Government of JERSEY

National Risk Assessment: Proliferation Financing

Government of Jersey

April 2025

Table of Contents

Foreword

The Government of Jersey is committed to maintaining the highest standards in the fight against illicit financial activities - including proliferation financing (PF) - which pose a significant threat to international peace and security. PF is the act of providing funds or financial services which support the development, production and spread of weapons of mass destruction, their delivery systems and related materials.

As a responsible International Finance Centre, Jersey recognises the crucial role that the sector plays in preventing the use of financial services for nefarious purposes, in contravention of national laws or, where applicable, international obligations.

This National Risk Assessment has been conducted as part of our ongoing efforts to understand Jersey's PF risk level and align with international best practices. The Assessment provides an overview of the PF risks within Jersey and identifies the measures we have in place, as well as those we need to enhance to mitigate these risks effectively.

In conducting this assessment, we have adopted a collaborative approach, engaging with a wide range of stakeholders including Government of Jersey agencies, the Jersey Financial Services Commission, financial services businesses, and international partners. Our risk assessment demonstrates a comprehensive understanding of the challenges we face and will enable us to develop robust strategies to address them.

Ongoing review, identification, and assessment of PF threats will continue, potentially leading to the identification of additional threats and vulnerabilities, and corresponding mitigation strategies.

The findings of this National Risk Assessment underscore the importance of continued vigilance, cooperation, and innovation in combating PF. It is only through collective efforts that we can prevent Jersey's financial services businesses from being exploited for activities that threaten global security.

We remain committed to strengthening our regulatory framework, enhancing our risk-assessment capabilities, and working closely with international counterparts to ensure that Jersey continues to play its part in the global effort to prevent PF activities.

I would like to extend my gratitude to all those who contributed to this important work. Together, we will ensure that Jersey remains a safe and secure financial centre, resilient to the evolving threats posed by PF.

Deputy Ian Gorst

Minister for External Relations

Government of Jersey

April 2025

1. Executive summary and recommended actions

Executive summary

Jersey, as a leading international finance centre (**IFC**),[1] plays a crucial role in the global financial system. While it has a stringent anti-money laundering (**AML**), countering of terrorist financing (**CFT**) and countering of proliferation financing (**CPF**) regime, the Island's expertise in managing corporate structures with cross-jurisdictional touchpoints can make it attractive to bad actors seeking to obscure the origin of funds before proliferation financing (**PF**)-related procurement.

The primary aim of Jersey's PF National Risk Assessment (**NRA**) is to identify, assess, understand, prevent and mitigate the risks associated with PF within Jersey. This includes evaluating the vulnerabilities and threats to the jurisdiction's financial services which are used, in whole or in part, for the development, production, or dissemination of weapons of mass destruction (**WMD**) and their delivery mechanisms, and related materials.

Jersey's commitment to playing a proactive role in the global CPF effort is reflected in the Island's national strategy for combatting financial crime, its active participation in international forums, and its adherence to international standards. Jersey has developed a comprehensive legal and regulatory framework designed to detect, deter, and prevent the misuse of its financial system for PF purposes. There are both legal and operational gateways to ensure timely cooperation and exchanges of information between stakeholders, nationally and internationally.

Jersey's PF NRA represents a key component of our commitment. By systematically identifying and assessing the risks associated with PF, the PF NRA enables Jersey to strengthen its defences against this global threat and to contribute effectively to the international non-proliferation regime. It ensures that *all* businesses operating in or from within Jersey (including financial services businesses[2], entities registered with the Jersey Financial Services Commission (**JFSC**) Registry, and those administered under the Control of Borrowing (Jersey) Law 1947), are aware of their obligations and allows them to implement appropriate systems and controls to mitigate their PF risks.

Through this assessment, Jersey seeks to reaffirm its commitment to global security and to demonstrate its proactive stance in preventing the misuse of its financial system for activities that could endanger international peace and stability.

Although this report will show that Jersey's safeguarding measures are stringent, there is no room for complacency. The Island has experienced potential PF abuse (see **Appendix 1)**.

This report sets out that, on balance, **Jersey's main vulnerability is in the PF process stage of obscuring of funds and money flows. This is most likely to occur through corporate and financial infrastructure abuse by proliferators and their associates.** This is in line with the typical PF typology whereby complex proliferation networks and tactics are utilised to obfuscate transactions and relationships.

The Island's overall level of PF risk is assessed as **Medium Low**.

2. Recommended actions

3.1 Continue to develop PF Risk Understanding in Private Sector This can be achieved by upskilling and outreach in the private sector in relation to:		**Agencies Responsible:**
3.1.1	**Reinforcement of the requirement to make sanctions reporting disclosures to the Minister, in addition to suspicious activity reports (SARs) to the Money Laundering Reporting Officer (and/or Jersey's Financial Intelligence Unit (FIUJ), as and when required.**	FSIU FIUJ JFSC
3.1.2	**PF typologies.**	FIUJ
3.1.3	**Red flag indicators of potential export control and/or sanctions evasion.**	FIUJ
3.1.4	**Supply chain and dual-use goods understanding.**	FIUJ
3.1.5	**Payment processing vulnerabilities.**	FIUJ

3.2 Continue to develop PF Risk Understanding in Public Sector This can be achieved by:		Agencies Responsible:
3.2.1	**Considering whether sector-specific PF risk analysis and data capture should be undertaken (dependant on risk profile) when carrying out the next PF NRA.**	GoJ
3.2.2	**Competent authorities ensuring personnel receive relevant training to develop and/or maintain adequate skills and capabilities.**	All
3.2.3	**Competent authorities to continue to monitor and respond to geopolitical events and changes in typologies and modus operandi.**	All

3.3 Increase domestic and international Engagement This can be achieved by:		Agencies Responsible:
3.3.1	**FIUJ continuing its public-private partnership engagements for information sharing.**	FIUJ
3.3.2	**Competent authorities considering engaging more closely with jurisdictions with which Jersey has a significant number of financial and/or trade connections.**	SoJP FIUJ LOD
3.3.3	**Competent authorities considering Jersey's vulnerability to exploitation by DPRK diplomats for PF purposes.**	JCIS GoJ

3. Introduction

3.1. International obligations

3.1.1 The United Nations' Security Council (**UNSC**) has primary responsibility for the maintenance of international peace and security and takes the lead in determining the existence of a threat to peace or an act of aggression. In some cases, the UNSC can resort to imposing sanctions or even authorise the use of force to maintain or restore international peace and security. The UN Security Council Resolutions (**UNSCRs**) form the cornerstone of the global sanctions regarding proliferation. These legally binding resolutions impose obligations on UN member states to prevent and suppress PF activities. For example, UNSCR 1540, adopted in 2004, obliges all member states to refrain from providing any form of support to non-state actors seeking to acquire WMD.

3.1.2 As a British Crown Dependency, Jersey is not recognised as a UN member state in its own right and cannot propose designations directly to the relevant UNSC Committee. However, the Jersey - FCDO Memorandum of Understanding on Listing/De Listing[3] allows for the Island to request the UK, who is responsible for Jersey at the UN, to make such proposals on its behalf. Also in place is a written procedure setting out how such proposals are to be made, which includes references to the relevant criteria and procedures published by the relevant UNSC Committees.

3.1.3 All UNSC sanctions designations are immediately and automatically effective in Jersey, as are UK autonomous sanctions, through the Sanctions and Asset-Freezing (Jersey) Law 2019 (**SAFL**) and the Sanctions and Asset-Freezing (Implementation of External Sanctions) (Jersey) Order 2021 (**SAFL Order**) and its subsequent Orders and Regulations. Since 1 July 2023 financial services businesses have been obliged to implement all changes and sign up to GOJ and JFSC sanctions notifications,[4] as well as maintain adequate policies and procedures, and systems and controls to effectively counter PF and sanctions evasion.

3.1.4 In 2020, the international standard setter for AML/CFT/CPF, the Financial Action Task Force (**FATF**), revised their international standards (often referred to as the FATF Recommendations)[5] concerning PF. The standards set out a comprehensive and consistent framework of measures which countries should implement to combat money laundering and terrorist financing, as well as the financing of proliferation of WMD.

3.1.5 FATF Recommendation 1 (assessing risk and applying a risk-based approach) calls on countries to identify, assess and understand their money laundering, terrorist and PF risks, and to take action to effectively mitigate those risks.

3.1.6 In the context of FATF Recommendation 1 (revised in October 2020 together with its interpretive note), PF risk refers strictly to the potential breach, non-implementation or evasion of the targeted financial sanctions (**TFS**) obligations referred to in FATF Recommendation 7[6]. This limits the assessment of risk exposure to the UNSCRs concerning the Democratic People's Republic of Korea (**DPRK**) and the Islamic Republic of Iran (**Iran**). **For this risk assessment Jersey has taken a broader approach to PF risk due to the serious consequences that may follow of failing to address the exposure**.

3.1.7 FATF Recommendation 1 requires that:

3.1.7.1. Countries take commensurate action aimed at ensuring that PF risks are mitigated effectively, including designating an authority or mechanism to coordinate actions to assess risks, and allocate resources efficiently for this purpose.

3.1.7.2. Where countries identify higher risks, they should ensure that they adequately address such risks.

3.1.7.3. Where countries identify lower risks, they should ensure that the measures applied are commensurate with the level of PF risk, while still ensuring full implementation of TFS as required in FATF Recommendation 7.

3.1.7.4. **Financial services businesses**, are required to have processes in place to identify, assess, monitor, manage and mitigate money laundering, terrorist financing and PF.

3.1.8 Other PF relevant FATF Recommendations include:

3.1.8.1. FATF Recommendation 2: requires effective national cooperation and coordination mechanisms to combat PF to be in place

3.1.8.2. FATF Recommendation 15: requires virtual asset service providers (**VASP**) to be regulated for AML/CFT purposes and extends Recommendation 1 to VASPs.

3.1.9 A number of FATF Immediate Outcomes are relevant in assessing effectiveness for PF purposes – Immediate Outcomes 1 and 11.

3.2. PF definition and scope

3.2.1 We have considered the complexities resulting from the absence of an internationally agreed definition of PF. In determining the scope of this risk assessment, we have taken into consideration the FATF's broad working definition, which has been in place since 2010. We accept that there are limitations to this definition, and therefore sought to apply a broader perspective, including consideration of related activities, as well as corporate and financial infrastructure.

3.2.2 This broader assessment perspective is recommended by the Royal United Services Institute (**RUSI**), an independent think-tank that specialises in Defence and Security studies. This broader understanding aligns with the FATF view[7].

3.2.3 FATF's broad working definition:

"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".[8]

3.3. Methodology

3.3.1 Whilst international methodologies for completing money laundering and terrorist financing risk assessments are relatively mature, this is not currently the case for PF risk. Consequently, this PF NRA uses a bespoke methodology encompassing elements of the RUSI risk methodology[9].

3.3.2 Our methodology also closely aligns with the approach used in previous NRAs undertaken by the GOJ and international best practices, in that it:

3.3.2.1. relies on industry data and information held by the competent authorities

3.3.2.2. is completed through collaborative working by Jersey competent authorities

3.3.2.3. considers risk in three parts – threat, vulnerability and consequence

3.3.2.4. adheres to a three-tiered structure approach of identifying, assessing, and evaluating data and information.

3.3.3 The methodology is somewhat different to Jersey's previous assessments in that it follows the RUSI model of assessing PF risk in a broader context rather than a World Bank-based methodology. It takes into consideration that PF abuse tends to be network driven, utilising a three stage PF process to support the development and acquisition of WMDs.[10] This process often involves complex financial transactions and elaborate corporate, financial and people structures and relationships, which can be challenging to demystify and trace.

The PF three stage process

3.3.4 PF, and the laundering it entails, is known to consist of a three-stage process:

3.3.4.1. *Stage 1 - Raising of funds*: Funds are collected through Proliferation State government contracts and budgets. These funds are diverted for illicit PF purposes in the second stage. Funds may also emanate from illicit activities overseas such as ransomware attacks.

3.3.4.2. *Stage 2 - Obscuring of funds and money flows*: Stage 1 funds are laundered into the international financial system, disguising their true origin and destination. This can involve a series of complex financial transactions and parties, such as using middlemen, shell or front companies, complex corporate structuring and network associates, offshore accounts, false invoicing and cryptocurrency transactions. Transactions may initially take place in jurisdictions near sanctioned jurisdictions, using accounts that are owned by foreign nationals (as opposed to Iranian and DPRK nationals).

3.3.4.3. *Stage 3 - Procurement and transport of goods and technology*: The laundered funds are used to obtain materials, technology, parts or expertise needed for WMD development or acquisition. The purchase of goods is often less obvious than buying a particular weapon, since doing so would raise alarm bells. To circumvent the sanctions in place, proliferators often purchase individual component parts and materials that can be used to construct WMDs. Those components may have both a civil use and a military use (known as dual use goods[11]). For example, a smartphone can be used to launch nuclear missiles and hydrogen peroxide can be used to legitimately bleach paper or to act as a missile propellant. Some goods appear on export control lists to seek to manage and control their movements.[12] The JFSC administers Jersey's Sound Business Practice Policy (**SBPP**)[13] which highlights the heightened risk surrounding PF-related activities and dual use goods. To effectively mitigate the PF risk, a clear understanding of supply chains, whereby all parties[14] are aware of the diversion risk posed by illicit procurement efforts, is required to effectively understand, assess, manage and mitigate risks.

Collaborative working

3.3.5 To achieve the greatest understanding of PF risk it is fundamental that competent authorities work collaboratively and engage the private sector. Whilst there is regular and significant inter-agency working in Jersey with respect to TFS implementation and PF, a specific competent authority PF NRA working group was established for the drafting of the PF NRA comprising representatives from the:

3.3.5.1. JFSC, the AML/CFT/CPF regulator

3.3.5.2. Law enforcement and intelligence authorities (the States of Jersey Police, the Economic Crimes and Confiscation Unit (**ECCU**), the Jersey Customs and Immigration Service (**JCIS**), and the FIUJ

3.3.5.3. Financial Sanctions Implementation Unit (**FSIU**)[15].

Risk in three parts

3.3.6 In completing the PF risk assessment Jersey considered PF from various aspects, including the unknown risks, data/information and considering that a threat could reasonably manifest itself in Jersey based on a qualitative assessment.

3.3.6.1. ***Threat***: The intent and capability of natural or legal persons or arrangements, networks or groups, objects or activity, with the potential to cause harm to a State, society, economy etc. through PF-related activities, directly or indirectly financing chemical, biological, radiological and nuclear (**CBRN**) materials or weapons procurement, or through the potential breach, non-implementation or evasion of sanctions (including TFS). This report considered threat actors and threat modalities.

3.3.6.2. ***Vulnerability*****:** Weaknesses or susceptibilities that may be exploited by the threat (by threat actors, via their threat modality models) or that may support or facilitate the breach, non-implementation or evasion of sanctions.

3.3.6.3. ***Consequence*****:** The potential and actual negative impacts whereby funds or assets are made available to proliferators or designated persons.

3.3.7 Consideration has also been given to the strength of controls/mitigants in place.

State threat actors

3.3.8 We have named two Proliferation States (DPRK and Iran) and one State of proliferation concern[16] (Russia) in this NRA. Due to the serious threat that proliferation of WMD and PF present to peace and security (including human life and dignity, the environment and infrastructure etc.), and the significant impact that it would have in terms of harming businesses and the Island's reputation, we also assessed the exposure to PF risk in a wider context, including UK autonomous PF sanctions regimes.

3.3.9 Additional jurisdictions were identified using publicly available source material including academic publications and consideration of PF NRAs of other jurisdictions. The jurisdictions were selected on the basis that they present strong geographical or other links to countries that present an active proliferation or PF threat.[17] Given the rapidly changing nature of international events that may affect any given country's exposure to proliferation and PF, it is not appropriate to include a list of the target jurisdictions (**PF jurisdictions of interest**) in this report, although they were considered as part of our analysis and assessment.

Information and data considered and assessment period

3.3.10 No specific industry data collection was undertaken to complete this risk assessment. Rather data and information held by the competent authorities relating to the two years ended 31 December 2023 (and in some instances also for part of 2024) has been utilised and augmented with additional commentary where material changes have occurred.

3.3.11 The Island decided to conduct its first PF risk assessment at a national level and considered threats and vulnerabilities across the Island as a whole rather than by sector. However, the PF NRA includes an analysis of data and information relating to certain sectors due to their significance to the overall financial services industry and economy in Jersey.

3.3.12 The FSIU considered whether any Sanctions Compliance Reports were of relevance.

3.3.13 The JFSC undertook analysis of jurisdictions of PF concern, identified by the PF NRA Working Group, including the three threat actors referenced in sections 1.3.8 and 4.2 herein. It analysed supervisory risk data and JFSC Registry data for connections with the jurisdictions of PF concern. This included a review of fund flows, natural persons, legal persons, legal arrangements, beneficial owners and controllers, banking branches and subsidiaries, insurance business and permit holders, and any activities that fall within the JFSC's SBPP that could be associated with proliferation or PF. It also considered financial service businesses supervisory performance and any reserve companies[18] in the Island.

3.3.14 The Jersey Ships Registry considered its registration data and how its register may be attractive to abuse by proliferators.

3.3.15 JCIS considered whether any information held on export and import of goods was of relevance.

3.3.16 FIUJ considered whether any SAR information was of relevance.

3.3.17 The Law Officers' Department (**LOD**) analysed whether any incoming Mutual Legal Requests for Assistance were of relevance.

4. PF threats

4.1. Threat modalities

4.1.1 The PF threat was considered through three activity categories (threat modalities) that traditionally impact on the level of PF risk that countries face because of their contextual factors, the vulnerabilities that may lead to those threats materialising, and the consequences thereof, as well as existing measures in place to mitigate the risk.

4.1.1.1. **Trade in proliferation-sensitive technologies and goods, or services and delivery channels supporting the same** – this category concerns products, services and delivery channels that are directly associated with trade in WMD goods. It is most relevant to countries that trade in raw materials (e.g., metals and chemicals) or technologies that are used for proliferation of WMD, or that are involved in the procurement of dual use goods or have technological know-how that is useful for proliferators to progress and sustain their WMD activities.

4.1.1.2. **Other revenue raising activities** – this concerns the exposure to any economic activity that can raise revenue for a proliferator. For example, since DPRK has significant restrictive measures (including TFS) on what economic activity it may undertake outside its territory, it seeks to gain access to revenue streams from:

(i) Legitimate business activities abroad which it can use for its nuclear and missile development programs. This may take the form of, for example, IT services[19], restaurants, building construction, food and textile export, luxury goods trade, sale of natural resources

(ii) Illicit activities such as labour exploitation, cybercrime, counterfeit activities, smuggling of goods, wildlife trafficking and arms and weapons sales. It may also involve the confiscation of Proliferation State nationals' earnings from abroad.

Countries most exposed to this activity category tend to have historic, political and/or diplomatic ties with proliferators.

4.1.1.3. **Corporate and financial infrastructure useful for a proliferator** – this activity category **facilitates** the trade in proliferation-sensitive goods, and revenue raising activities. It also concerns any financial services offered, including to those designated under TFS or trade finance (letters of credit). Proliferators will exploit corporate wealth structuring (shell/front companies and complex structuring) and take advantage of financial services businesses to access the regulated financial system and investment opportunities, often through third party proxies, intermediaries, diplomats and joint venture partnerships. They may also take advantage of cash, hawala systems, trade in gold, or trade in commodities that are non-fungible. Often, they utilise falsification methods or aliases to seek to circumvent restrictive measures and they may target financial services businesses that have weaker AML/CFT/CPF controls, or jurisdictions with weaker monitoring

and oversight mechanisms (e.g., weaker legislative powers or export controls).

4.2. Threat actors

4.2.1 Proliferation States:

4.2.1.1. *DPRK* - a primary threat actor of global PF concern, which continues to develop its nuclear weapons and ballistic missile capabilities.[20] Most economic and financial activity with the DPRK is prohibited through UNSC international sanctions. Such sanctions, alongside UK autonomous sanctions, are immediately and automatically effective in Jersey through SAFL and the SAFL Order. They cover a range of activities including the provisioning of financial services, revenue-generation, caps on oil imports and prohibitions on the provisioning of financial services.[21] The objective of DPRK sanctions is to prohibit DPRK's ability to finance its WMD programme. Open-source intelligence suggests DPRK is becoming actively involved in fighting alongside Russia in Ukraine.[22]

4.2.1.2. *Iran* - a major actor of proliferation concern, which continues to advance its nuclear and missile programmes.[23] To target its proliferation activities and networks, there are a range of activity-based sanctions and TFS in place.[24] Iran also took an active part in the Israel-Hezbollah conflict in 2024, firing ballistic missiles.[25]

4.2.2 States of Proliferation Concern:

4.2.2.1. *Russia* - is not considered an actor of proliferation concern in the context of FATF standards, although it has been suspended from the FATF since February 2023 as a result of its actions with respect to Ukraine. Nevertheless, the UK and other jurisdictions have sanctioned Russian parties for their use of chemical weapons in the UK and on the battlefield in Ukraine. Russia is known for applying sanctions evasion practices to gain access to goods and technology to be used for weapons development purposes[26] and the Russian government and Russian-based entities are understood to have contributed to DPRK and Iranian sanctions evasion.[27] UK autonomous sanctions apply which are immediately and automatically effective in Jersey through SAFL and the SAFL Order, including those associated with military production and engaged in the illicit procurement of Western technologies for integration into its missile systems.[28] Sanctions are significant and varied. They include financial, trade, shipping and immigration sanctions. Other jurisdictions have also noted Russia as a proliferation concern in their NRAs.[29]

5. PF vulnerabilities

5.1. Jersey's PF vulnerability as an IFC

5.1.1 Jersey's status as a leading IFC, while beneficial for competitiveness and attracting foreign customers and investors, also makes the Island vulnerable to exploitation by proliferators. They look to access the global financial system through a reputable jurisdiction that offers a wide range of financial services and technologies to support and obfuscate their activities.

Products and services

5.1.2 Jersey's position in the global economy, and the financial services it offers, makes it particularly susceptible to several threats, including, for example:

5.1.2.1. Payments linked to proliferation-related activities or actors (via PF networks and associates) may pass through Jersey's financial system.

5.1.2.2. Many Jersey-based financial services businesses have extensive global operations. This includes countries that are particularly vulnerable to PF activities, due to the presence of active PF networks or trade with Proliferator States or actors.

5.1.2.3. Even if proliferation-sensitive items or technology are not physically shipped from or through Jersey, the financial transactions related to the trade may be facilitated by Jersey businesses, both directly and indirectly.

Strength of controls/mitigants

5.1.3 Financial services businesses are required to have processes in place to identify, assess, monitor, manage and mitigate money laundering, terrorist financing and PF. Sanctions evasion tactics and PF schemes are often elaborate. For example, it is unlikely that the beneficial owners and controllers will be named designated persons. Financial services businesses must be diligent in their on-boarding, customer due diligence measures, on-going monitoring and scrutiny, to gain clarity as to whether their customers are in fact acting as agents for another, and/or whether the customers, or their associates are connected with proliferators or nefarious activities (see case studies under **Appendix 1**). The evidence collated through JFSC's thematic examinations related to PF suggest that there is still a vulnerability in ensuring full compliance with the regulatory framework:[30]

5.1.3.1. 2023 thematic focused on establishing how well effective measures have been implemented by a limited number of financial services businesses (6) to counter terrorist financing and PF. Key findings were in the area of:

(i) Corporate Governance – for example, failing to adequately consider PF risk as part of their business risk assessment.

(ii) Systems and Controls – for example, limited or no reference to PF in policies and procedures, failure to adequately consider PF risk as part of customer risk assessment and/or at the time of periodic reviews.

(iii) Training and Awareness – for example, failure to provide any or adequate PF and/or TFS training.

5.1.3.2. 2022 sanctions screening effectiveness thematic: 19 out of 23 financial services businesses examined had no findings. The remaining four had one finding each. This suggests businesses understand their screening tools and have in place appropriate oversight of the effectiveness and efficiency of them.

5.2. Other vulnerabilities

5.2.1 Jersey possesses two main ports, the airport and harbour. However, it is not a major transhipment or transit point and is geographically distant from countries of proliferation concern, nevertheless the ports could present a vulnerability to PF abuse. For example, illicit dual use trade has occurred in the region.[31]

5.2.2 The everchanging risk landscape presents challenge for the public and private sector. It may affect access to resources, particularly when significant geopolitical events occur. During the assessment period the escalation of Russian sanctions presented such a challenge and was met.

5.2.3 Based on evidence gathered and engagement with the private sector partners, we concluded that awareness of proliferation procurement methodologies within certain elements of the industrial sector is limited. This lack of PF awareness in parts of Jersey's economy can lead to a lack of understanding of how certain industrial products may be manipulated for hostile use or in CBRN programs, even though it is mitigated due to the limited presence of businesses handling CBRN products on the Island.

5.2.4 The need for businesses to maintain financial viability can sometimes limit their willingness to reject orders that may raise compliance concerns, making these companies particularly vulnerable to approaches from proliferating actors. Furthermore, limited understanding of PF across Jersey's broader economy can mean compliance checks are less effective due to a lack of awareness regarding the activities of PF actors.

5.2.5 Not submitting a SAR as soon as practicable presents an additional vulnerability. Case study 2 in **Appendix 1** suggests a potential failure in this respect. This vulnerability would equally apply in cases where submitting a sanctions compliance report to the Minister is not forthcoming.

5.2.6 Understanding this exposure is important so that we can further refine our mitigation strategies to protect Jersey's economy from exploitation.

6. PF threats and vulnerabilities - identification, mitigation and evaluation

6.1. Regulatory framework, collaborative working, awareness raising and training

Regulatory framework

6.1.1 Jersey maintains a robust regulatory framework to counter the PF risk comprising legislation and regulatory requirements supported by guidance. Its CPF approach closely mirrors that of the UK.

6.1.2 The defence of Jersey falls within the remit of the British Crown and thus the UK Government. As such, Jersey does not have an independent military service and does not produce military grade goods on the Island.

6.1.3 By maintaining a robust legal, regulatory and institutional framework, Jersey effectively addresses the PF risk, contributing to global security efforts and ensuring compliance with international standards.

6.1.4 The authorities also have adequate powers. The Minister has delegated certain statutory functions to members of the FSIU to provide for the more effective implementation of sanctions: powers to require information and documents, and to disclose information. The JFSC also has significant powers under the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 to enforce compliance with the legal and regulatory framework in respect of systems and controls.

Collaborative working

6.1.5 Jersey adopts a whole-government approach to CPF, fostering collaboration and cooperation among government departments and competent authorities. This streamlined approach is facilitated by Jersey's size, which allows for easier cross-departmental coordination and reduces 'red-tape'. For instance, all government departments and agencies involved in CPF work are either located in the same building or within close proximity. Working closely in this way acts as a mitigant to risk exposures.

6.1.6 In 2021 the authorities created the TFS-TF-PF Policy Working Group and in 2022 the PF Operational Working Group (PF OWG) consisting of representatives of the GOJ, FSIU, FIUJ, LOD, ECCU, JCIS, States of Jersey Police (**SOJP**), JFSC, Office of the Jersey Charity Commissioner, and Ships Registry - Ports of Jersey Limited (**PoJ**). Jersey has also entered into several bi-lateral and multilateral agreements.

6.1.7 FSIU works with a wide range of international partners on financial sanctions implementation, engaging – for example – with colleagues in the UK's Foreign, Commonwealth and Development Office (**FCDO**), Office of Financial Sanctions Implementation (**OFSI**) and the Office of Trade Sanctions (**OTSI)** amongst others.

6.1.8 FIUJ is a member of the Egmont Group, facilitating international cooperation and information sharing with other financial intelligence units globally. It also collaborates with other partners such as the International Anti-Corruption Coordination Centre.

6.1.9 Jersey's Ships Registry is a member of Red Ensign Group.

Awareness raising and training

6.1.10 Each competent authority has access to the FATF Academy Introductory E-learning Course and training to the private and public sector is continuous. For example, Jersey held CPF conferences in 2017 and 2023.

6.2. Trade in proliferation-sensitive goods and technologies, or services and delivery channels supporting the same

6.2.1 Jersey's limited direct exposure, noted in this section, does not make us immune from PF risk. The FATF recognises that due to the high volume and cross-border nature of assets managed and transferred, IFCs and trade centres/transshipment hubs may be vulnerable to misuse for the movement and management of funds or assets linked to proliferation activity.

6.2.1.1. Jersey faces limited direct Iranian and DPRK PF threats. This is partly due to our geographical location and lack of involvement in weapons development, manufacturing, research or dissemination of WMD, or the proliferation goods market. The Island has minimal trade relations with Iran and no trade relations with DPRK.

6.2.1.2. There is a greater exposure to Russia based on historic business relations via regulated Trust and Company Services Providers (**TCSPs**), although this has significantly decreased in recent years. For 2023 JFSC's supervisory data from regulated TCSPs included data regarding activities of the Jersey companies they administer - data was received for nearly 24,000 Jersey companies. The data was analysed and limited exposure was identified for the following SBPP activities:

(i) Involvement directly or indirectly, in the exportation or importation of goods or technology, which would require an authorisation or licence under Jersey dual use legislation.

Four Jersey companies reported this activity – none in a PF jurisdiction of interest.

(ii) Manufacture/maintenance/sale/supply/delivery/transfer/purchase/importation/exportation/transportation/financing or financial assistance/use/provision of brokering services/training or technical assistance of/for arms, weapons, ammunitions, countermeasures or other military or defence equipment, goods technology, and personnel involvement directly or indirectly in the same.

Three Jersey companies reported this activity – none in a PF jurisdiction of interest.

(iii) Involvement, directly or indirectly, in mining, drilling or quarrying for natural resources.

211 Jersey companies reported this activity – with 15 Jersey companies reporting the activity with a connection to a PF jurisdiction of interest, none with a connection to DPRK or Iran, one being connected with Russia.

6.2.2 In terms of effectively managing exposure, due to the importance, scale and scope that TCSPs present in the Island, for AML/CFT/CPF purposes many Jersey-TCSPs are regulated and supervised alongside the banking sector (i.e., to a higher extent

than the FATF Recommendations require – FATF treats TCSPs as Designated Non-Financial Businesses and Professions (**DNFBP**)). Jersey's TCSPs act as gatekeepers, providing an additional level of on-going monitoring and scrutiny concerning the activities of companies they administer. This acts as a mitigating factor when it comes to PF threat exposure.

6.2.3 All Jersey persons, including legal persons and arrangements registered with the JFSC Registry as well as Jersey residents, irrespective of whether they operate within or outside Jersey, must equally follow requirements imposed under Jersey's sanctions regimes, some of which are designed to prevent financing being obtained by proliferating actors globally. The sanctions restrict trade and exchange of technological know-how with proliferators.

6.2.4 PF activities may indirectly capture the provision of insurance. The JFSC supervisory data shows that, in terms of general insurance business, no permit holder with the following insurance permit class has declared a connection with any of the PF jurisdictions of interest:

Class	Activity
5	Aircraft
11	Aircraft Liability
6	Ships
12	Liability for ships
7	Goods in transit
3	Land vehicles
10	Motor Vehicle Liability

6.2.5 Proliferators rely heavily on 'third countries' for the transhipment of proliferation-sensitive or other dual-use goods and materials, as well as trade which is prohibited for a particular country or entity. This is done to obfuscate the true end-user, or origin, of the goods, to evade any destination or origin-focused sanctions compliance measures that manufacturers and financial institutions may have in place. Popular transhipment hubs are jurisdictions with significant trade flows and in geographically opportune locations for the movement of goods to and from sanctioned jurisdictions. The threat of being used as a transhipment jurisdiction is likely low for Jersey, as its trade is relatively limited (in comparison to major trading hubs) and well-documented by local authorities.

6.2.6 A large proportion of the DPRK's sanctions evasion activity is conducted through maritime activities. This means that the DPRK relies heavily on its ability to operate vessels in a way to avoid scrutiny. To this end, the DPRK often registers its vessels under the flags of other countries, which host open registries.

6.2.7 While Jersey has two ports, it is not a major transhipment or transit point and it is situated far from countries of proliferation concern. Jersey does not maintain an Aircraft register, but it operates a Ships Register, and vessels can be registered by individuals not resident in Jersey so long as they have a Jersey resident representative. Therefore, there is a possibility that DPRK or DPRK-linked entities may wish to register a vessel in Jersey. The tonnage limit associated with the Jersey Ships Register limits this threat somewhat but does not eliminate it (only vessels below 400GT may be registered). Smaller vessels may still be used for smuggling oil, fish, drugs or other commodities trade prohibited for the DPRK. There is also the possibility that luxury vessels purchased by DPRK entities may be registered in Jersey. The export of luxury goods – including yachts – to DPRK is prohibited under UNSC sanctions.

6.2.8 Jersey recognises the typologies associated with ships and has taken action to address the threat outlined above. For example, in March 2022 the UK amended the Russia (Sanctions) (EU Exit) Regulations 2019 (**Russia Regulations**), imposing a wide range of sanctions against Russian vessels, including prohibiting the registration of ships on the UK Ship Register where they are owned, controlled, chartered or operated by a designated person or persons connected with Russia, or where they are a "specified ship". The FSIU initiated a programme of work to ensure compliance with the Russia Regulations. These discussions concluded with Ministers directing the PoJ to undertake relevant action to take a risk-based and proportional approach to registering/de-registering vessels from the Jersey Ships Registry.

6.2.9 In parallel to the abovementioned activity, GOJ worked with the PoJ and the LOD to introduce an amendment to the Shipping (Registration) (Jersey) Regulations 2004 - Representative Person Law to ensure that, moving forward, it is easier to identify the ultimate beneficial owner(s) of a vessel. The amendment will come into force in June 2025. This will make it easier to enforce compliance with relevant regulations and limit any risks.

6.2.10 The success of Jersey's approach to managing and mitigating the risk posed by its Ships Registry has been recognised by Red Ensign Group members and is being promoted as best practice by the UK FCDO as "best in class" amongst the Red Ensign Group.

6.2.11 Most of Jersey's trade in goods flow via the UK, this trade is regulated by Jersey's Customs Union arrangement with the UK and the other Crown Dependencies[32]. Given trade flows, most goods which enter Jersey would be cleared by Customs at the UK border, therefore significantly reducing the risk of proliferation goods entering Jersey. Additionally, JCIS undertake a sophisticated automated "single trade window" screening process of all goods entering/exiting Jersey against UK Sanctions Lists and the UK's list of dual-use/controlled goods using consignee/consignor details.

6.2.12 Over the course of the last five years, the GOJ has significantly invested in enhancing border security capabilities, including the introduction of new customs IT systems that enable simultaneous and semi-automated checks against sanctions and controlled goods lists.

6.2.13 On 12 September 2024 the UK OFSI issued an Advisory noting that it is almost certain that DPRK IT workers are disguising themselves, for circumvention purposes, as freelance IT workers operating from a country that is not subject to PF sanctions, to provide service to the UK.[33] The Advisory provides a stark reminder of the importance of understanding where goods and services emanate from, to avoid inadvertently supporting sanctions evasion efforts. There is a limited control in financial services businesses as they are required to engage the JFSC concerning any outsourcing that they undertake which may include IT services.[34] Overall, however, currently we do not have adequate information to ascertain how well supply chains are understood and managed, both in terms of products and services.

6.2.14 Jersey is presented with a challenge in varying levels of awareness of PF and trade expertise amongst both the private and public sector, and the ability to detect suspicious behaviour.[35]

6.2.15 The PF risk in respect of this threat modality is considered **Medium Low**.

6.3. Revenue raising activities

6.3.1 Jersey's economy is dominated by the financial sector, accounting for 46% of the total 2023 Gross Value Added (GVA) with the banking sector being the biggest contributor.[36] Jersey is an important IFC and hosts branches of several major international financial institutions. As a result, Jersey may be an attractive and

convenient jurisdiction to set up financial accounts and through which to transact. Jersey's status as a tax-neutral jurisdiction contributes to Jersey's attractiveness for the investment of financial assets and thus the volume of assets that pass-through Jersey's financial system.[37]

6.3.2 DPRK and Iran have been known to transact using accounts in important financial centres, as they provide convenient access to the wider international financial system. As such, Jersey may be targeted by proliferators for the establishment of financial structures and accounts to be used in transactions in support of proliferation-related activity in other jurisdictions.

6.3.3 Tracking DPRK illicit finance through international banking is a difficult task. This is because much of the country's illicit revenue is kept offshore and used to pay creditors and debtors. It is often the case that DPRK and DPRK-linked entities direct creditors to pay debtors, which resembles an 'off-the-books' ledger system and becomes challenging to detect. For example, in cases of illicit labour in West and Sub-Saharan Africa, the payor was directed to remit payments to an oil supplier—thus, completely avoiding any link to DPRK or a DPRK-linked entity.[38] This underscores the importance of the regulated sector monitoring and reporting accounts for pass-through activity or transactions that are not consistent with the stated business purpose or are otherwise suspicious.

6.3.4 Banking Sector: Jersey's robust banking sector, serving a global clientele, can be a target for entities seeking to launder funds destined for proliferation activities. The sheer volume and complexity of transactions processed through Jersey's banks can make it challenging to detect suspicious activities specifically linked to PF. No Jersey companies with a deposit-taking registration have a branch or subsidiaries in any of the PF jurisdictions of interest. Data regarding monies flowing through the Jersey banking sector is collected on an annual basis. Consideration of this shows that no monies were received from or sent to the DPRK or Iran during the assessment period.

6.3.5 Regulated TCSPs: Jersey's financial services industry comprises a substantial number of TCSPs that manage assets and facilitate business transactions for international clients. These services can be exploited by individuals or entities seeking to conceal the origins and destinations of funds, making it difficult to track transactions associated with PF. However, as reported previously this is a highly regulated sector with many TCSPs supervised in the same manner as the banking sector.

6.3.6 VASPs: The DPRK has been known to exploit Virtual Assets (**VA**) and the VA industry to generate revenue for the regime, including through cyber-attacks on VASPs, demands for ransomware payments in virtual assets, crypto jacking[39] and the use of VAs and VASPs for the layering of illicit financial transactions.[40] In the reporting period the attacks have risen for hackers associated with DPRK[41]. There have been less recorded instances of Iranian use of VAs for sanctions evasion, but the country has a significant virtual asset mining industry, which may be used for the generation of revenue[42] or to carry out trade while bypassing restrictions on Iranian transactions within the traditional financial system.[43] Jersey is aware of emerging risks from VAs and has completed a VASP NRA.[44] Whilst the risk assessment was based on data from 2022, the position in 2023 remains largely unchanged. The VASP NRA notes that the VA sector in Jersey is small, and the associated risks are limited. Based on data submitted by Jersey registered VASPs, there are no known connections to, or value transfers to/from, higher risk jurisdictions for PF. There is equally no information for 2022 and 2023 suggesting PF abuse of registered VASPs.

6.3.7 The DPRK has extensively used its diplomatic staff and assets in support of proliferation and PF activities. DPRK diplomats and embassy staff have been known to support sanctions evasion through the establishment of financial infrastructure and

corporate entities abroad; facilitating business connections and brokering business deals – including in the sphere of arms sales; acting as representatives of DPRK businesses; leasing diplomatic real estate and operating businesses out of embassies; as well as smuggling goods and cash across borders in diplomatic luggage.[45] Due to the assets, protections and other privileges granted to diplomats – including their official status – they are well-placed to support sanctions-evasion activity, including PF. There have also been several cases where DPRK diplomats or embassy staff have used the names of their family members to establish accounts, which have then been used to facilitate sanctions evasion activities. London hosts a DPRK embassy; and as there is free movement of people between Jersey and the UK, DPRK diplomats accredited to the UK may be able to travel to Jersey and set up corporate entities or financial accounts or engage in other activities in support of sanctions evasion. A consideration of the vulnerability of Jersey's financial and corporate infrastructure – particularly when it comes to the effectiveness of sanctions screening and other due diligence at point of onboarding – would help further assess the degree to which Jersey is vulnerable to exploitation by DPRK diplomats for PF purposes.

6.3.8 Jersey does not maintain any cultural or diplomatic ties with DPRK, Iran or Russia.

6.3.9 Jersey is not offering flags of convenience, nor does it sell citizenships and/or arrange for citizenships.

6.3.10 The PF risk in respect of this threat modality is considered **Low**.

6.4. Financial and corporate infrastructure abuse

6.4.1 Based on common PF typologies, Jersey cases of potential PF abuse and other financial crime activity in the Island, and the nature of Jersey being an IFC, this is the most likely threat modality to manifest in Jersey.

6.4.2 One of the most common features of sanctions-evasion activities is the use of shell companies to disguise true beneficial ownership information.

6.4.3 Jersey does not permit the establishment of shell companies; it has historically had inactive companies held by regulated TCSPs however implementation of a "fast-track" process for company incorporations means that these "reserve companies" are no longer required and no such companies existed during the assessment period. Jersey was one of the first jurisdictions in the world to implement a company registry.[46] It is leading in its kind with beneficial ownership and control information being accessible by law enforcement and taxation authorities. On 24 February 2025 Jersey enabled obliged entities and their representatives to access the JFSC's Obliged Entity Beneficial Ownership Register and further access is under consideration. The integrity of Registry data is regularly assessed to ensure it remains adequate, accurate and up-to-date. Supervisory inspections are prioritised for businesses that undertake sensitive activity (under the SBPP) or that are linked to high-risk jurisdictions. When inaccurate information is discovered, action is taken to address it. During 2023, the Registry found that inaccuracies had been minor infractions overall.[47]

6.4.4 The Jersey Company Registry includes information regarding the beneficial owners and controllers of Jersey companies. Consideration of the registry for connections to Iran and the DPRK concluded that:

6.4.4.1. no person has a declared nationality, place of birth or address in the DPRK, and

6.4.4.2. 13 individuals were identified with Iranian nationality of which 12 were born in Iran but none have declared Iranian addresses. All

Jesey companies with which these individuals are associated are administered by a regulated TCSP which adds a level of control.

6.4.5 In an effort to consider data as thoroughly as possible with respect to the DPRK and recognising that individuals will try to hide their DPRK connections, an exercise was completed which considered the beneficial owners and controllers of Jersey companies using the top 10 most common names in the Korean peninsula. The top two most common Korean surnames are “Kim” and “Lee”, this caused a level of complexity as these are first names for both males and females in the western world. This complexity was compounded as Korean names are often written as “surname, first name”. In total “Lee” and “Kim” were present in 87% of the identified names of interest. Despite this, based on the work completed no suspicions were raised although many assumptions were required to manage the data and complete the exercise.

6.4.6 There remain historic Russian connections with Jersey. As of 31 January 2025, and in line with the reporting obligations of relevant financial institutions:

6.4.6.1. 408 sanctions compliance reports had been submitted to the Minister in connection with the Russia sanctions regime.

6.4.6.2. The reports concern a number of issues relating to sanctions compliance, including, but not limited to, assets that have been frozen.

6.4.6.3. The reports of frozen assets received by the Minister totalled £1,385,900,000 (rounded to the nearest £100,000).

6.4.7 It is understood that proliferation States and other proliferators are unlikely to be represented themselves in formal registers. They may use close associates or intermediates to act as their proxies to obscure their involvement.[48]

6.4.8 Jersey is a leading jurisdiction for the establishment of corporate entities and trusts. Company incorporation and management is often facilitated by the large number of TCSPs operating in Jersey. Regulated TCSPs are involved in all corporate registrations by non-Jersey residents. The sophistication and supervision of the regulated TCSP sector makes Jersey an attractive jurisdiction, including potentially also for proliferators wanting to appear to undertake legitimate business. They act as gatekeepers and present an additional layer of scrutiny and ongoing monitoring.

6.4.9 Regulated TCSPs have been assessed as having high risk exposure to money laundering in Jersey’s national assessment of money laundering risk.

6.4.10 RUSI’s open-source intelligence research has found that over the last decade, there has been a clear trend whereby DPRK ‘shops’ for jurisdictions with opaque rules and regulations. This is most common in the DPRK’s illicit oil smuggling schemes.[49]

6.4.11 Under the legal and regulatory framework all financial services businesses must establish and maintain appropriate and consistent policies and procedures to counter AML/CFT/CPF/TFS. They must, for example, undertake sanctions screening for all business relationships and one-off transactions. That screening must include customers, their beneficial owners and controllers and other associated parties. Since 1 July 2023, supervised persons must also sign up to receive GOJ and JFSC sanctions notifications. In addition, entities can use PF-TFS risk indicators.

6.4.12 The PF risk in respect of this threat modality is considered **Medium**.

7. Consequences

7.1. Human and environmental cost

7.1.1 Proliferation of WMD, their delivery systems and related materials is a serious concern for all. In the wrong hands, at best, it will cause global instability, threaten peace and security, cause damage to infrastructure, our planet and biodiversity, and/or cause human loss and suffering. At worst, it can have existential consequences.

7.1.2 The DPRK launched an intercontinental ballistic missile (**ICBM**) on 31 October 2024, which reportedly covered approximately 1,000 kilometres, before landing around 200 kilometres from a Japanese island. A United Nations Security Council meeting was held shortly afterwards where Khaled Khiari, Assistant Secretary-General confirmed that "*the DPRK's launch of yet another ICBM is of serious concern and represents a grave threat to regional stability*"[50].

7.2. Reputational and economic damage

7.2.1 Huge reputational damage would be caused should it transpire that parties connected with Jersey have failed in their obligations concerning proliferation and PF. Its impact would not just affect the party concerned, it would also disproportionately affect the Island, businesses and persons associated with us, and those who conduct business in Jersey. It would likely have significant financial consequences too.

7.2.2 Such reputational and economic damage is challenging to restore and it may have a negative impact for years.

7.3. Punitive measures, criminal and regulatory risk

7.3.1 Punitive measures such as sanctions designations may be imposed by the UN.

7.3.2 The relevant competent authorities are committed to exercising their functions and powers fairly and responsibly. Due to the seriousness of proliferation and PF, this may warrant not just supervisory responses such as civil penalties, but also criminal charges.

7.3.3 As such we would encourage prompt and pro-active:

7.3.3.1. reporting of SARs and/or sanctions compliance reports (as relevant) and

7.3.3.2. engagement and candour with the FSIU, law enforcement and the JFSC.

8. Conclusion

8.1.1 Although this report shows that Jersey's safeguarding measures are stringent, there is no room for complacency. On balance, Jersey's main vulnerability is in the second PF process stage of the PF three stage process (obscuring of funds and money flows). This is most likely to occur through corporate and financial infrastructure abuse by proliferators and their associates. This is in line with the typical PF typology whereby complex proliferation networks and tactics are utilised to obfuscate transactions and relationships.

8.1.2 The overall PF risk for Jersey, based on the considerations outlined in this report of threats, vulnerabilities and mitigating measures is considered **Medium-Low**. The key factors supporting this were:

8.1.2.1. Where areas were identified where more information was required to adequately analyse and determine the full extent of the risk, a conservative approach was adopted. The intention is that the relevant information will be collected and considered in the next PF NRA.

8.1.2.2. It is acknowledged that the PF skills base and PF capacity needs to be further developed across the public sector as well as within the private sector.

9. Glossary

Defined terms indicated throughout this document are outlined below. It is not intended that the meanings given below should necessarily be, or become, formal definitions. They are provided only to assist in simplifying the content of this document, making it clear.

AML	Anti-Money Laundering
CBRN	Chemical, Biological, Radiological and Nuclear material and weapons
CFT	Countering of Terrorist Financing
CPF	Countering of Proliferation Financing
DNFBPs	Designated Non-Financial Businesses and Professions
DPRK	Democratic People's Republic of Korea
ECCU	Economic Crimes and Confiscation Unit
FATF	Financial Action Task Force
FCDO	Foreign, Commonwealth and Development Office
Financial services business	as defined in Schedule 2 of the Proceeds of Crime (Jersey) Law 1999 and includes FIs, DNFBPs and VASPs
FIUJ	Jersey Financial Intelligence Unit
FSIU	Financial Sanctions Implementation Unit
GOJ	Government of Jersey
IFC	International Finance Centre
ICBM	Intercontinental Ballistic Missile
Iran	The Islamic Republic of Iran
JCIS	Jersey Customs and Immigration Service
JFSC	Jersey Financial Services Commission
LOD	Law Officers' Department
NRA	National Risk Assessment
OFSI	Office of Financial Sanctions Implementation
OTSI	Office of Trade Sanctions
PEP	Politically Exposed Person
PF	Proliferation Financing
PF jurisdictions of interest	Range of target jurisdictions that were considered during the PF risks assessment process, out of which three were named: DPRK, Iran and Russia.
PoJ	Ports of Jersey

Regulated TCSP	A TCSP that has is registered with the JFSC in accordance with the Financial Services (Jersey) Law 1998
RUSI	Royal United Services Institute
Russia	The Russian Federation
Russia Regulations	The Russia (Sanctions) (EU Exit) Regulations 2019
SAFL	Sanctions and Asset-Freezing (Jersey) Law 2019
SAFL Order	Sanctions and Asset Freezing (Implementation of External Standards) (Jersey) Order 2021
SAR	Suspicious Activity Report
SBPP	Sound Business Practice Policy
TCSP	Trust and Company Services Provider
TFS	Targeted Financial Sanctions
The Minister	The Minister for External Relations
UK	United Kingdom
UN	United Nations
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
VA	Virtual Assets
VASPs	Virtual Asset Service Providers
WMD	Weapons of Mass Destruction

Appendix 1: Case studies

Jersey cases:

Case Study 1: PF-related TFS checks by a Financial Services Business

In 2023, a financial services business submitted a sanctions compliance report in respect of a link between one of its former customers, a Jersey registered company (Company A), one of the directors of Company A (an individual (Person A - not a designated person), and an associated entity (Company B).

The financial services business identified this connection through its automated overnight screening system, with a 'hit' against Person A. The financial services business investigated the matter, carrying out manual screening and discovered the connection between Person A and Company B, as well as in adverse media found online.

Company B was named in the UNSC Panel of Experts report as possibly being connected to PF activity relating to the UNSC DPRK sanctions regime. A subsequent UNSC Panel of Experts report named Company B in the context of links to other companies suspected of involvement in sanctions evasion/proliferation activity.
The financial services business had provided registered office services to Company A of which Person A was the ultimate beneficial owner (as well as being a director). It had not provided any services to Company B.
Company A was neither mentioned in the reports, nor in any adverse media. However, Company A was the Limited Partner in a multi-jurisdictional structure that included Company B.

Person A also had an ownership stake in Company B.

None of the information received by the FSIU to date provides any evidence of any sanctions breach, potential or actual. All information received by the FSIU was shared with, and discussed with, the FIUJ and JFSC. The matter has been referred to the ECCU for consideration.

Case Study 2: A potential failure of a bank to file a SAR on a suspicion related to proliferation of WMD

In 2023, the authorities identified a case of potential failure by an obliged entity to file a SAR to the FIUJ concerning suspicion of money laundering stemming from proliferation of WMD (although not directly associated with the relevant Iran or DPRK UNSCRs).

The source of wealth of a non-resident with an account in Jersey may have resulted from family money associated with illicit proliferation activity. The individual was a Politically Exposed Person due to his relations with an individual, who was widely believed to be a central participant in the black-market trade of nuclear technology. The natural person with a Jersey account had no fixed income, but operated funds received from the family, some of which was used in an attempt to purchase property.

The bank failed to identify the family connection and ties to the U.S. Department of Treasury Office of Foreign Assets Control (OFAC) sanctioned individuals.

The case was initiated in 2023 due to a request from a foreign Financial Intelligence Unit, long after the accounts of the natural person in question were closed in Jersey (in 2017). Only upon receiving a Proceeds of Crime Notice from the FIUJ did the bank file a SAR. The investigation on breaches of the AML/CFT/CPF legislation by the obliged entity is still ongoing.

[1] See MONEYVAL (2024), Anti-money laundering and counter-terrorist financing measures Jersey Fifth Round Mutual Evaluation Report. [Online] Available at: https://www.gov.je/Industry/Finance/FinancialCrime/pages/fatfandmoneyval.aspx. See also Financial Action Task Force (2024), Consolidated Assessment Ratings. [Online] Available at: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-ratings.html

[2] Financial services business is defined in Schedule 2 of the Proceeds of Crime (Jersey) Law 1999 and includes financial institutions (FI), designated non-financial businesses and professions (DNFBPs) and virtual asset service providers (VASPs).

[3] Government of Jersey (2023), *Memorandum of understanding between the Foreign, Commonwealth and Development Office (FCDO) and the Financial Sanctions Implementation Unit (FSIU) concerning proposals for listings and request for de-listing from the United Kingdom and the United Nations sanctions measures in relation to the Bailiwick of Jersey.* [Online] Available at: https://www.gov.je/SiteCollectionDocuments/Industry%20and%20finance/FCDO%20Jersey%20Listing%20Delisting%20MOU%20-%20Signed.pdf

[4] See Section 6.2.2 of the JFSC's Handbook for the Prevention and Detection of Money Laundering, the Countering of Terrorist Financing and the Countering of Proliferation Financing (AML/CFT/CPF Handbook).

[5] FATF Recommendations (February 2012, revised November 2023), *International standards on combatting money laundering and the financing of terrorism and proliferation*. [Online] Available at: https://www.fatf-gafi.org/en/publications/fatfrecommendations/fatf-recommendations.html

[6] FATF Recommendation 7 specifically addresses the need for jurisdictions to implement TFS to comply with UNSCRs relating to PF. It also calls for effective mechanisms to freeze funds and assets, ensuring that financial services businesses are not misused to support proliferation activities.

[7] Page 11, Financial Action Task Force (2021), *Guidance on Proliferation Financing risk assessment and mitigation*. [Online] Available at: https://www.fatf-gafi.org/en/publications/financingofproliferation/documents/proliferation-financing-risk-assessment-mitigation.html

[8] FATF (2010), *Combatting Proliferation Financing: A Status Report on Policy Development and Consultation. [Online] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Status-report-proliferation-financing.pdf*

[9] On 23 February 2023, Jersey finance industry professionals received updates from a RUSI Research Fellow. A full interview, which provides an overview of PF is available here: https://www.youtube.com/watch?v=SQ0PCjrEPDg and here: https://www.youtube.com/watch?v=fOgBSVRnbCc

[10] See Centre for New American Security (2018), *The Financing of WMD Proliferation – Conducting Risk Assessments*. [Online] Available at: https://www.cnas.org/publications/reports/the-Financing-of-WMD-Proliferation

[11] Dual-use items are goods, software, technology, documents and diagrams which can be used for both civil and military applications. They can range from raw materials to components and complete systems, such as aluminium alloys, bearings, or lasers. They could also be items used in the production or development of military goods, such as machine tools, chemical manufacturing equipment and computers.

[12] UK Government (2013), *Guidance: Consolidated list of strategic military and dual-use items that require export authorisation*. [Online] Available here: https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation

[13] Jersey Financial Services Commission (2023), *Sound Business Practice Policy*. [Online] Available at: https://www.jerseyfsc.org/industry/guidance-and-policy/sound-business-practice-policy/

[14] Such parties include, and are not limited to, exporters, re-exporters, manufacturers, distributors, resellers and service providers such as financial services businesses, freight forwarders, warehouse operators and customs brokers.

[15] The FSIU is responsible for implementing an effective sanctions regime and ensuring a whole-Island approach to sanctions implementation in accordance with FATF standards. It coordinates the introduction of sanctions measures and assists the Minister for External Relations (the Minister) (who serves as the Competent Authority) in carrying out their duties and statutory functions.

[16] Pg 14 - Royal United Service Institute "A Guide to Conducting a National Proliferation Financing Risk Assessment: 2024"

[17] For example, they acted as important transhipment or trading hubs, they allowed sanctions evasion practices such as ship-to-ship transfers to occur in their territorial waters, their export and import controls were weak, they facilitated financial transactions of PF concern etc.

[18] These are inactive companies, owned by a trust company business, which is reflected in the JFSC Registry along with details of beneficial ownership and significant persons.

[19] UK Office of Financial Sanctions Implementation (2024), *Advisory on North Korean IT workers.* [Online] Available at: https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

[20] See the United Nations Security Council's (UNSC) Committee Panel of Expert reports for DPRK accessible here: https://main.un.org/securitycouncil/en/sanctions/1718/panel_experts/reports. The important work

of the Committee came to an end in March 2024 when the Russian Federation (Russia) vetoed its continued work, jeopardizing international peace and security, something which was widely condemned. See UK Government (2024), *Press release: Joint statement following Russia's veto of the mandate renewal of the UN Security Council's 1718 Committee Panel of Experts.* [Online] Available at: https://www.gov.uk/government/news/joint-statement-following-russias-veto-of-the-mandate-renewal-of-the-un-security-councils-1718-committee-panel-of-experts

[21] See United Nations (2006), *Security Council Committee Established pursuant to resolution 1718 (2006).* [Online] Available at: https://main.un.org/securitycouncil/en/sanctions/1718

[22] POLITICO (2024), *Videos appear to show North Korean troops at Russian military base.* [Online] Available at: https://www.politico.eu/article/videos-appear-show-north-korea-troops-russia-military-base-nato-ukraine-war-south-korea/

[23] For the UNSC Iranian sanctions regime 18 October 2023 marked the Transition Day under the Joint Comprehensive Plan of Action, when certain restrictions on Iran's nuclear and missile programmes were lifted. However, Jersey automatically and immediately implements UK's autonomous sanctions regime which continues to apply these sanctions to Iran. See UK Government (2023), *Press release: Joint Comprehensive Plan of Action (JCPoA) Transition Day: UK statement*. [Online] Available at: https://www.gov.uk/news/uk-statement-on-joint-comprehensive-plan-of-action-JCPoA-transition-day

[24] See UK Government (2023), *Guidance: Financial sanctions, Iran relating to nuclear weapons.* [Online] Available at: https://www.gov.uk/government/publications/financial-sanctions-iran-nuclear-proliferation and UK Government (2024), *Financial sanctions, Iran.* [Online] Available at: https://www.gov.uk/government/publications/financial-sanctions-iran

[25] Centre for Strategic and International Studies (2024), *Escalating to War between Israel, Hezbollah, and Iran.* [Online] Available at: https://www.csis.org/analysis/escalating-war-between-israel-hezbollah-and-iran

[26] See UK Government (2024), *Guidance: Preventing Russian Export Control and Sanctions Evasion - Updated Guidance for Industry*. [Online] Available at: https://www.gov.uk/government/publications/preventing-russian-export-control-and-sanctions-evasion

[27] Haynes, D. (2013), Russia flew €140m in cash and captured Western weapons to Iran in return for deadly drones, source claims, *Sky News* [9 November] [Online] Available at: https://news.sky.com/story/russia-gave-eur140m-and-captured-western-weapons-to-iran-in-return-for-deadly-drones-source-claims-12741742#:~:text=Russia%20flew%20%E2%82%AC140m%20in%20cash%20and%20a%20selection%20of,a%20security%20source%20has%20claimed.

[28] Royal United Service Institute (2022), *Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine.* [Online] Available at: https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine

[29] See for example the UK: HM Treasury (September 2021), *National Risk Assessment on Proliferation Financing*. [Online] Available here: https://assets.publishing.service.gov.uk/media/65a01397e96df50014f844fe/Risk_assessment_of_proliferation_financing__1_.pdf and the USA: U.S. Department of Treasury (2022), *The National Proliferation Financing Risk Assessment* [Online] Available at: https://home.treasury.gov/system/files/136/2022-National-Proliferation-Financing-Risk-Assessment.pdf

[30] Jersey Financial Services Commission (2024), *Examination findings and questionnaires.* [Online] Available at: https://www.jerseyfsc.org/industry/examinations/examination-findings-and-questionnaires/

[31] Guernsey Evening Press (2024), *Entrepreneur who moved to Sark imported military goods.* [Online] (18 January) Available at: https://guernseypress.com/news/2024/01/18/entrepreneur-who-moved-to-Sark-imported-military-goods/

[32] Government of Jersey (2018), *UK – Jersey Customs Arrangement*. [Online] Available at: https://www.gov.je/Government/Departments/JerseyWorld/pages/relationshipeuanduk.aspx#:~:text=On%2026%20November%202018%20the,Jersey%20and%20the%20United%20Kingdom

[33] UK Office of Financial Sanctions Implementation (2024), *Advisory on North Korean IT workers.* [Online] Available at: https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

[34] Jersey Financial Services Commission (2023), *Outsourcing policy*. [Online] Available at: https://www.jerseyfsc.org/industry/guidance-and-policy/outsourcing-policy/

[35] Partially supported by MONEYVAL (2024), *Anti-money laundering and counter-terrorist financing measures Jersey Fifth Round Mutual Evaluation Report*. [Online] Available at: https://www.gov.je/Industry/Finance/FinancialCrime/pages/fatfandmoneyval.aspx

[36] Government of Jersey (2023), *National Accounts: GVA and GDP.* [Online] Available at: https://www.gov.je/Government/JerseyInFigures/BusinessEconomy/pages/nationalaccounts.aspx

[37] Jersey Finance (2018), *Jersey - A Tax Neutral Jurisdiction.* [Online] Available at: https://www.jerseyfinance.je/our-work/jersey-for-tax-neutrality/#:~:text=Jersey%20as%20a%20tax%20neutral,of%20funds%2C%20assets%20and%20countries

[38] Brewer, J. (2017), *Study of Typologies of Financing WMD*. [Online] Available at: https://www.kcl.ac.uk/csss/assets/study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf

[39] Taking over an unwitting user's computer to mine cryptocurrency without their knowledge.

[40] Royal United Service Institute (2022), *Compliance Harmony: How North Korean Cryptocurrency Abuse Is Expanding*. [Online] Available at: https://rusi.org/explore-our-research/publications/commentary/compliance-harmony-how-north-korean-cryptocurrency-abuse-expanding

[41] Chainalysis (2024), *Funds stolen from Crypto-Platforms Fall More Than 50% in 2023, But Hacking Remains A Significant Threat As Number of Incidents Rises*. [Online] Available here: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/ and Chainalysis (2023), 2022 Biggest Year Ever for Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-Linked attackers. [Online] Available here: https://chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking

[42] Elliptic (2021), *How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil*. [Online] Available at: https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions#:~:text=Bypassing%20Sanctions%20%2D%20Through%20Bitcoin%20Mining&text=Iran%2Dbased%20miners%20are%20paid,financial%20institutions%20to%20be%20circumvented

[43] Reuters (2022), *Iran makes first import order using cryptocurrency – report.* [Online] Available at: https://www.reuters.com/business/finance/iran-makes-first-import-order-using-cryptocurrency-tasnim-2022-08-09/

[44] Government of Jersey (2024), *Virtual Asset Services Providers National Risk Assessment.* [Online] Available at: https://www.gov.je/Industry/Finance/FinancialCrime/NationalRiskAssesmnents/pages/vaspnationalriskassessment.aspx

[45] Royal United Service Institute (2022), From Missions to Missiles: North Korea's Diplomats and Sanctions-Busting, *RUSI.* [Online] Available at: https://static.rusi.org/343_EI_DPRK%20Diplomats.pdf; UNSC (2014), Yun Ho Jin, [Online] Available at: https://www.un.org/securitycouncil/sanctions/1718/materials/summaries/individual/yun-ho-jin; UNSC (2019), Final Report of the Panel of Experts Submitted Pursuant to Resolution 2407 (2018), S/2019/171, [5 March], p. 5; UNSC (2018), Final Report of the Panel of Experts Submitted Pursuant to Resolution 2345 (2017), p. 70; UNSC (2018), Final Report of the Panel of Experts Submitted Pursuant to Resolution 2345 (2017), p. 75.

[46] See for example the World Bank's SAR (Stolen Asset Recovery) Initiative (2011), *The Puppet Masters: How the Corrupt use Legal Structures to Hide their Stolen Assets and What to do About it*.

[47] See JFSC Registrar of Companies Report (2024), *Registry Supervision Inspection Programme 2023 – Quarterly feedback paper - 1 October to 31 December and annual reflection for 2023. Adequate, accurate and current information Assessment.* [Online] Available at: https://www.jerseyfsc.org/media/7396/registry-supervision-inspection-programme-q4-2023.pdf

[48] See for example U.S. Department of Justice (2021), *Iranian Nationals Charged with Conspiring to Evade U.S. Sanctions on Iran by Disguising $300 Million in Transactions Over Two Decades*. [Online] Available at: https://www.justice.gov/opa/pr/iranian-nationals-charged-conspiring-evade-us-sanctions-iran-disguising-300-million#:~:text=WASHINGTON%20%E2%80%93%20A%20federal%20criminal%20complaint,tankers%20%E2%80%93%20on%20Iran's%20behalf%20through and
Royal United Service Institute (2022), The Orlan Complex: *Tracking the Supply Chains of Russia's Most Successful UAV*. [Online] Available at: https://static.rusi.org/SR-Orlan-complex-web-final.pdf and
Royal United Service Institute (2022), *Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine*. [Online] Available at: https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine

[49] Royal United Service Institute (2021), *Project Sandstone Special Report: Black Gold: Exposing North Korea's Oil Procurement Networks*. [Online] Available at: : https://www.rusi.org/explore-our-research/publications/special-resources/project-sandstone-special-report-black-gold-exposing-north-koreas-oil-procurement-networks

[50] DPR Korea's latest missile launch a 'grave threat' to regional stability | UN News