign currencies vital to the DPRK government. These actors, operating primarily through networks located in Russia and China, orchestrate schemes, set up front or shell companies, and

70 Department of the Treasury, "Treasury Sanctions Actors Financing the North Korean Weapons of Mass Destruction Program," (March 27, 2024), Treasury Sanctions Actors Financing the North Korean Weapons of Mass Destruction Program | U.S. Department of the Treasury

manage surreptitious bank accounts to move and disguise illicit funds, evade sanctions, and finance the DPRK's unlawful WMD and ballistic missile programmes.

Source: United States

150. Some countries and international organisations like the United Nations Office on Drugs and Crime (UNODC) and the World Bank provide training, technical assistance, and funding to strengthen institutional and enforcement capacities of countries with limited resources. Programmes focus on improving regulatory frameworks, enhancing monitoring systems, and increasing awareness of PF risks among public and private sectors. Providing expertise on implementing effective export controls and end-user verification, and assisting countries in adopting advanced monitoring systems to detect and report proliferation-related financial activities are crucial to effectively counter proliferation financing.

Box 49. Jurisdiction Example: European programme EU P2P (Partner to Partner)

The EU P2P (Partner to Partner) export-control programme aims to strengthen export controls for dual-use goods and arms trade worldwide. Managed by the European Commission and the European External Action Service and coordinated by Expertise France, the Programme's objectives are to promote and reinforce international cooperation in the field of dual-use export controls, Arms Trade Treaty implementation, and arms export controls by strengthening national and regional capacity, taking into account the balance between security and economic considerations. The programme includes awareness raising activities on PF risks and technical assistance to draft National Risk Assessment of Proliferation Financing.

Source: France

Challenges for International Cooperation

151. As discussed in other parts of this report, jurisdictional differences in legal frameworks and sanctions programmes present the main challenge to effective international cooperation against complex PF and sanctions evasion schemes (including different approaches to criminalisation of PF, which is discussed in the Detection, Investigation, and Prosecution sections). PF networks and those facilitating sanctions evasion operate across borders, exploiting regulatory disparities, leveraging different financial systems and international trade, posing a threat to global security. Hence, addressing these risks require robust international cooperation, to strengthen the ability of governmental authorities to prevent, detect, and disrupt illicit activities. Also, cooperation among countries and international organisations is required, because of many countries lack the infrastructure or expertise to monitor and counter PF and sanctions evasion effectively.

6. Conclusion and Priority Areas

152. While many countries completed a PF risk assessment in recent years or will complete their first by the end of 2025, the FATF Global Network is at varying stages of identifying and mitigating threats and vulnerabilities relevant to complex PF and sanctions evasion schemes. Unfortunately, the joint effort to combat and prevent PF and sanctions evasion may become increasingly difficult in the coming years. Well-resourced state and non-state actors will continue to probe for weaknesses in enforcement, preventive measures, and legal frameworks and take advantage of new technologies and ongoing shifts in the geopolitical landscape.

153. The best way to protect the international financial system against this evolving PF risk is to strengthen the existing and nascent links that compose CPF controls around the world. Countries have made notable strides in updating their CPF legal frameworks and implementing PF-TFS over the past decade, but there may be need for a collective leap forward in the effective implementation of CPF regimes. In the context of the revisions to FATF Recommendation 1, the FATF Global Network already has a blueprint to move toward this goal. As described in the 2021 PF Guidance, countries are required to identify, assess, understand, and mitigate their PF risks. Additionally, private sector entities are required to implement processes to identify, assess, monitor, manage, and mitigate PF risks, but they may do so within the framework of their existing TFS and/or compliance programmes.[71] [72] Countries should also consider whether additional efforts may be required to address PF risks, including through detection and reporting tools; domestic coordination and collaboration; investigations and prosecutions; and international cooperation. [73]

154. This study shows that PF and sanctions evasion actors frequently rely on the use of intermediaries to mask their illicit activities and conceal the real end-user of dual-use goods and other items destined for proliferating or sanctioned countries. Sophisticated schemes are employed to obscure the identity of those individuals, companies, and countries involved in the evasion of sanctions, which can make it difficult to detect illicit activity. To promote the FATF Global Network taking a joint step forward to prevent and combat complex PF and sanctions evasion schemes, there are several priority areas of focus that should be considered.

71 Guidance on Proliferation Financing Risk Assessment and Mitigation

72 In the context of PF risk, risk-based measures by financial institutions and DNFBPs seek to reinforce and complement the full implementation of the strict requirements of Recommendation 7, by detecting and preventing the non-implementation, potential breach, or evasion of targeted financial sanctions. In determining the measures to mitigate PF risks in a sector, countries should consider the PF risks associated with the relevant sector. By adopting risk-based measures, competent authorities, financial institutions and DNFBPs should be able to ensure that these measures are commensurate with the risks identified, and that would enable them to make decisions on how to allocate their own resources in the most effective way.

73 In line with Recommendation 2 and its Interpretive Note, countries should have an inter-agency framework in place to mitigate proliferation financing risks more effectively.

Recommendations for further FATF work on CPF

a) **Periodic Update on PF**: Consider updating the current situation, trends, and methods sections of this report regularly. PF and sanctions evasion risk will remain a significant challenge for the FATF Global Network to address for the foreseeable future. However, the threats, vulnerabilities, and typologies underpinning our collective understanding of this issue are certain to evolve and reshape on an ongoing basis. Given the nature of assessing PF risk, it is important for countries and the private sector to maintain an understanding of the current landscape. Without the UNSCR 1718 POE reports, the FATF should help key stakeholders to monitor the risk landscape.

b) **Promote Public-private Sector Collaboration**: Consider using this report and insight from the public consultation to structure outreach to the private sector as part of a FATF event, and then use their feedback to develop a follow-up guidance report that is more focused on actions that can be taken in partnership with FIs, DNFBPs, and VASPs to strengthen CPF preventive measures. For example, there could be a relevant session or series of sessions organised for the 2026 Private Sector Consultative Forum. Because the FATF Global Network reported a heavy reliance on SARs/STRs to initiate PF and sanctions investigations, more coordinated outreach and guidance can be used to strengthen public-private information sharing across relevant sectors.

c) **WMD PF Definition**: Within five years, consider adding an official definition for WMD PF to the FATF General Glossary, taking into account the results of the horizontal review of the FATF Global Network's PF risk assessments. As outlined in this report, jurisdictional differences in the approach to PF and sanctions evasion can undermine or complicate detection, investigation, and international cooperation on this topic. A unified and generally accepted definition would mitigate frustrations in preventing and combating PF and sanctions evasion.

d) **Horizontal Review of PF NRAs:** Within three years, consider conducting a horizontal review of the FATF Global Network's PF risk assessments. As described in this report, countries are at varying stages of identifying, assessing, understanding, and mitigating PF risk, and using a series of new techniques to do so. Also, there appears to be an uneven understanding of vulnerabilities relevant to PF and sanctions evasion. Given the important task ahead for both the public and private sector to better understand PF risk in line with the FATF Standards, a horizontal review may help identify good practices after the FATF Global Network has had more time to assess PF risk.

Annex A: Risk Indicators

1. The indicators provided below are a non-exhaustive list derived from the information received by the FATF in the course of this project. The indicators are designed to enhance the ability of public and private sector entities to identify suspicious transactions and/or activity associated with relevant PF and sanctions evasion schemes. While several indicators identified may not appear to have a direct or exclusive connection with PF or sanctions evasion and may be indicative of other forms of illicit activity, they may nonetheless be relevant when trying to identify PF and sanctions evasion schemes.

How to use these indicators

2. An indicator can increase the likelihood of the occurrence of unusual or suspicious activity. The existence of a single indicator in relation to a customer or transaction may not alone warrant suspicion of a transaction of PF or sanctions evasion, nor will the indicator necessarily provide a clear indication of such activity, but it could prompt further monitoring and examination, as appropriate. Similarly, the occurrence of several indicators could also warrant closer examination. Whether one or more of the indicators suggests a suspicious transaction or activity is also dependent on the business, product, or service that an institution or market participant is offering; how it interacts with its customers.

3. The indicators listed below are relevant to both the public and private sectors. With respect to the latter, the indicators are relevant to financial institutions, including banks and money value transfer services, designated non-financial businesses and professions, and virtual asset service providers, and small and mid-size businesses and large conglomerates operating in, or with touchpoints to, dual-use goods or other relevant sectors. Within the private sector, these indicators are intended to be used by personnel responsible for compliance, transaction monitoring, investigative analysis, client onboarding and relationship management, and other areas that work to prevent PF, sanctions evasion, and predicate crimes.

4. Some of the risk indicators require the cross-comparison of various data elements (e.g., financial transactions, customs data) often held in external sources. Due to this reliance on external data, the private sector may not observe all the indicators identified below. For some of the risk indicators, the private sector will need additional contextual information from competent authorities, e.g., via engagement with law enforcement authorities or FIUs. In using these indicators, private sector entities should also take into consideration the totality of the customer profile, including information obtained from the customer during the due diligence process, trade financing methods involved in the transactions if applicable, and other relevant contextual risk factors.

5. The following table sets out the risk indicators that are grouped into three broad categories: 1) customer information/behaviour; 2) transactions; and 3) trade activities. Customer information/behaviour indicators can be used when conducting CDD, while transaction indicators may be used for monitoring transactions, including export transactions. Trade activities can provide further context to factor into broader risk management processes. While there is overlap between some of the risk indicators in each category, the FATF Global Network sought to prioritize providing as much information as possible to support the public and private sectors.

1. Customer information/behavior

1. Use of corporate vehicles (e.g., shell companies) to obscure ownership, the source of funds, or the countries/entities involved, particularly sanctioned countries.
2. Obscuring the end user through transaction layering, with procurement agents routing shipments, communications, and finances through multiple layers of companies, brokers, and intermediaries.
3. When customer uses complicated structures to conceal connection of goods imported / exported, for example, uses layered letters of credit, front companies, intermediaries, and brokers.
4. Changes to standard business documents to obscure the ultimate customer.
5. Details of parties are similar to parties listed under WMD sanctions or trade controls (for example, names, addresses, or telephone numbers)
6. The accounts are owned by, or transactions are carried out by companies with opaque ownership structures, shell companies or one-day firms.
7. Customer is involved in supplying, selling, or delivering restricted or high-risk goods and/or technology.
8. Customer has previously had dealings or maintains relationships with individuals or entities now subject to sanctions.
9. Parties are physically located in countries of diversion concern (states that allow the provision of proliferation-sensitive goods, or their financing, through their territory)
10. A customer or a customer's counterparty conducts transactions with domestic sanction regime designated entities and individuals, or transactions that contain a nexus to identifiers listed for domestic sanction regime designated entities and individuals, such as email addresses, physical addresses, phone numbers, passport numbers, or convertible virtual currency (CVC) addresses.
11. Customer affiliated with universities and research institutions handling dual-use goods or products subject to export control.
12. Transactions involve a purported civil end-user, but basic research indicates the address is a military facility or co-located with military facilities in a country of concern.
13. A customer acquires new vessels for no apparent economic or business purpose.
14. A business model is fully export-oriented, acting as a pass-by entity.
15. Company is operating in the shipping, import/export, textile, garment, fishery, and/or seafood industry.
16. Client insists on confidentiality regarding transactions or shows inadequate concern about regulatory compliance related to sanctions and PF.
17. Transactions involve entities whose business registration indicates work on "special purpose" projects.
18. Customer requests to borrow personal information from co-workers to secure contracts.
19. The customer transacts in goods that are unrelated to its normal business and may involve dual-use equipment or technology (e.g., chemical reactors, machine tools, missile system components).

20. Customer's contact information, such as phone numbers, does not match the destination country.
21. A customer refuses to provide details to banks, shippers, or third parties, including details about end-users, intended end-use(s), or company ownership.
22. Companies serving as fronts for illicit activities lack online presence despite handling significant transactions.
23. Cyber spoofing of email or web addresses to make illegitimate inquiries appear to come from legitimate businesses, often leveraging known business relationships.
24. IP address does not match the customer's reported location.
25. A corporate name which is overly generic, non-descriptive, or easily mistaken with that of another better-known corporate entity. Additionally, the corporate name may be regularly misspelled in different ways.

2. Transactions

1. Transactions involve smaller-volume payments from the same end-user's foreign bank account to multiple, similar suppliers.
2. Transactions involve a last-minute change in payment routing that was previously scheduled from a country of concern but is now routed through a different country or company.
3. Routing a prohibited transaction through the financial system, causing a financial institution to process payments in violation of domestic sanction regime.
4. Funds may flow cyclically between companies, with one ceasing payment and another initiating payment to the same beneficiary.
5. A customer uses financial services and/or conducts transactions that are physically distanced from the actual trade of goods.
6. Omitting references to sanctioned parties or countries in financial transaction documentation.
7. Transactions pass through countries or financial centers known for weak sanctions enforcement or for engaging in illicit trade schemes.
8. Use of complex or unusual payment routes, including chains of multiple financial institutions, especially if they pass through countries with inadequate PF controls or sanctions.
9. Transactions that use open accounts/open lines of credit for payments in conjunction with known transshipment countries.
10. Purchases under a letter of credit that are consigned to the issuing bank, not the actual end user.
11. The customer's request the issuance of a letter of credit related to dual-use products or products subject to export control before approval is given for the opening of an account.
12. The outstanding amounts of deposits in their deposit accounts increased steeply, followed by cash withdrawal, as an indication of the possibility of such transactions being conducted.
13. A customer transfers funds overseas similar in value to recent cash deposits

14. The customers use individuals' accounts for the payment for the products.
15. The use of numerous bank accounts.
16. Lack of clear justification for a trade transaction or the reason for paying a large sum, especially if it is not in line with the client's normal business activities.
17. The volume and value of goods do not match the volume of payments.
18. Customer requests payment in virtual assets to evade KYC/AML measures.
19. Transfers through virtual asset service providers, especially if they involve low-regulated countries or if decentralised exchanges are used without proper due diligence.
20. Use of unofficial or alternative channels, such as money transfer systems (hawala), which can be used to circumvent sanctions restrictions.
21. Creation of new addresses for virtual assets to create the 'appearance' of their non-involvement in sanctioned crypto exchanges
22. Transactions related to payments for defense or dual-use products from a company incorporated after February 24, 2022, and based in a non-Global Export Control Coalition (GECC) country

3. Trade Activities

1. Changing an item's shipping instructions when the item arrives at a freight forwarder, without the knowledge of the exporter.
2. Last-minute changes to shipping instructions that contradict customer history or business practices.
3. A change in the shipping documents of the final consignee or location prior to or during shipment.
4. Customer requests shipment to an address not listed on their identification documents.
5. A product whose quality is not consistent with the technological level of the country of destination is being exported.
6. The transaction(s) involve the shipment of goods inconsistent with normal geographical trade patterns i.e. where the country involved does not normally export or import or usually consumed the types of goods concerned.
7. Trade transactions involving equipment or materials capable of use in military or nuclear programs (e.g., high-strength alloys, centrifuges).
8. Listing a freight forwarder or an operator of charter aircraft as the end user.
9. Products are transported through roundabout means, including the use of a small or obsolete ship.
10. Items arrive in small, frequent shipments to a central location before being combined.

11. Transactions involve freight-forwarding firms operating in high-risk transshipment areas.
12. Routing purchases through transshipment points commonly used to redirect restricted items to embargoed destinations.
13. Transactions associated with atypical shipping routes for a product and destination.
14. When a freight forwarding / customs clearing firm being listed as the product's final destination in the trade documents.
15. When goods destination/shipment country is different from the country, where proceeds are sent/ received without any plausible reason.
16. Falsifying shipping documentation, such as bills of lading and invoices, to conceal shipping routes, embarkation ports, consignees, or shipping agents.
17. Substitution of names of goods that fall under sanctions or export controls, as well as the use of false contracts to conceal the end user.
18. Supporting documents, such as a commercial invoice, do not list the actual end-user.
19. Misclassification of goods in documentation to evade detection, such as using non-sensitive descriptions for restricted items.
20. Discrepancies between information in commercial, transportation and financial documents. For example, discrepancies between invoices and shipment information (type of goods, weight, value, destination).
21. DPRK exporters disguise the origin of goods produced in DPRK by affixing country-of-origin labels that identify a third country.
22. Third-country suppliers shift manufacturing or subcontracting work to a DPRK factory without informing the customer or other relevant parties.
23. DPRK-flagged merchant vessels have been physically altered to obscure their identities and pass as different vessels.
24. Luxury goods are shipped frequently to central warehouses in third countries.
25. Rapid shifts to new purchasers for transactions involving restricted luxury goods.
26. The purchase and delivery of construction materials.
27. Substantial financial activity unrelated to the stated business purpose, such as payments unrelated to textiles, fisheries, or coal exports.
28. Customers that are manufacturing or trading companies use cash in transactions regarding industrial products or other trade transactions.
29. Whether the declared price of the cargo is low compared with the transportation cost.
30. The flag of registry of a ship is changed frequently.

31. Involvement of FTZs, which can be exploited to obfuscate origin and movement of sensitive items.