SINGAPORE'S 2024 PROLIFERATION FINANCING (PF) NATIONAL RISK ASSESSMENT AND COUNTER-PF STRATEGY

CONTENTS		
S/N	**Section**	**Page**

EXECUTIVE SUMMARY

The proliferation financing risks posed by the Democratic People's Republic of Korea and the Islamic Republic of Iran continue to be a concern for the United Nations Security Council and international community amid an increasingly volatile external environment. Recognising that Singapore's status as an international financial centre and key trading and transhipment hub makes us susceptible to the risks of proliferation of weapons of mass destruction and proliferation financing, counter-proliferation financing has been long identified as a priority area for Singapore.

To update and deepen Singapore's proliferation financing risk understanding, Singapore carried out a proliferation financing national risk assessment, building on our existing proliferation financing risk understanding and tapping on relevant Singapore authorities and private sector players for a comprehensive assessment. The key findings from our proliferation financing national risk assessment are as follows and summarised in a table on the next page:

- Taking into consideration information from a range of sources including investigations, suspicious transaction reports, intelligence and international typologies (including those featured in the relevant United Nations Security Council Panel of Experts' reports), Singapore faces the key proliferation financing threats of misuse of legal persons, ship-to-ship transfers, movement of dual-use goods, export of luxury goods and misuse of virtual assets. More details can be found in **Section 5: "Singapore's Key Proliferation Financing Threats"**.

- Having identified Singapore's key proliferation financing threats, we ascertained the sectors with greater exposure to these threats. For the financial sectors, the following were identified: banks, digital payment token service providers, remittance agents and maritime insurers; for the non-financial sectors, corporate service providers, precious stones and precious metals dealers, and lawyers. We carried out vulnerability assessments of these sectors, taking into account feedback from sector supervisors and industry. More details of our assessment of these higher-proliferation financing risk sectors can be found in **Section 6: "Singapore's Key Sectoral Vulnerabilities"**.

- To better position ourselves to manage Singapore's key proliferation financing threats and higher-proliferation financing risk sectors, Singapore has developed a counter-proliferation financing strategy. More details can be found in **Section 7: "Singapore's Counter-Proliferation Financing Strategy"**.

All financial institutions and designated non-financial businesses and professions in Singapore (including those sectors that are **not** identified as being exposed to higher proliferation financing risks in **Section 6: "Singapore's Key Sectoral Vulnerabilities"**) and their sector supervisors are reminded to remain alert to proliferation financing risks, and to factor in the findings from this proliferation financing national risk assessment as they review and enhance their counter-proliferation financing controls, policies and measures. Singapore will continue to monitor the evolving proliferation financing risk environment and update our proliferation financing national risk assessment periodically.

Summary of Key Findings from Singapore's Proliferation Financing National Risk Assessment

SINGAPORE'S KEY PROLIFERATION FINANCING (PF) THREATS

- Misuse of legal persons
- Ship-to-ship transfers
- Movement of dual-use goods
- Export of luxury goods
- Misuse of virtual assets

Details can be found in Section 5: "Singapore's Key Proliferation Financing Threats".

SINGAPORE'S HIGHER-PF RISK SECTORS

Taking into account each sector's threats, vulnerabilities and risk mitigation measures:

- Banks are exposed to higher PF risks as compared to the other financial sectors and non-financial sectors in Singapore.
- Digital payment token service providers and corporate service providers are exposed to some PF risks.
- Remittance agents, maritime insurers, precious stones and precious metals dealers, and lawyers are sectors to watch.

Details can be found in Section 6: "Singapore's Key Sectoral Vulnerabilities".

TABLE OF ACRONYMS

2021 FATF Guidance	FATF's June 2021 "Guidance on Proliferation Financing Risk Assessment and Mitigation"
ABS	The Association of Banks in Singapore
ACIP	AML/CFT Industry Partnership
ACRA	Accounting and Corporate Regulatory Authority
AGC	Attorney-General's Chambers
AIS	Automatic identification system
AML/CFT	Anti-money laundering and countering the financing of terrorism
CAD	Commercial Affairs Department
CPF	Counter-proliferation financing
CSP	Corporate service provider
Customs	Singapore Customs
DeFi	Decentralised finance
DNFBP	Designated non-financial business and profession
DPRK	Democratic People's Republic of Korea
DPTSP	Digital payment token service provider
FATF	Financial Action Task Force
FI	Financial institution
FSM DPRK Regulations	Financial Services and Markets (Sanctions and Freezing of Assets of Persons — Democratic People's Republic of Korea) Regulations 2023
FSM Iran Regulations	Financial Services and Markets (Sanctions and Freezing of Assets of Persons — Iran) Regulations 2023
GDP	Gross domestic product
IMC-EC	Inter-Ministry Committee on Export Controls
Iran	Islamic Republic of Iran
JCPOA	Joint Comprehensive Plan of Action
LLP	Limited liability partnership
MAS	Monetary Authority of Singapore
MFA	Ministry of Foreign Affairs
MHA	Ministry of Home Affairs
MinLaw	Ministry of Law
ML/TF	Money laundering and terrorism financing
NRA	National risk assessment
PF	Proliferation financing
PSMD	Precious stones and precious metals dealer
RIER	Regulation of Imports and Exports Regulations
RTIG	Risks and Typologies Interagency Group
STRO	Suspicious Transaction Reporting Office
UN DPRK Regulations	United Nations (Sanctions — Democratic People's Republic of Korea) Regulations 2010
UN Iran Regulations	United Nations (Sanctions — Iran) Regulations 2019
UNSC	United Nations Security Council
UNSC Panel of Experts on the DPRK	Panel of Experts to the Committee established pursuant to UNSCR 1718 (2006)
UNSCR	United Nations Security Council Resolution
VASP	Virtual asset service provider
WG	Work Group
WMD	Weapons of mass destruction

1 INTRODUCTION

1.1 The threat posed by the proliferation of weapons of mass destruction (WMD) and proliferation financing (PF) to international security and the international financial system remains real. The Democratic People's Republic of Korea (DPRK) continues to expand its nuclear and ballistic missile programme, and exploit vulnerabilities such as the anonymity associated with virtual assets. There are also challenges in the implementation of the Joint Comprehensive Plan of Action (JCPOA) involving the Islamic Republic of Iran (Iran)[1]. The United Nations Security Council (UNSC) and international community, including the Financial Action Task Force (FATF), remain highly concerned about PF risks, particularly those posed by the DPRK.

1.2 As an international financial centre and key trading and transhipment hub, Singapore is cognisant that we are susceptible to PF risks. Countering PF has been identified as a priority for Singapore, and PF risks have been in focus since Singapore's 2014 Money Laundering and Terrorism Financing (ML/TF) Risk Assessment Report. Singapore authorities continue to raise the level of industry PF risk awareness and understanding.

1.3 Singapore is fully committed to complying with and implementing the relevant United Nations Security Council Resolutions (UNSCRs), as well as supporting the full and effective implementation of the FATF Standards. The publication of this PF national risk assessment (PF NRA) serves to synthesise and deepen our whole-of-society PF risk understanding. The PF NRA seeks to:

(a) Further uplift the level of awareness and understanding of PF risks among Singapore's financial institutions (FIs), which include digital payment token service providers (DPTSPs)[2], and designated non-financial businesses and professions (DNFBPs), whose gatekeeping roles make them a key line of defence in detecting and preventing PF; and

(b) Support policymakers, law enforcement and sector supervisors so that they will be more targeted in their counter-PF (CPF) policies and strategies and PF risk mitigation measures, which would enhance the effectiveness of Singapore's CPF regime.

[1] The United Nations Security Council Resolution 2231 (2015), which endorsed the JCPOA, terminated all provisions of the United Nations Security Council Resolutions relating to Iran and PF, including 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010) but established specific restrictions including targeted financial sanctions. This lifts sanctions as part of a step-by-step approach with reciprocal commitments endorsed by the United Nations Security Council. Under the JCPOA, Termination Day is in October 2025 where the United Nations Security Council would proceed to terminate the United Nations Security Council Resolution 2231 (2015) and close Iran's nuclear file.

[2] Virtual asset service providers (as defined in the FATF Standards) include DPTSPs.

2 SCOPE AND METHODOLOGY

2.1 Taking reference from the FATF's June 2021 "Guidance on Proliferation Financing Risk Assessment and Mitigation" (2021 FATF Guidance), "PF" refers to the raising, moving or making available of funds, other assets or other economic resources, or financing, in whole or in part, to individuals or entities for the purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technology and dual-use goods for non-legitimate purposes).

2.2 Singapore's PF NRA covers the risks of breach, non-implementation and evasion of all UNSC sanctions imposed on the DPRK and Iran, including activity-based sanctions. This scope is broader than the scope of the FATF Standards (as at the time of writing) which only cover UNSC sanctions (e.g. asset freezing measures) imposed on UNSC-designated individuals and entities. Singapore decided to adopt this wider approach as it would:

(a) Provide a fuller understanding of our PF risks, taking into account Singapore's context (e.g. our status as an international financial centre and key trading and transhipment hub); and

(b) Better reflect the PF risks and typologies that Singapore had come across and observed over the years (e.g. in our law enforcement cases).

2.3 To ensure a comprehensive assessment of our PF risks, Singapore tapped on all relevant agencies including:

(a) Accounting and Corporate Regulatory Authority (ACRA), Singapore's corporate registrar and the supervisor of corporate service providers in Singapore;
(b) Attorney-General's Chambers (AGC), which prosecutes PF-related/proliferation-related cases and is Singapore's central authority for formal international cooperation;
(c) Commercial Affairs Department (CAD) (which is Singapore's primary PF investigative agency), including the Suspicious Transaction Reporting Office (STRO), Singapore's Financial Intelligence Unit;
(d) Ministry of Foreign Affairs (MFA), which chairs the Inter-Ministry Committee on Export Controls (please see **Section 4: "Singapore's Key Counter-Proliferation Financing Framework"** for more information on this Committee);
(e) Ministry of Home Affairs (MHA), the lead policy agency overseeing law enforcement efforts in Singapore, and the joint national anti-money laundering and countering the financing of terrorism (AML/CFT) and CPF Secretariat (with the Monetary Authority of Singapore);
(f) Ministry of Law (MinLaw), the supervisor of precious stones and precious metals dealers and law practice entities in Singapore;
(g) Monetary Authority of Singapore (MAS), the consolidated financial sector supervisor in Singapore, and the joint national AML/CFT/CPF Secretariat (with MHA);
(h) Singapore Customs (Customs), which investigates proliferation cases.

2.4 This assessment was overseen by the Risks and Typologies Interagency Group (RTIG), which is co-chaired by MHA and MAS. The RTIG is the main operational body responsible for identifying and reviewing ML/TF/PF risks, and for Singapore's NRAs. It comprises all operational, law enforcement, regulatory, supervisory and policy agencies involved in AML/CFT work in

Singapore. The RTIG's work is overseen by the AML/CFT Steering Committee and the AML/CFT Inter-Agency Committee[3].

2.5 In addition, we have leveraged our public-private partnership, the AML/CFT Industry Partnership (ACIP)[4] to set up a CPF Work Group (WG) which gathered industry feedback from relevant financial and non-financial sectors (e.g. banks, maritime insurers, lawyers) to enrich the PF NRA.

2.6 In line with the 2021 FATF Guidance, Singapore applied the following methodology to assess our PF risks, which are defined as a function of threats[5], vulnerabilities[6] and consequences[7]:

(a) **Examination of key PF threats to Singapore** – to identify and assess the key PF threats to Singapore, Singapore analysed information from a range of sources such as PF investigations, proliferation investigations, PF-related suspicious transaction reports, PF-related intelligence, PF-related requests for international cooperation via formal and informal channels, and international typologies (including those featured in the UNSC Panel of Experts' reports).

(b) **Analysis of key sectoral vulnerabilities** – for those specific sectors exposed to the key PF threats, we carried out sectoral vulnerability assessments, which included considering how the sectors could be exploited for PF purposes, the strength of the CPF controls within each sector, and industry feedback via surveys and focus group discussions.

(c) **Evaluation of consequences upon specific sectors exposed to key PF threats** – the PF risk level of each sector was assessed as a function of the sector's threats and vulnerabilities (including controls) with consequences deemed as severe generally.[8]

[3] The AML/CFT Steering Committee comprises the Permanent Secretary of MHA, the Managing Director of MAS and the Permanent Secretary of the Ministry of Finance, and drives Singapore's overall AML/CFT/CPF policy coordination. The AML/CFT Inter-Agency Committee is co-chaired by MHA and MAS, and implements the policy decisions made by the AML/CFT Steering Committee.

[4] ACIP is a public-private partnership platform which brings together relevant stakeholders from the Singapore Government and industry to collaboratively identify, assess and mitigate key and emerging ML/TF/PF risks. It is co-chaired by CAD and MAS, and supported by a core group of senior and experienced AML/CFT/CPF compliance officers from the industry.

[5] "Threats": individuals and entities (including UNSC-designated individuals and entities) with the potential to cause harm by breaching, evading or exploiting a failure to implement UNSC sanctions in the past, present or future.

[6] "Vulnerabilities": matters that can be exploited by a threat or that may support or facilitate the breach, non-implementation or evasion of UNSC sanctions.

[7] "Consequences": outcomes where funds or assets are made available to individuals and entities (including UNSC-designated individuals and entities) with the potential to cause harm.

[8] Given Singapore's context, the consequences would be more severe where there is a cross-border element and less severe otherwise.

3 SINGAPORE'S RISKS AND CONTEXT

3.1 Located in Southeast Asia, Singapore's strategic geographical location has enabled us to develop into a key trading and transhipment hub.[9] Situated along the vital shipping lanes in the Straits of Malacca, Singapore is one of the busiest ports in the world, connected to more than 600 ports in over 120 jurisdictions and with more than 140,000 vessel calls annually. In addition, Singapore has strong global connectivity with an airport serving over 100 airlines flying to over 300 cities in about 80 jurisdictions worldwide.

3.2 In 2023, Singapore's gross domestic product (GDP) at current market prices was S$673.3 billion, with per capita GDP of S$113,779. Singapore's top trading partners are China, Malaysia, the US and the European Union.

3.3 Singapore is a dynamic international business and financial centre, characterised by an open and diversified economy, well-developed business infrastructure and an efficient financial system. We have been ranked by the International Monetary Fund as one of 29 systematically-important financial centres in the world, and Singapore is host to more than 1,000 FIs offering a wide variety of financial products and services and serving a broad and diverse customer base. Singapore's financial centre is dominated by banks and is one of the world's fastest-growing wealth management centres, primarily due to the wide range of wealth management services offered. As of 2023, Singapore had about S$5.4 trillion assets under management with about 77% of the funds sourced from outside Singapore.[10]

3.4 Singapore is also known as a FinTech hub with a digitally-savvy population and ease of access to digital financial services, including those related to virtual assets.

3.5 Given Singapore's context, we are inherently exposed to PF threats and activities, as well as ML/TF threats and activities. Please refer to Singapore's updated Money Laundering National Risk Assessment and Terrorism Financing National Risk Assessment for more details.

[9] Singapore's updated Money Laundering National Risk Assessment, page 12
[10] MAS' "Singapore Asset Management Survey 2023"

4 SINGAPORE'S COUNTER-PROLIFERATION FINANCING FRAMEWORK

4.1 For an effective CPF regime, there should be:

(a) A robust CPF regulatory framework;
(b) Strong interagency cooperation and coordination;
(c) A well-functioning export controls regime;
(d) Targeted supervisory efforts and decisive law enforcement action;
(e) Strong international cooperation.

These various facets of Singapore's CPF framework are described in this section.

(A) Robust CPF regulatory framework

4.2 Singapore has given effect to the UNSCRs relating to the DPRK and Iran through the enactment of various legislative instruments including:

(a) Financial Services and Markets (Sanctions and Freezing of Assets of Persons — Democratic People's Republic of Korea) Regulations 2023 (FSM DPRK Regulations);
(b) Financial Services and Markets (Sanctions and Freezing of Assets of Persons — Iran) Regulations 2023 (FSM Iran Regulations);
(c) United Nations (Sanctions — Democratic People's Republic of Korea) Regulations 2010 (UN DPRK Regulations);
(d) United Nations (Sanctions — Iran) Regulations 2019 (UN Iran Regulations).

4.3 The FSM DPRK Regulations and FSM Iran Regulations are applicable to FIs in Singapore, and the UN DPRK Regulations and UN Iran Regulations applicable to individuals and entities (including DNFBPs but excluding FIs) in Singapore and Singapore citizens outside Singapore. These Regulations are compliant with the relevant UNSCRs in place, including the activity-based sanctions such as the prohibition against providing financial services that may contribute to any trade with the DPRK[11].

4.4 Any changes to the relevant UNSC sanctions lists would be given immediate effect domestically.[12] The obligations to freeze the assets of, and to not deal with, UNSC-designated individuals and entities would thus apply immediately, and any frozen assets should be reported to the relevant Singapore authorities as soon as possible. FIs and DNFBPs that subscribe to MAS' website would be alerted when there are updates to the relevant Regulations and UNSC sanctions lists.

(B) Strong interagency cooperation and coordination

4.5 As mentioned in paragraph 2.4, the RTIG is the main operational body responsible for identifying and reviewing ML/TF/PF risks. Its work is overseen by the AML/CFT Steering Committee, which drives Singapore's overall AML/CFT/CPF policy coordination and is supported by the AML/CFT Inter-Agency Committee. The AML/CFT Inter-Agency Committee implements the policy decisions made by the AML/CFT Steering Committee.

[11] Please see regulation 10 of the FSM DPRK Regulations for the specific prohibitions.
[12] Any changes to a UNSC sanctions regime are carefully considered and assessed by Singapore authorities before domestic legislation is amended.

4.6 The AML/CFT Steering Committee, AML/CFT Inter-Agency Committee and RTIG work closely with the Inter-Ministry Committee on Export Controls (IMC-EC) which oversees Singapore's export controls framework, including relevant policy and operational issues relating to the proliferation of WMD and PF. The IMC-EC is chaired by MFA and comprises relevant policy and law enforcement agencies.

4.7 The IMC-EC monitors Singapore's implementation of relevant UNSCRs. This Committee, through the Permanent Mission of the Republic of Singapore to the United Nations in New York, is also Singapore's focal point on sanctions-related engagements with the UNSC, including the relevant UNSC Panels of Experts.

4.8 In addition, the IMC-EC coordinates interagency follow-ups (including enforcement action by law enforcement agencies) when Singapore receives information/intelligence relating to the proliferation of WMD and PF.

(C) Well-functioning export controls regime

4.9 Even if all the other aspects of a CPF regime (as described in this section) are in place, the regime would not be able to effectively counter PF without the support of a robust export controls regime to curb the proliferation of WMD. In Singapore, the regulation of the export, transhipment, transit and brokering of strategic goods[13] and strategic goods technology is implemented through the Strategic Goods (Control) Act and its subsidiary legislation.

4.10 Besides having a strong strategic goods control system, Singapore implements UNSC trade prohibitions through the Regulation of Imports and Exports Regulations (RIER) which prohibit the import into, export from, transhipment in and transit through Singapore of specific goods – any changes to the trade prohibitions in the UNSCRs related to the DPRK and Iran are implemented via regulation 6(1)(b) of the RIER. Since 8 November 2017, Singapore has prohibited the import into, export from, transhipment in and transit through Singapore of all commercially-traded goods from or to the DPRK. This prohibition goes beyond the DPRK-related UNSCRs and reflects our firm anti-proliferation stance.

(D) Targeted supervisory efforts and decisive law enforcement action

4.11 To ensure FIs' and DNFBPs' compliance with the FSM DPRK Regulations, FSM Iran Regulations, UN DPRK Regulations and UN Iran Regulations, sector supervisors cover CPF in the course of their regular AML/CFT supervision (e.g. onsite inspections, offsite engagements, surveillance).

4.12 Sector supervisors also conduct outreach and have issued guidance to raise industry's awareness of their CPF obligations, PF risks and recommended PF risk mitigation measures. For higher-risk sectors, sector supervisors engage them more closely.

4.13 When breaches of our laws are detected, Singapore has taken action against non-compliant individuals and entities. Upon receiving credible and actionable information/intelligence via the IMC-EC mechanism or from their international counterparts, Singapore law enforcement agencies (CAD and Customs) would assess whether there are reasonable grounds to commence a PF or proliferation investigation in Singapore. Where necessary, law enforcement would work with other Singapore agencies and international counterparts to build a case and net a

[13] "Strategic goods" refer to military goods or dual-use goods listed in the Strategic Goods (Control) Order. As defined in the Strategic Goods (Control) Act, "dual-use goods" are goods capable of being used for both a non-military purpose and a military purpose or relevant activity, and "military goods" are goods solely or predominantly designed or modified for a military purpose, including any part or component thereof.

successful prosecution. From 2019 to 2023, law enforcement and AGC successfully prosecuted 22 individuals and eight entities for PF-related/proliferation-related breaches of Singapore's laws, including some that have been featured in the case studies in **Section 5: "Singapore's Key Proliferation Financing Threats"**.

(E) Strong international cooperation

4.14 Given the transnational nature of WMD proliferation and PF schemes (e.g. abuse of front companies, shell companies, FIs and other intermediaries across multiple jurisdictions to evade sanctions controls), there is a need for strong international cooperation in our fight against PF.

4.15 It is hence important that Singapore agencies exchange information/intelligence relating to WMD proliferation and PF with international counterparts via the IMC-EC mechanism, as well as bilaterally. Singapore agencies (including CAD, Customs, MAS and MFA) maintain warm relations and have regular engagements with international counterparts, which have helped agencies and their counterparts to remain alert to emerging typologies and develop cases. Singapore also has regular dialogues with key international partners (e.g. the annual Singapore-US Counter-Proliferation Dialogue where a variety of counter-proliferation and CPF issues are discussed; the annual bilateral meeting between Customs and the US Bureau of Industry and Security to discuss strategic goods licensing and enforcement matters).

5 SINGAPORE'S KEY PROLIFERATION FINANCING THREATS

5.1 As mentioned in **Section 2: "Scope and Methodology"**, to identify the key PF threats to Singapore, Singapore considered information from a range of sources e.g. PF investigations, proliferation investigations, PF-related suspicious transaction reports, PF-related intelligence, PF-related requests for international cooperation via formal and informal channels, and international typologies (including those featured in the UNSC Panel of Experts' reports). Specifically, Singapore has observed the following:

- From PF-related intelligence that Singapore had received from our international partners from 2019 to 2023, ship-to-ship transfers (around 45%), movement of dual-use goods (around 20%) and export of luxury goods (around 20%) were the three areas featured the most commonly in the intelligence received.

- From PF investigations initiated by Singapore authorities from 2019 to 2023, we noted that the misuse of legal persons (around 17% of investigations), misuse of virtual assets (around 17%), export of luxury goods (around 25%) and ship-to-ship transfers (around 42%) were the most commonly featured in the investigations. In terms of sectors, the banking sector was featured the most commonly.

Further details of the key PF threats identified can be found in this section.

(A) Misuse of legal persons

5.2 Legal persons (e.g. companies) have been known in some instances to be used by proliferators to evade sanctions imposed on the DPRK and Iran. For instance, this was observed in cases in Singapore, as well as noted by the Panel of Experts to the Committee established pursuant to UNSCR 1718 (2006) (UNSC Panel of Experts on the DPRK)[14] and in the 2021 FATF Guidance[15] which stated that both the DPRK and Iran frequently use front companies, shell companies, joint ventures and complex and opaque ownership structures to circumvent the DPRK-related and Iran-related UNSCRs. It was also noted in the 2021 FATF Guidance[16] that shell companies, which can be relatively quick and simple to set up, provide UNSC-designated individuals and entities with the ability to conduct business anonymously. Such companies can be used for a brief period of time to move monies for a particular transaction or series of transactions, and UNSC-designated individuals and entities have been found to use extensive networks of shell companies. Apart from tapping on the traditional banking system, UNSC-designated individuals and entities may seek the services of professionals such as company service providers and lawyers in the creation or management of legal persons to provide respectability and legitimacy to their activities.

5.3 As noted, in Singapore's context, Singapore authorities have observed the misuse of legal persons for PF purposes (e.g. use of Singapore operating companies, including those which are long-established, to trade with sanctioned entities with transactions layered through front companies and accounts in third countries; setting up of separate legal persons to ringfence sanctioned activities; use of shell companies set up by foreign beneficial owners with little or no substantial business operations in Singapore[17]). The following case shows how companies

[14] E.g. the UNSC Panel of Experts on the DPRK's report dated 7 March 2023 (page 54) stated that "the use of shell and front companies to layer business transactions is a known tactic used to evade sanctions".
[15] 2021 FATF Guidance, page 25
[16] 2021 FATF Guidance, pages 41 and 42
[17] MAS' August 2018 guidance paper, "Sound Practices to Counter Proliferation Financing"

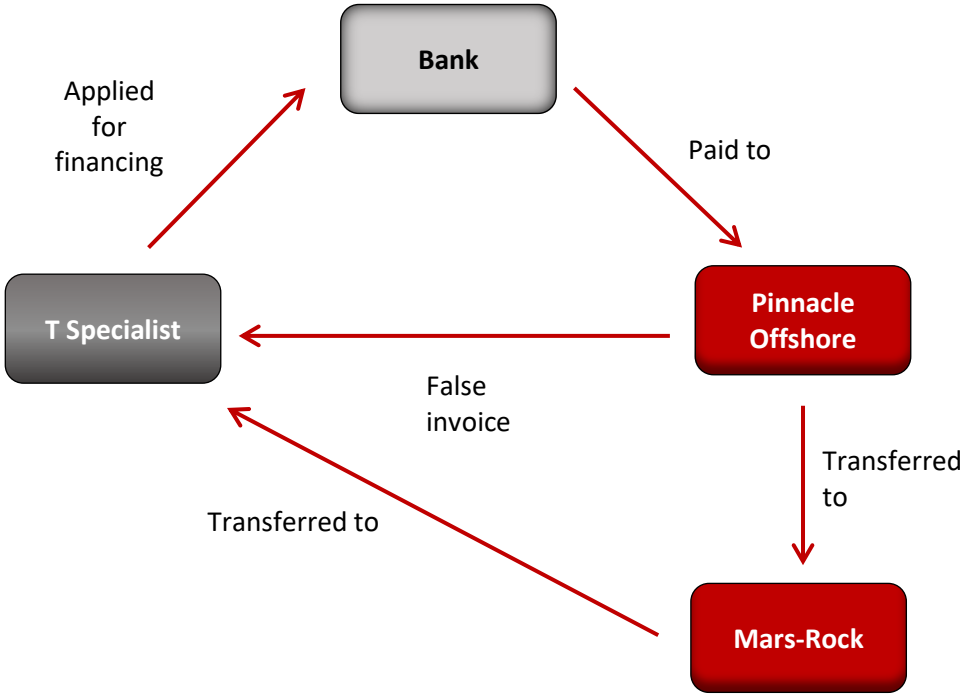
were misused using ML techniques in connection with violations of UNSC sanctions (i.e. export of luxury goods to the DPRK which is prohibited).[18]

CASE STUDY 1 – Use of companies and false documentation

This case illustrates how Singapore actively followed up on intelligence received from an international partner and initiated a domestic investigation.

From 2010 to 2017, Ng Kheng Wah (Ng), through T Specialist International (S) Pte Ltd (T Specialist), supplied prohibited luxury items amounting to more than S$6 million to the Korean Bugsae Shop, a departmental store chain in the DPRK, in breach of regulation 5(a) of the UN DPRK Regulations.

When the owner of the Korean Bugsae Shop failed to make timely payments for the items received, Ng devised an invoice-financing fraud scheme to generate liquidity for T Specialist. Ng used 81 invoices purportedly issued by Pinnacle Offshore Trading Inc (Pinnacle Offshore), owned by Wang Zhiguo (Wang), to T Specialist to deceive five banks into granting more than US$95 million in trade financing loans to T Specialist for the non-existent sale of items from Pinnacle Offshore to T Specialist. The banks were deceived into making payments of the invoice amounts to Pinnacle Offshore, which then transferred these funds to the bank accounts of T Specialist and its affiliated companies such as Mars-Rock Offshore Trading (Mars-Rock). This scheme is depicted in the diagram below.



Ng pleaded guilty to 10 charges of abetment by engaging in a conspiracy to supply designated luxury items to the Korean Bugsae Shop in the DPRK in breach of regulation 5(a) of the UN DPRK Regulations, and 10 charges of abetment by engaging in a conspiracy to cheat the banks under section 420 read with section 109 of the Penal Code. 69 similar charges for contravening regulation

[18] For instance, in a 2022 Royal United Services Institute commentary, "Three Key Takeaways from the Latest Panel of Experts Report on North Korea" by Dr Aaron Arnold, it was observed that "Last year's Pandora Papers leak – another in a now long and growing list – shined a light on how wealthy elites hide their cash behind companies with opaque ownership structures. It should come as no surprise that North Korean operatives use the same channels and infrastructure to disguise their identities – enabling access to otherwise restricted financial services".

5(a) of the UN DPRK Regulations and 71 similar cheating charges were also taken into consideration for sentencing. Ng was sentenced to a total imprisonment term of 34 months.

T Specialist was convicted of 10 charges for contravening regulation 5(a) of the UN DPRK Regulations, and two charges of acquiring benefits from criminal conduct under section 47(1)(c) punishable under section 47(6) of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA). 69 similar charges for contravening regulation 5(a) of the UN DPRK Regulations and six similar CDSA charges were also taken into consideration for sentencing. T Specialist was fined a total of S$880,000 for its offences.

Wang was convicted of 10 charges of abetment by engaging in a conspiracy to cheat the banks under section 420 read with section 109 of the Penal Code. 71 similar charges were taken into consideration for sentencing. Wang was sentenced to a total imprisonment term of 12 months.

(B) Ship-to-ship transfers

5.4 As noted by the UNSC Panel of Experts on the DPRK[19] and in the 2021 FATF Guidance[20], UNSC-designated individuals and entities use the maritime sector to deliver components and materials for use in WMD or their delivery systems, and generate revenue which can provide the underlying financing for a WMD programme. Tactics adopted include ship-to-ship transfers and false shipping documentation to conceal a shipment's origin or destination.

5.5 In Singapore's context, Singapore authorities have observed the use of the maritime sector for PF purposes – this could include the misuse of shipping companies, ship charterers, shipping logistics companies, as well as maritime insurers. In particular, CAD has investigated a number of ship-to-ship transfer cases including the following.

CASE STUDY 2 – Ship-to-ship transfers and use of false documentation

Arising from agencies' surveillance, Singapore uncovered that from September 2019 to November 2019, Kwek Kee Seng (Kwek) 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 supply was facilitated through ship-to-ship transfers on the first six occasions and took place at the Nampo Port in the DPRK on the last occasion. The alleged acts constitute a violation of the UN DPRK Regulations.

In order to facilitate the payments for the purchase and supply of gasoil to the DPRK, Kwek allegedly utilised the bank account of a company, of which he was a director, on four occasions. He also allegedly falsified documents belonging to the company on two occasions. In addition, on five occasions, Kwek allegedly utilised the bank account of another company under his control to receive payments for the prohibited supply of gasoil to the DPRK.

Kwek also allegedly lied to the investigation officer and disposed of evidence pertaining to his involvement in the supply of gasoil to the DPRK, and allegedly failed to inform the Police about the supply of gasoil to the DPRK by another vessel in February 2019.

[19] E.g. Annex 44 of the UNSC Panel of Experts on the DPRK's report dated 1 March 2022 described a number of evasion methods such as the transmission of falsified or inconsistent automatic identification system identifiers, reporting of false destinations, changing of flag registries in quick succession (also known as flag-hopping), use of layered ownership and management structures, use of front companies and shell companies and use of multiple intermediaries.

[20] 2021 FATF Guidance, page 24

Consequently, Kwek has been charged with the following offences:

- Seven counts of supplying a designated export item to a person in the DPRK in contravention of regulation 5(a) of the UN DPRK Regulations;
- Two counts of falsification of accounts under section 477A of the Penal Code;
- Five counts of acquiring benefits from criminal conduct under section 47(3) read with section 59 of the CDSA;
- Two counts of obstructing the course of justice under section 204A of the Penal Code; and
- One count of failing to provide information about a prohibited transaction in contravention of regulation 14(1)(c) of the UN DPRK Regulations.

Additionally, the first company of which Kwek was a director has been charged with four counts of transferring financial assets that may contribute to a prohibited activity in contravention of regulation 12(1)(b) of the UN DPRK Regulations and the second company faces five counts of acquiring benefits from criminal conduct under section 47(3) of the CDSA. Court proceedings are ongoing.

(C) Movement of dual-use goods

5.6 As noted by the UNSC Panel of Experts on the DPRK[21], although international sanctions and UN Member States' controls are significantly reducing the procurement and proliferation possibilities for the DPRK, the DPRK has continued to seek dual-use components and technology needed for its WMD programme. It has also been noted[22] that Iran maintains an extensive overseas network of procurement agents, front companies, intermediaries and suppliers to obtain sensitive dual-use items. These procurement networks use a variety of methods to evade export controls and sanctions including obscuring the end-users through a layered approach, falsifying end-use documentation and shipment details, routing shipments through several jurisdictions, and using deceptive tactics to access the international financial system.

5.7 In Singapore's context, given Singapore's status as a key transhipment and transit hub, we could be used as a gateway to move dual-use goods for eventual use in WMD-related programmes or activities. Customs has come across such cases including the following.

CASE STUDY 3 – Interdiction of shipment to Iran

Based on information received alleging that a shipment of 10 containers of sodium chlorate transhipping through Singapore was destined for Iran's weapons industries, Customs offloaded and inspected the 10 containers. The shipment, which came from an Asian jurisdiction, was to be transhipped through Singapore in December 2023 with the declared destination purportedly a jurisdiction in the Middle East. Sodium chlorate is used in the manufacture of ammonium perchlorate, a controlled item under the Strategic Goods (Control) Order (SGCO), and as an oxidiser for solid rocket fuel.

[21] UNSC Panel of Experts on the DPRK's report dated 1 March 2022, page 14

[22] "Iran Ballistic Missile Procurement Advisory" dated 18 October 2023 issued by the US Department of Commerce, the US Department of State, the US Department of the Treasury and the US Department of Justice

Given the facts of the case, Customs exercised its catch-all controls[23] and issued a relevant activity[24] notification under section 5(2)(d) of the Strategic Goods (Control) Act (SGCA) to deny the shipment's onward journey to Iran and for the shipment to be returned to the Asian jurisdiction. This case illustrates how Singapore was able to disrupt the journey of a shipment of proliferation concern to Iran even without any conviction of any individual or entity in Singapore.

5.8 While the dual-use goods in the following case were not destined for the DPRK or Iran, the case illustrates how Singapore had identified and acted against false end-use documentation which concealed the actual end-user of such dual-use goods.

CASE STUDY 4 – Movement of dual-use goods

Customs investigated into Hydronav Services (Singapore) Pte Ltd (Hydronav) based on information alleging that the company had exported strategic goods from Singapore to Myanmar without a permit (which is required under section 5(1)(a) of the SGCA). The investigation revealed that Hydronav's sales manager, Poiter Agus Kentjana (Poiter) oversaw the sale of a multibeam echosounder system (EM system) to an entity in Myanmar. The EM system, procured from an entity in Norway, is a controlled item under the SGCO. Hydronav did not obtain the requisite SGCA permit to export the EM system even though both Poiter and a director of Hydronav, Wui Ong Chuan (Wui) were aware that the EM system was subject to controls under the SGCA.

The investigation also revealed that Poiter falsely submitted an end-user statement to the Norwegian authorities stating that the EM system was intended for an end-user in Indonesia to deceive the Norwegian authorities into approving the export of the EM system from Norway to Singapore. Poiter did so because two prior applications submitted by Hydronav that listed an entity in Myanmar as the end-user had been rejected by the Norwegian authorities. He subsequently made a false police report in Indonesia to claim that the EM system had been stolen when the manufacturer of the EM system asked to inspect the installation of the EM system in Indonesia. Wui was aware of the false end-user statement and false police report made by Poiter. As both instances were cheating offences under the Penal Code, the case was referred to the Police for investigation.

Customs' investigation further uncovered that in July 2017, Hydronav had also exported an unmanned aerial vehicle (UAV), a controlled good listed under the SGCO, to Myanmar for a demonstration and without the requisite permit under the SGCA even though Wui was aware that the UAV was subject to export controls.

Hydronav, Wui and Poiter were fined S$1.13 million, S$45,000 and S$35,000 respectively for offences under the SGCA and the Penal Code.

[23] "Catch-all controls" refer to the control of goods or technology which are not specified in the SGCO but are intended or likely to be used for nuclear, chemical or biological weapons purposes, including missiles which are capable of delivering any such weapon.

[24] Under the Strategic Goods (Control) Act, "relevant activity" is defined as: (a) the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of any nuclear, chemical or biological weapon; or (b) the development, production, maintenance or storage of missiles which are capable of delivering any such weapon.

(D) Export of luxury goods

5.9 The export of luxury goods to the DPRK is a longstanding area of concern for the UNSC as the monies used to fund these goods could be from illicit sources. The UNSC Panel of Experts on the DPRK has noted that the partial reopening of the DPRK's borders in 2023 (after the COVID-19 pandemic) had facilitated the reappearance in retail trade of a large variety of foreign goods including some that could be considered luxury goods (e.g. new foreign-made vehicles).[25] The Panel further noted in 2024[26] increased transhipments of luxury goods to the DPRK via third countries, and recommended that entities which are in the business of exporting luxury goods should be more vigilant when arranging shipments to the region and via entrepot zones while the Panel continued to investigate possible networks involved in the illegal supply of luxury goods to the DPRK.

5.10 The export of luxury goods to the DPRK is thus an area that Singapore (including the private sector) has remained alert to, especially since we have observed a few cases including Case Study 1 and the following case.

CASE STUDY 5 – Export of luxury goods to the DPRK

A shipment of red wine and assorted fruit juices from South Africa was to be transhipped through Singapore to China in January 2020. Upon inspection by Customs, a total of 1,158 cartons of red wine and 174 cartons of assorted fruit juices were detected. The consignee indicated in the shipping documents was a China-based entity while the consignee indicated in the commercial invoice was Sangmyong General Trading Corp. Sangmyong General Trading Corp had been mentioned in the UNSC Panel of Experts on the DPRK's reports in 2012 and 2013 for its involvement in the shipping of luxury goods to the DPRK.

Regulation 5(a) of the UN DPRK Regulations prohibits any person in Singapore and any citizen of Singapore outside Singapore from supplying, selling or transferring, directly or indirectly, any designated export item or designated luxury item to any person in the DPRK, whether or not the item originated in Singapore. Wine is a designated luxury item while fruit juices are designated export items specified in the Seventh Schedule to the RIER. Hence, the shipment was seized by Customs as there was a contravention of regulation 5(a) of the UN DPRK Regulations.

An application for the forfeiture of the seized goods was made to the Singapore District Courts, and due notice was given to parties that might be interested in the seized goods. However, no party turned up during the forfeiture hearing to contest the forfeiture or to claim the seized goods. The goods were eventually forfeited under regulation 17(1) of the UN DPRK Regulations. This case demonstrates how Singapore was able to disrupt the flow of prohibited items to the DPRK even without having to secure a conviction against any individual or entity in Singapore.

CASE STUDY 6 – Export of commercially-traded goods to the DPRK

Arising from intelligence, Customs conducted an investigation into a case involving the potential supply and export of prohibited goods to the DPRK through Dalian, China and Klang, Malaysia. Its investigation revealed that from November 2017 to September 2018, a Singaporean, Phua Sze Hee (Phua), then-manager at Pokka International Pte Ltd (Pokka), sold Pokka-branded beverages with a total value of around S$1.30 million to Singapore companies knowing that these beverages would

[25] UNSC Panel of Experts on the DPRK's report dated 12 September 2023, page 45
[26] UNSC Panel of Experts on the DPRK's report dated 7 March 2024, page 32

end up being exported to the DPRK for commercial trade. One of these companies was A-linkz Marketing Pte Ltd (A-linkz). Tay Kiong Chiak (Tay), a director of A-linkz, purchased the beverages for S$110,032 from Phua and subsequently exported the beverages to the DPRK.

Regulation 6(2)(c)(ii) of the RIER prohibits any exportation from, transhipment in or transit through Singapore of any goods that are for the purpose of trade with any person in the DPRK with these prohibitions going beyond the DPRK-related UNSCRs. Phua and Tay were accordingly convicted for breaches of regulation 6(2)(c)(ii) of the RIER and sentenced to five weeks' imprisonment and 12 days' imprisonment respectively. This case demonstrates how Singapore has adopted tighter sanctions-related measures than those in the UNSCRs and enforced these measures in practice even for the illegal export of non-luxury goods.

(E) Misuse of virtual assets[27]

5.11 In its 2023 report[28], the UNSC Panel of Experts on the DPRK indicated that it continued to investigate the violations of the UNSC financial sanctions by DPRK cyberactors, and noted that illicitly-obtained virtual assets are protected by both the anonymity of the blockchain and the intentional obfuscation of the passage of assets through cryptocurrency exchanges. Chainalysis noted in February 2024 that DPRK-linked hacks have been on the rise over the past few years with cyber-espionage groups such as Kimsuky and Lazarus Group utilising various malicious tactics to acquire large amounts of virtual assets – DPRK-linked hackers apparently stole about US$428.8 million from decentralised finance (DeFi) platforms in 2023, and targeted centralised services (US$150 million stolen), exchanges (US$330.9 million) and wallet providers (US$127 million).[29]

5.12 Additionally, the FATF observed in 2023[30] that the DPRK's illicit virtual assets-related activities (including ransomware attacks and sanctions evasion) for PF purposes had enabled an unprecedented number of recent launches of ballistic missiles (including intercontinental ballistic missiles) – this threat is significant given both the scale of the funding (US$1.2 billion worth of stolen virtual assets since 2017 including virtual assets stolen from DeFi arrangements) and the serious consequences of PF. The FATF further noted in 2024[31] that virtual assets continue to be used to support the proliferation of WMD, and that the DPRK continues to steal or extort virtual assets from victims and use increasingly sophisticated methods to launder illicit proceeds which often involve anonymity-enhancing coins, mixers, DeFi arrangements and cross-chain bridges before converting stablecoins into fiat currencies at over-the-counter brokers concentrated in certain jurisdictions[32].

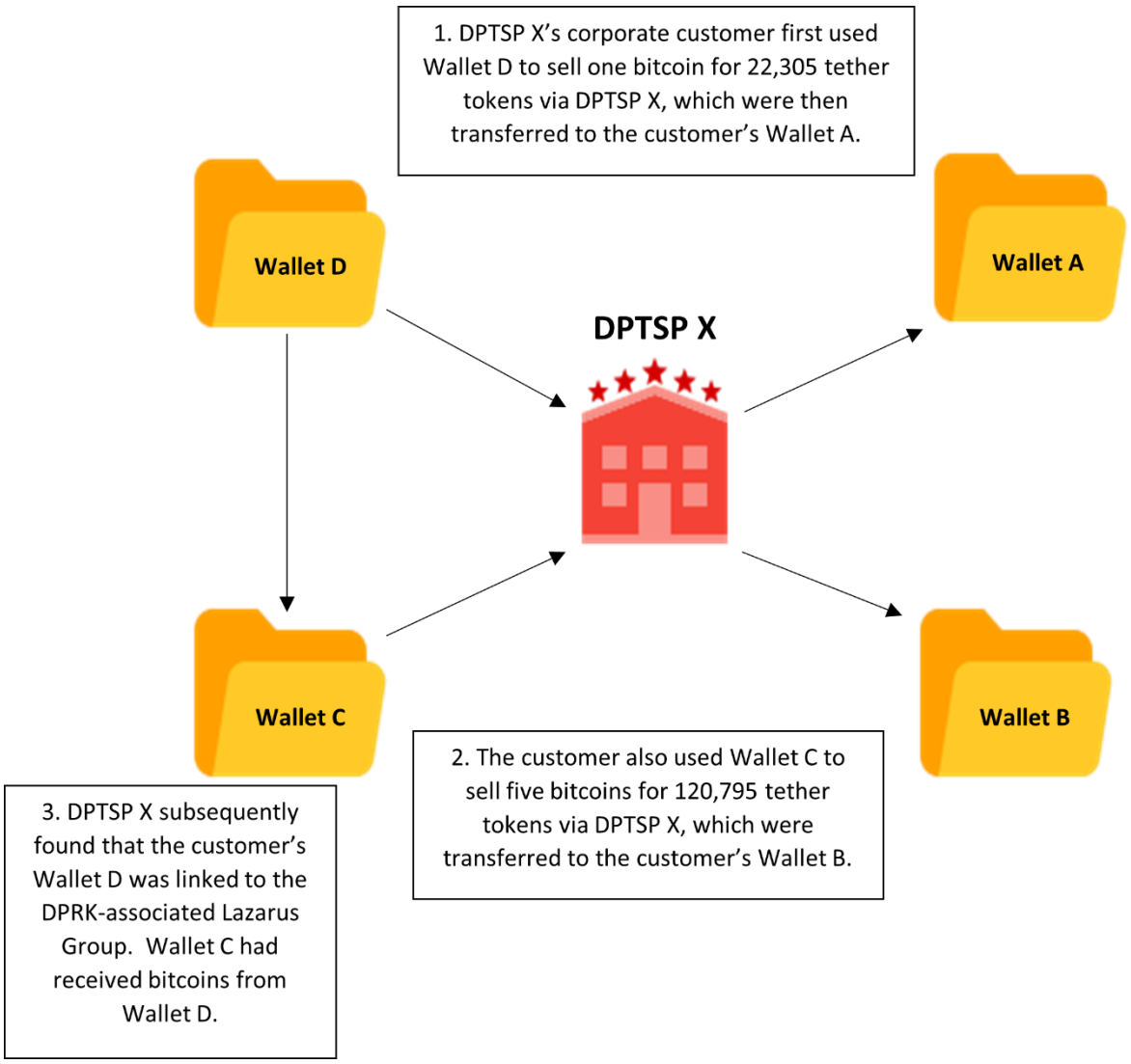
5.13 Since 2020, Singapore has taken steps to subject DPTSPs in Singapore to AML/CFT/CPF regulation and supervision – more details can be found in **Section 6: "Singapore's Key Sectoral**

[27] For more details on Singapore's risks in relation to virtual assets, please refer to Singapore's Virtual Assets Risk Assessment at https://www.mas.gov.sg/regulation/anti-money-laundering/ml-tf-pf-risk-assessments.
[28] UNSC Panel of Experts on the DPRK's report dated 7 March 2023, page 74
[29] Chainalysis' February 2024 "The 2024 Crypto Crime Report", pages 42 and 43
[30] FATF's June 2023 "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers", page 3
[31] FATF's June 2024 "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers", page 3
[32] FATF's June 2024 "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers", page 26. Please also refer to the 2021 FATF Guidance (page 28) which further describes how the DPRK has used virtual assets to support its WMD proliferation activities.

Vulnerabilities". The case study below illustrates how a DPTSP in Singapore was exposed to a customer with a sanctions nexus.

CASE STUDY 7 – Risk mitigation measures applied by DPTSP

A DPTSP in Singapore carried out two transactions where it received bitcoins from a customer's wallet that it converted to tether tokens and sent to another wallet belonging to the same customer. The DPTSP was alerted that one of the customer's wallets was linked to the DPRK-associated Lazarus Group. The DPTSP immediately suspended its customer's account (including freezing all funds within) and filed a suspicious transaction report.



(F) Measures to address key PF threats

5.14 To tackle these key PF threats, Singapore authorities have implemented, and will continue to implement, various measures to keep pace with the ever-changing sanctions evasion tactics:

- ***Misuse of legal persons:*** The misuse of legal persons is a priority risk area for Singapore. To guard against PF risks, ACRA conducts screening of companies and their key appointment holders during company incorporation and on an ongoing basis. To further safeguard against UNSC-designated individuals and entities seeking to legitimise or

facilitate their activities through the services of professional intermediaries such as banks, corporate service providers and lawyers, etc., Singapore has in place rules to require these intermediaries to conduct customer due diligence checks, including customer screening. Other measures applied by Singapore authorities include using data analytics to uncover likely networks of rogue entities and sharing the information on such networks among fellow agencies to facilitate a whole-of-Government response; making it a requirement in law for FIs and corporate service providers[33] in Singapore to consider applying enhanced due diligence measures to higher-risk legal persons (e.g. shell companies); providing guidance to industry on the AML/CFT controls that should be in place to effectively address the misuse of legal persons[34]; introducing an FI-to-FI information sharing platform to address the misuse of legal persons among other risks (please see paragraph 6.9 for details).

- ***Ship-to-ship transfers:*** Singapore authorities have been conducting outreach to raise industry's PF risk awareness – for instance, the Maritime Port and Authority of Singapore regularly issues circulars to the shipping industry on Singapore's obligations to comply with the relevant UNSCRs and updates to the UNSCRs.

- ***Movement of dual-use goods:*** Singapore implements a strategic goods control list which covers military goods and technology, and dual-use goods and technology that are designed for commercial applications but can have military applications or potentially be used as precursors or components of WMD. The list is reviewed on an annual basis to keep up with international best practices. Singapore also works closely with our international partners with regard to shipments of proliferation concern, and conducts inspections and audits to ensure compliance with Singapore's laws.

- ***Export of luxury goods:*** Since 8 November 2017, Singapore has prohibited the import into, export from, transhipment in and transit through Singapore of all commercially-traded goods from or to the DPRK. This goes beyond the scope of prohibitions set out in the DPRK-related UNSCRs and provides a strong foundation for Singapore authorities to manage the PF risks emanating from the export of luxury goods to the DPRK. Singapore also works closely with our international partners and targets shipments that may be destined for the DPRK to identify potential contraventions of our laws.

- ***Misuse of virtual assets:*** As mentioned in paragraph 5.13, Singapore has taken steps to subject DPTSPs in Singapore to AML/CFT/CPF regulation and supervision, as well as conducted outreach from as early as 2019 to raise industry's PF risk awareness. For more details, please refer to **Section 6: "Singapore's Key Sectoral Vulnerabilities"**, subsection (B) on DPTSPs.

[33] ACRA is amending the Accounting and Corporate Regulatory Authority (Filing Agents and Qualified Individuals) Regulations 2015 to effect this requirement by 1H 2025.

[34] E.g. MAS' August 2023 guidance paper, "Strengthening AML/CFT Controls and Practices to Detect and Mitigate Risks of Misuse of Legal Persons/Arrangements and Complex Structures"

6 SINGAPORE'S KEY SECTORAL VULNERABILITIES

6.1 Having identified the key PF threats to Singapore and the specific sectors exposed to such PF threats, Singapore carried out vulnerability assessments of these sectors (incorporating feedback from sector supervisors and industry) and assessed the sectors' PF risk levels as follows:

- **Banks** have been assessed to be exposed to higher PF risks in light of their wide range of services, international typologies and the cases that we have observed in Singapore;

- **For the other financial sectors**, DPTSPs are exposed to some PF risks given international typologies and their activities which entail dealing with virtual assets that are known to be misused by individuals and entities involved in the proliferation of WMD and PF. Remittance agents and maritime insurers are sectors to watch (i.e. these sectors and their supervisors need to remain vigilant);

- **Among the DNFBP (non-financial) sectors**, corporate service providers are exposed to some PF risks given international typologies and their role in the formation of companies, and some corporate service providers may be the directors of these companies. Precious stones and precious metals dealers and lawyers are sectors to watch (i.e. these sectors and their supervisors need to remain vigilant).

More details can be found below.

6.2 For the sectors that are not featured here, they have been assessed to be of lower PF risk in light of international typologies and their lower exposure to Singapore's key PF threats. **For avoidance of doubt, these lower-PF risk sectors would still have to comply with the relevant CPF-related obligations (including the relevant Regulations). As their PF risks are more general, such lower-PF risk sectors would not be expected to conduct individual PF risk assessments but should nonetheless pay heed to the PF risks highlighted in this PF NRA in the conduct of their business.**

FINANCIAL SECTORS

(A) Banks

(I) Exposure to key PF threats

6.3 While UNSC-designated individuals' and entities' access to the formal financial system has become increasingly cut off due to the introduction of various financial sanctions[35] and banks have become more alert to PF typologies and sanctions evasion tactics, the DPRK continues to find ways to access the international financial system and engage in illicit financial operations in violation of the DPRK-related UNSCRs[36]. It was also noted in paragraph 5.6 that Iran's procurement networks use deceptive tactics to access the international financial system.

6.4 In Singapore's context, banks are exposed to the key PF threats identified in **Section 5: "Singapore's Key Proliferation Financing Threats"** i.e. misuse of legal persons, ship-to-ship transfers, movement of dual-use goods, export of luxury goods and misuse of virtual assets. Banks have been observed to be among the key intermediaries in these activities, particularly

[35] 2021 FATF Guidance, page 28

[36] UNSC Panel of Experts on the DPRK's report dated 7 March 2024, page 53

in relation to the misuse of legal persons and in support of the movement of dual-use goods and/or export of luxury goods. Further, based on industry engagement[37], banks have identified PF typologies including the misuse of legal persons (e.g. use of shell companies, front companies, complex ownership/control structures and third party intermediaries; DPRK-linked financial facilitators running multiple companies with the same owners/managers, contact details and employees), ship-to-ship transfers (e.g. bank's customer providing shipping-related services to a vessel that conducted a ship-to-ship transfer for the DPRK) and movement of dual-use goods, as well as the use of false documentation and stripping of information.

(II) Key sectoral vulnerabilities

Status as international financial centre and key trading and transhipment hub

6.5 Singapore's status as an international financial centre and key trading and transhipment hub, as well as our geographical proximity to the DPRK make us vulnerable to being used for PF purposes as proliferators seek to embed PF-related transactions within the voluminous legitimate transactions that banks process on a daily basis. As such, while banks in Singapore generally have relatively higher PF risk awareness and understanding and more developed CPF controls as compared to the other financial sectors, they have to remain vigilant against evolving PF typologies.

Challenges faced in ascertaining the use of dual-use goods for illicit purposes

6.6 While MAS has provided guidance to alert banks to the risk of dual-use goods being used for illicit purposes and corresponding risk mitigation measures that could be put in place[38], it remains challenging for banks in Singapore and globally to identify dual-use goods and ascertain whether the goods would be used illicitly – banks' staff may not necessarily possess the relevant technical qualifications and knowledge across a wide range of goods to allow them to understand the varying applications of dual-use goods. Moreover, the descriptions of goods in trade documents may be worded such that they do not allow for the easy identification of dual-use goods. MAS will continue to work with industry to provide guidance and relevant information as necessary to support banks on this front.

(III) Key PF risk mitigation measures

6.7 As stated in **Section 4: "Singapore's Counter-Proliferation Financing Framework"**, FIs (including banks) in Singapore have to comply with the FSM DPRK Regulations and FSM Iran Regulations. MAS monitors banks' compliance with these Regulations as part of its regular AML/CFT[39] supervisory efforts (e.g. AML/CFT onsite inspections and offsite engagements, surveillance), and has taken action against banks that breached the Regulations. In addition, regular engagements of banks on CPF have been carried out to strengthen their risk understanding – aside from industry outreach (e.g. via the annual Association of Banks in Singapore (ABS) Financial Crime Seminar and townhall sessions for banks), MAS conducted thematic supervisory visits to a number of banks from December 2017 to May 2018, which focussed on (among others) understanding how banks ensured the effectiveness of their CPF frameworks and

[37] A survey of a number of banks was conducted by the ACIP CPF WG to understand their level of PF risk awareness and the robustness of their CPF controls.

[38] E.g. MAS' October 2015 "Guidance on Anti-Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking"

[39] Banks in Singapore are subject to AML/CFT regulation by MAS and are required to comply with the AML/CFT requirements in MAS Notice 626, "Prevention of Money Laundering and Countering the Financing of Terrorism – Banks".

controls and identified higher-risk customers and transactions. The discussions during the visits also centred around common PF typologies, and the need for banks to be vigilant and ensure robust controls were in place to detect sanctions evasion. MAS subsequently[40] shared the key findings from the supervisory visits and sound practices observed with banks and other FIs to use as benchmarks when reviewing and enhancing their existing controls. Additionally, MAS carried out thematic inspections of selected FIs (including banks) in 2021 which focussed on their name screening frameworks and processes – name screening is a fundamental control in the countering of ML/TF/PF risks. Another guidance paper was issued setting out MAS' supervisory expectations and good practices noted.[41]

6.8 ACIP, a key public-private partnership platform which comprises nine key Singapore banks and ABS, has been tapped on to raise ACIP banks' awareness of emerging PF risks and sanctions evasion typologies (including risks associated with unilateral sanctions). In addition, the topic of sanctions is regularly on the agenda of the annual ABS Financial Crime Seminar (which is one of Singapore's largest industry outreach events) with attendees from banks (and other sectors) and with local and foreign experts speaking about trends and best practices.

6.9 To enhance the detection and mitigation of ML/TF/PF risks, MAS has been using data analytics to strengthen its capabilities on this front and has been encouraging FIs to make use of data analytics to bolster their controls – major banks now deploy data analytics to, for instance, facilitate investigations involving sanctioned names and flag mismatches between a customer's stated country of domiciliation and digital footprints which could be linked to sanctioned jurisdictions. In addition, to address PF risks (among other risks), on 1 April 2024, MAS launched a digital platform, COSMIC (which stands for "Collaborative Sharing of ML/TF Information and Cases")[42] together with six key banks in Singapore. COSMIC allows banks to overcome information asymmetry by securely sharing with one another (if stipulated thresholds are met) information on customers that exhibit multiple red flags which may indicate financial crime concerns. Such sharing addresses the situation where banks were previously unable to quickly alert one another to suspicious customers to prevent criminals from carrying out illicit transactions through a web of individuals and entities that had accounts with different banks. MAS and STRO can use the information from COSMIC in their risk surveillance and analysis work respectively to detect illicit networks within Singapore's financial system for more timely supervisory intervention and to support law enforcement efforts.

6.10 Generally, banks are aware of their CPF obligations and the key PF risk areas, and have in place sanctions and AML/CFT policies, procedures and controls, including screening measures. From the survey of the key banks involved in corporate banking, which was conducted by the ACIP CPF WG[43] to understand the banks' level of PF risk awareness and the robustness of their CPF controls, some banks indicated that they have a group CPF framework to ensure their compliance with the FSM DPRK Regulations and FSM Iran Regulations, and to manage their PF risks.

6.11 **Taking into account this sector's threats (including international typologies), vulnerabilities and risk mitigation measures, banks in Singapore have been assessed to be exposed to higher PF risks as compared to the other financial sectors and DNFBP sectors in Singapore.**

[40] MAS' August 2018 guidance paper, "Sound Practices to Counter Proliferation Financing"

[41] MAS' April 2022 guidance paper, "Strengthening AML/CFT Name Screening Practices"

[42] More information on COSMIC can be found at: https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic.

[43] The ACIP CPF WG also carried out similar surveys of DPTSPs, remittance agents, maritime insurers, corporate service providers and lawyers.

(B) DPTSPs

(I) Exposure to key PF threats

6.12 The UNSC Panel of Experts on the DPRK noted in 2020 that the DPRK had exploited loosely-regulated networks of virtual asset service providers (VASPs) and over-the-counter brokering services[44] in order to convert illicitly-obtained virtual assets into fiat currencies. The Panel also noted that these transactions highlighted several vulnerabilities within the global financial system to sanctions evasion, including VASPs with little or no know-your-customer protocols, the lack of regulation in some jurisdictions of over-the-counter brokering services, and the lack of transparency in cryptocurrency to fiat currency conversions within FIs.[45] As of 2023, DPRK cyberthreat actors continued to target VASPs and the virtual asset industry more broadly for the purpose of evading UNSC sanctions.[46] The 2021 FATF Guidance mentioned that VASPs provide products which have been mined and stolen by UNSC-designated individuals and entities, as well as a platform for moving monies across international borders instantly.[47]

6.13 In Singapore's context, DPTSPs are primarily exposed to the key PF threat of misuse of virtual assets (or digital payment tokens) as identified in **Section 5: "Singapore's Key Proliferation Financing Threats"**. As noted in that section (please see Case Study 7) and from MAS' regular surveillance of the DPTSP sector in Singapore (detailed in paragraph 6.19), some DPTSPs have detected transactions with a sanctions nexus. Also, based on industry engagement[48], DPTSPs have identified PF typologies including the use of shell companies, nominees and false documentation. DPTSPs should thus continue to be vigilant against PF and regularly review and enhance their CPF controls.

(II) Key sectoral vulnerabilities

Anonymity associated with virtual assets

6.14 Virtual assets could be misused for nefarious purposes because of the pseudonymity (or in some cases, anonymity) they offer, convenience they provide as an instantaneous value transfer medium, and cross-border nature of virtual asset transactions.[49] The UNSC Panel of Experts on the DPRK has noted that DPRK cyberactors had engaged in trading multiple forms of virtual assets (including alternative coins), with the DPRK specifically targeting anonymity-enhanced cryptocurrencies in order to provide additional layers of security and to frustrate traceability. [50]

[44] Over-the-counter brokers help to provide liquidity in cryptocurrency markets by matching buyers and sellers.
[45] UNSC Panel of Experts on the DPRK's report dated 28 August 2020, page 44
[46] UNSC Panel of Experts on the DPRK's report dated 12 September 2023, page 56
[47] 2021 FATF Guidance, page 24
[48] A survey of a number of DPTSPs was conducted by the ACIP CPF WG to understand their level of PF risk awareness and the robustness of their CPF controls.
[49] MAS' Guidelines to MAS Notice PSN02, "Prevention of Money Laundering and Countering the Financing of Terrorism - Holders of Payment Services Licence (Digital Payment Token Service)", page 57
[50] UNSC Panel of Experts on the DPRK's report dated 28 August 2020, page 43

Uneven implementation of AML/CFT requirements internationally

6.15 In 2019, the FATF Standards were extended to virtual assets and VASPs. However, while the situation is improving[51], as of June 2024[52], there continues to be a lack of implementation of the relevant FATF Standards globally, which means that virtual assets and VASPs remain vulnerable to misuse and the overall implementation of AML/CFT rules globally remains behind that of other financial sectors. It is thus vital that all jurisdictions act rapidly to fully implement the FATF Standards to make it more difficult for bad actors (including proliferators) to exploit VASPs, and to level the playing field for law-abiding VASPs that have been diligently complying with the applicable AML/CFT/CPF requirements.

(III) Key PF risk mitigation measures

6.16 As stated in **Section 4: "Singapore's Counter-Proliferation Financing Framework"**, FIs (including DPTSPs) in Singapore have to comply with the FSM DPRK Regulations and FSM Iran Regulations. MAS monitors DPTSPs' compliance with these Regulations as part of its regular AML/CFT[53] supervisory efforts (e.g. AML/CFT onsite inspections and offsite engagements, surveillance). Singapore was in fact one of the first in the world to regulate DPTSPs for AML/CFT/CPF.[54] To manage the risks from DPTSPs' activities, MAS has put in place stringent licensing requirements and a robust due diligence process to ensure that only licence applicants (including their AML/CFT/CPF controls) that meet MAS' licensing standards are granted a licence. Legal opinion and external auditor assessment requirements have also been imposed to further strengthen the assessment rigour during the licensing process.

6.17 MAS recognised that the ML/TF/PF risk awareness and understanding of AML/CFT/CPF requirements within this sector might not be strong given that it is a nascent space and industry players might be less familiar with the requirements. As such, even before the domestic legislation came into effect and before MAS started licensing DPTSPs, MAS issued guidance[55] and engaged the industry to explain the applicable requirements and MAS' supervisory expectations. Additionally, DPTSPs were invited to participate in the annual ABS Financial Crime Seminar (one of Singapore's largest industry outreach events) with local and foreign experts speaking about trends and best practices – this is part of ongoing efforts to increase PF risk awareness in the DPTSP sector and allow DPTSPs to learn from the best practice controls implemented in mature sectors such as the banking sector.

6.18 In 2022, MAS carried out thematic inspections of newly-licensed DPTSPs to assess the effectiveness of their AML/CFT frameworks and to have an early sensing of common areas of weakness within the sector which would need further clarification and guidance. The thematic inspections focussed on key control areas including sanctions compliance to understand

[51] In the outcomes for the FATF Plenary held from 26 to 28 June 2024, the FATF noted that "in real terms, the number of jurisdictions that are compliant or largely compliant with the FATF Standards in this [virtual assets/VASP] area has increased (33 in 2024; 25 in 2023). However, three quarters of jurisdictions (75%; 97 of 130) are only partially or not compliant with the FATF Standards in this area".

[52] FATF's June 2024 "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers", pages 2 and 4

[53] DPTSPs in Singapore are subject to AML/CFT regulation by MAS and are required to comply with the AML/CFT requirements in MAS Notice PSN02, "Prevention of Money Laundering and Countering the Financing of Terrorism - Holders of Payment Services Licence (Digital Payment Token Service)".

[54] https://www.mas.gov.sg/news/media-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks

[55] MAS' March 2021 guidance paper, "Strengthening AML/CFT Controls of Digital Payment Token Service Providers"

whether DPTSPs are familiar with their sanctions obligations given that there are international typologies involving the misuse of virtual assets to evade sanctions. Thus far, MAS has found that DPTSPs are generally familiar with their sanctions obligations, and have adopted screening tools to screen customers (and related parties such as directors and natural persons authorised to act on behalf of the customer) against relevant sanctions lists at onboarding and on an ongoing basis. DPTSPs also use blockchain analytics tools to detect any exposure to wallet addresses with a sanctions nexus at onboarding and on an ongoing basis.

6.19 These findings from the thematic inspections are in line with the: (a) findings from the industry survey where the majority of DPTSPs indicated that they either have in place standalone CPF policies, procedures and controls or rely on their sanctions and AML/CFT policies, procedures and controls to ensure their compliance with the FSM DPRK Regulations and FSM Iran Regulations, and to manage their PF risks; and (b) observations made in the course of MAS' regular surveillance of Singapore's DPTSP sector – while there are potential sanctions risks, they are small at this point in time and in most cases, DPTSPs were able to detect and take appropriate risk mitigation measures in response to transactions with a sanctions nexus (e.g. customers' transactions with unilaterally-sanctioned entities), including exiting the customer relationship, suspending the customer's account (so that no further transactions could be carried out) and filing a suspicious transaction report. MAS will be publishing a guidance paper containing the key observations from the thematic inspections so that DPTSPs will be able to assess their controls and strengthen them where necessary.

6.20 **Taking into account this sector's threats (including international typologies), vulnerabilities (including the global state of play) and risk mitigation measures, DPTSPs in Singapore have been assessed to pose some PF risks.**

(C) Remittance agents (Cross-border money transfer service[56] providers)

(I) Exposure to key PF threats

6.21 As banks become increasingly aware of PF risks and sanctions evasion methods, the banking channel has become more challenging for proliferators to access. Proliferators could therefore turn to remittance agents to gain access to the international financial system. Based on industry engagement[57], remittance agents have identified possible PF typologies including the use of false documentation.

(II) Key sectoral vulnerabilities

Nature of services provided

6.22 Remittance agents tend to offer cross-border remittance services which are more cost-effective and efficient as compared to those offered by banks. In Singapore's context, remittance agents' customers are typically Singapore's foreign migrant worker population from neighbouring countries. This reduces the likelihood of remittance agents being used for PF purposes as their remittances would unlikely be related to the DPRK.

[56] "Cross-border money transfer service" is defined as any service of accepting money in Singapore, whether as principal or agent, for the purpose of transmitting, or arranging for the transmission of, the money to any person outside Singapore. It also includes any service of receiving any money from outside Singapore for, or arranging for the receipt of any money from outside Singapore by, any person in Singapore, whether as principal or as agent.

[57] A survey of a number of remittance agents was conducted by the ACIP CPF WG to understand their level of PF risk awareness and the robustness of their CPF controls.

(III) Key PF risk mitigation measures

6.23 As stated in **Section 4: "Singapore's Counter-Proliferation Financing Framework"**, FIs (including remittance agents) in Singapore have to comply with the FSM DPRK Regulations and FSM Iran Regulations. MAS monitors remittance agents' compliance with these Regulations as part of its regular AML/CFT[58] supervisory efforts (e.g. AML/CFT onsite inspections and offsite engagements, surveillance). Based on supervisory and industry engagement, remittance agents in Singapore appear to have a reasonable level of PF risk awareness with the large established remittance agents being well-aware of their PF (and TF) sanctions risks and generally putting in place controls, including screening. Also, remittance agents surveyed by the ACIP CPF WG either have in place standalone CPF policies, procedures and controls or rely on their sanctions and AML/CFT policies, procedures and controls to manage their PF risks. The more sophisticated remittance agents have built up data analytics capabilities and have been able to detect and block potential sanctions evasion. MAS will continue to engage remittance agents to strengthen their PF risk awareness and implementation of controls.

6.24 **Taking into account this sector's threats (including international typologies), vulnerabilities and risk mitigation measures, remittance agents in Singapore have been assessed to be a sector to watch (i.e. the sector and sector supervisor have to remain vigilant).**

(D) Maritime insurers

(I) Exposure to key PF threats

6.25 The UNSC Panel of Experts on the DPRK has observed suspect vessels transmitting falsified or inconsistent identifiers on their automatic identification systems (AIS) and reporting false destinations.[59] Suspect vessels trading in restricted or banned commodities and exhibiting AIS transmission gaps continue to sail in and around waters where illicit ship-to-ship transfer activities typically occur – few (if any) non-DPRK vessels appear to transmit AIS signals in the DPRK's waters based on commercial maritime database platforms with suspect vessels dropping their AIS signals while sailing towards the DPRK and retransmitting once back in non-DPRK waters. To obscure the connection with the DPRK, complicit actors also falsify shipping documentation to conceal the cargo's origin or destination. Such indicators could provide grounds for investigation by the relevant public and private sector parties including the parties that flag, charter, operate, insure, class or finance the vessels.

6.26 In Singapore's context, maritime insurers, which could provide insurance and reinsurance services, are primarily exposed to the key PF threat of ship-to-ship transfers as identified in **Section 5: "Singapore's Key Proliferation Financing Threats"**. While this threat is more pertinent to the shipping industry which the relevant Singapore authorities continue to engage, maritime insurers in Singapore may find themselves providing insurance to vessels involved in illicit ship-to-ship transfer activities. Based on industry engagement[60], maritime insurers have identified possible PF typologies including the use of complex ownership structures, insured vessels' AIS transponders being turned off or manipulated, and use of false documentation.

[58] Remittance agents in Singapore are subject to AML/CFT regulation by MAS and are required to comply with the AML/CFT requirements in MAS Notice PSN01, "Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Specified Payment Services)".

[59] UNSC Panel of Experts on the DPRK's report dated 7 March 2024, page 23

[60] A survey of a number of maritime insurers was conducted by the ACIP CPF WG to understand their level of PF risk awareness and the robustness of their CPF controls.

(II) Key sectoral vulnerabilities

Nature of services provided

6.27 As recently as March 2024, the UNSC Panel of Experts on the DPRK was still noting in its report various tactics used within the maritime sector to evade sanctions. As such, the risk of being exploited by proliferators continues to be relevant for maritime insurers which support the shipping industry.

(III) Key PF risk mitigation measures

6.28 As stated in **Section 4: "Singapore's Counter-Proliferation Financing Framework"**, FIs (including maritime insurers) in Singapore have to comply with the FSM DPRK Regulations and FSM Iran Regulations. MAS monitors maritime insurers' compliance with these Regulations as part of its regular supervisory engagements, industry outreach and surveillance. In addition, in May 2019, MAS issued AML/CFT Guidelines[61] to insurers (including maritime insurers) to raise industry awareness of their ML/TF/PF risks and appropriate risk mitigation measures. In particular, the Guidelines reiterated the need to comply with the FSM Regulations and that insurers should put in place screening checks as part of their suite of risk mitigation measures. Based on industry engagement, maritime insurers appear to have a reasonable level of PF risk awareness with all maritime insurers surveyed having sanctions and relevant AML/CFT policies, procedures and controls in place to address PF risks. We note that in most cases, maritime insurers' contracts would have carve out clauses to void any insurance coverage should there be sanctions concerns. MAS will continue to engage maritime insurers to strengthen their PF risk awareness and implementation of controls.

6.29 **Taking into account this sector's threats (including international typologies), vulnerabilities and risk mitigation measures, maritime insurers in Singapore have been assessed to be a sector to watch (i.e. the sector and sector supervisor have to remain vigilant).**

DNFBP SECTORS

(E) Corporate service providers (CSPs)

(I) Exposure to key PF threats

6.30 As noted by the UNSC Panel of Experts on the DPRK[62], CSPs present a key vulnerability in the implementation of financial sanctions, allowing the DPRK to easily create front companies offshore and in some Asian financial centres, where the DPRK leverages the assistance of non-DPRK nationals and uses the companies to open and maintain bank accounts to move monies worldwide. The Panel also noted the DPRK's reliance on CSPs to facilitate (both wittingly and unwittingly) its sanctions evasion activities.[63] Further, the FATF in its 2021 FATF Guidance noted that "company service providers, lawyers and accountants involved in the creation or management of companies and other legal persons or legal arrangements, in particular, face transaction and service risks."[64]

[61] MAS' May 2019 "Guidelines on Prevention of Money Laundering and Countering the Financing of Terrorism - Direct General Insurance Business, Reinsurance Business, and Direct Life Insurance Business (Accident & Health Policies)"

[62] E.g. in the UNSC Panel of Experts on the DPRK's report dated 5 March 2018, pages 4 and 5

[63] UNSC Panel of Experts on the DPRK's report dated 4 March 2021, pages 52 and 57

[64] 2021 FATF Guidance, page 41

6.31 In Singapore's context, our law enforcement has not observed CSPs to be involved in the setting up of companies to facilitate PF specifically. In addition, CSPs are required to put in place robust AML/CFT controls which guard against PF risks, including customer screening – CSPs in Singapore are subject to AML/CFT regulation by ACRA and are required to comply with the AML/CFT requirements in the Accounting and Corporate Regulatory Authority (Filing Agents and Qualified Individuals) Regulations 2015. Nonetheless, given that CSPs are involved in the upstream incorporation of companies, they are exposed to the PF threat of misuse of legal persons as identified in **Section 5: "Singapore's Key Proliferation Financing Threats"**. Based on industry engagement[65], CSPs have identified possible PF typologies including the use of nominees and false documentation.

(II) Key sectoral vulnerabilities

Involvement of professional intermediaries to provide respectability and legitimacy to potential PF activities

6.32 CSPs are business entities and individuals that provide services such as corporate advisory, office hosting and corporate secretarial services, and filing of statutory returns. In practice, CSPs primarily facilitate the company formation process but do not normally manage or control the companies they help incorporate – CSPs' involvement is typically limited to the incorporation stage and the fulfilment of ongoing regulatory obligations.

6.33 UNSC-designated individuals and entities may attempt to involve professionals such as CSPs in the set up of companies to conduct proliferation and PF activities to provide respectability and legitimacy to such activities.

(III) Key PF risk mitigation measures

6.34 As stated in **Section 4: "Singapore's Counter-Proliferation Financing Framework"**, DNFBPs (including CSPs) in Singapore have to comply with the UN DPRK Regulations and UN Iran Regulations. CSPs in Singapore are regulated by ACRA for AML/CFT purposes and are thus required to carry out customer due diligence checks such as the identification and verification of the identities of their customers and customers' beneficial owners.[66] As such, ACRA monitors CSPs' compliance with the UN DPRK Regulations and UN Iran Regulations as part of its regular AML/CFT supervisory efforts (e.g. AML/CFT onsite inspections and offsite engagements), and has not noted major deficiencies. Based on industry engagement, to ensure their compliance with these Regulations and to manage their PF risks, CSPs have put in place sanctions and AML/CFT policies, procedures and controls (including screening).

6.35 Should UNSC-designated individuals and entities attempt to involve professional intermediaries such as CSPs to legitimise their activities, CSPs' regulatory obligations to conduct customer due diligence such as periodic screening against UNSC sanctions lists would be the first line of defence against such tactics. In addition, CSPs are required to flag out corporate entities that may have no real economic purpose or that may have been incorporated for the purpose of circumventing sanctions, and file suspicious transaction reports as necessary. While proliferators could also use CSPs to gain access to the international financial and trading system by getting the CSPs' assistance to open corporate bank accounts following the incorporation of

[65] A survey of a number of CSPs was conducted by the ACIP CPF WG to understand their level of PF risk awareness and the robustness of their CPF controls.

[66] Foreigners must engage the services of a CSP to incorporate a company in Singapore which provides a layer of screening since CSPs are obligated to conduct customer due diligence checks.

a company, banks are separately required to carry out rigorous customer due diligence checks including payment screening, and this multi-gatekeepers approach helps to mitigate risks.

6.36 Further, to guard against the misuse of companies for PF purposes, ACRA conducts pre-incorporation and periodic screening of companies against UNSC sanctions lists. ACRA also carries out industry outreach to raise CSPs' risk awareness. For corporate transparency and to reduce the risk of bad actors (including proliferators) misusing the corporate form, ACRA has required companies and limited liability partnerships (LLPs) in Singapore to collect and maintain adequate, accurate and up-to-date information on their beneficial owners since 2017, and to file such information with ACRA's central, non-public beneficial ownership register since 2020. This register can be accessed by any domestic public agency for the purpose of administering or enforcing any written law in Singapore.

6.37 Recognising the critical role of CSPs as gatekeepers, ACRA recently made legislative changes in July 2024 to further uplift the standard of the CSP sector and enhance corporate transparency. These changes include requiring business entities that carry on a business of providing corporate services from Singapore to register as CSPs and be subject to AML/CFT regulation by ACRA; making explicit that CSPs have to comply with CPF obligations (e.g. the requirement to conduct PF risk assessments); and requiring Singapore-incorporated companies and foreign-incorporated companies registered with ACRA to file the information in their register of nominee directors and register of nominee shareholders (including the identities of the nominators) with ACRA which will maintain such information[67].

6.38 **Taking into account this sector's threats (including international typologies), vulnerabilities and risk mitigation measures, CSPs in Singapore have been assessed to pose some PF risks.**

(F) Precious stones and precious metals dealers (PSMDs)

(I) Exposure to key PF threats

6.39 The UNSC Panel of Experts on the DPRK noted in 2023[68] that the partial border opening by the DPRK following the COVID-19 pandemic might increase the number of DPRK nationals couriering high-value items – some DPRK nationals travelling overseas have been known to carry high-value items in their luggage including cash, gold and wildlife products to evade UNSC sanctions. The 2021 FATF Guidance also noted that PSMDs provide an alternative method for UNSC-designated individuals and entities to surreptitiously move financial resources across international borders[69] with UNSC-designated individuals and entities engaging such dealers to transport gold and diamonds to obtain foreign exchanges to finance their transactions[70].

[67] Upon disclosure to ACRA, only the nominee status of the director and nominee status of the shareholder will be publicly available. Domestic public agencies can access the information maintained by ACRA (e.g. identities of the nominators) for the administration or enforcement of any written law in Singapore.
[68] UNSC Panel of Experts on the DPRK's report dated 12 September 2023, page 55
[69] 2021 FATF Guidance, page 24
[70] 2021 FATF Guidance, page 25

(II) Key sectoral vulnerabilities

Varied levels of PF risk awareness

6.40 As this sector is one of the more recently AML/CFT-regulated sectors in Singapore (with the AML/CFT regime[71] taking effect in 2019), the level of PF risk awareness is varied but has improved over time. For instance, while the PSMDs that took part in the 2022 focus group discussions with MinLaw[72] did not have much PF risk awareness, PSMDs surveyed in 2024 (following MinLaw's industry engagements) showed an improvement in their level of PF risk awareness.

(III) Key PF risk mitigation measures

6.41 As stated in **Section 4: "Singapore's Counter-Proliferation Financing Framework"**, DNFBPs (including PSMDs) in Singapore have to comply with the UN DPRK Regulations and UN Iran Regulations. MinLaw monitors PSMDs' compliance with these Regulations as part of its regular AML/CFT supervisory efforts (e.g. AML/CFT onsite inspections and offsite engagements). MinLaw also recently introduced legislative changes in February 2024 to make explicit that PSMDs have to comply with CPF obligations, including the implementation of adequate CPF programmes and measures. MinLaw continues to increase PSMDs' understanding of their CPF obligations, and PF risks and typologies through means such as preparing training videos for PSMDs to view online and updating guidelines and other compliance materials which provide guidance on PF red flag indicators and CPF obligations.

6.42 Aside from the existing AML/CFT regime for PSMDs, it is noted that the specific risk of DPRK nationals moving high-value items across Singapore's borders is mitigated by: (a) strict visa/entry requirements for DPRK nationals; and (b) tough laws that have prohibited trade and related financial transactions with the DPRK. Specifically, since 8 November 2017, Singapore has prohibited the import into, export from, transhipment in and transit through Singapore of all commercially-traded goods from or to the DPRK which goes beyond the DPRK-related UNSCRs. Also, regulation 12A of the UN DPRK Regulations and regulation 10 of the FSM DPRK Regulations prohibit any person (including any FI) in Singapore from providing financial services or transferring financial assets or resources for the purposes of trade with the DPRK, including any person in or national of the DPRK.

6.43 **Taking into account this sector's threats (including international typologies), vulnerabilities and risk mitigation measures, PSMDs in Singapore have been assessed to be a sector to watch (i.e. the sector and sector supervisor have to remain vigilant).**

(G) Lawyers

(I) Exposure to key PF threats

6.44 The 2021 FATF Guidance noted that lawyers could be involved in the creation or management of companies and other legal persons or legal arrangements[73], which is a deliberate strategy deployed by proliferators to obscure the fact that funds and other assets are being ultimately

[71] PSMDs in Singapore are subject to AML/CFT regulation by MinLaw and are required to comply with the AML/CFT requirements in the Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Act.

[72] MinLaw (the sector supervisor of PSMDs in Singapore) held focus group discussions with PSMDs in 2022 to understand their level of PF risk awareness and the robustness of their CPF controls.

[73] 2021 FATF Guidance, page 41

made available to UNSC-designated individuals and entities[74]. In Singapore's context, lawyers that are involved in the creation of companies would be regulated as CSPs by ACRA for AML/CFT purposes. Hence, lawyers in Singapore are mainly exposed to a residual risk i.e. the PF threat of dealing with foreign-created legal persons (please see **Section 5: "Singapore's Key Proliferation Financing Threats"** for more details). Based on supervisory and industry engagement[75], Singapore has not observed in this sector instances of misuse in relation to PF, although lawyers surveyed have identified the possible PF typologies of use of shell companies and complex ownership and control structures.

(II) Key sectoral vulnerabilities

Nature of services provided

6.45 Lawyers may provide advisory services in connection with the structuring of complex ownership and control structures, with such services possibly being exploited by proliferators.

(III) Key PF risk mitigation measures

6.46 As stated in **Section 4: "Singapore's Counter-Proliferation Financing Framework"**, DNFBPs (including lawyers and law practice entities) in Singapore have to comply with the UN DPRK Regulations and UN Iran Regulations. MinLaw and the Law Society of Singapore work together to raise the industry's PF risk awareness, and monitor lawyers' and law practice entities' compliance with these Regulations as part of their regular AML/CFT[76] supervisory efforts (e.g. AML/CFT onsite inspections). MinLaw also recently introduced legislative changes in February 2024 to make explicit that lawyers and law practice entities have to comply with CPF obligations. Additionally, the Law Society of Singapore has issued a Practice Direction that provides guidance to lawyers on the discharge of their AML/CFT/CPF obligations. This Practice Direction is regularly updated and includes PF red flag indicators. These measures have helped to raise PF risk awareness within this sector – based on industry engagement, lawyers and law practice entities appear to have a reasonable level of PF risk awareness with most surveyed having sanctions and AML/CFT policies, procedures and controls in place to address PF risks.

6.47 **Taking into account this sector's threats (including international typologies), vulnerabilities and risk mitigation measures, lawyers and law practice entities in Singapore have been assessed to be a sector to watch (i.e. the sector and sector supervisors have to remain vigilant).**

(H) Conclusion of sectoral PF risk assessments

6.48 For the FIs and DNFBPs featured in this section, they should remain vigilant to emerging and evolving PF typologies and sanctions evasion tactics, and regularly review their policies, procedures and controls and enhance them when and where necessary. The relevant sector supervisors will continue conducting industry outreach and their supervisory engagements to deepen industry's PF risk understanding and monitor for compliance with the relevant Regulations.

[74] 2021 FATF Guidance, page 14

[75] A survey of a number of lawyers was conducted by the ACIP CPF WG to understand their level of PF risk awareness and the robustness of their CPF controls.

[76] Lawyers and law practice entities in Singapore are subject to AML/CFT supervision by MinLaw and the Law Society of Singapore and are required to comply with the AML/CFT requirements in the Legal Profession Act.

6.49 As for the FIs and DNFBPs **not** covered in this section and their sector supervisors, they should keep abreast of the ever-evolving PF typologies and sanctions circumvention methods used by proliferators which may impact them, and keep up-to-date with the relevant laws and information that may be provided by Singapore authorities.

7 SINGAPORE'S COUNTER-PROLIFERATION FINANCING STRATEGY

7.1 To support Singapore's overall efforts in the countering of PF, Singapore has established a CPF strategy:

- Maintaining strong cooperation at the national and international levels;
- Remaining alert to the ever-evolving PF risk environment;
- Keeping our regulatory instruments up-to-date and compliant with the relevant UNSCRs;
- Engaging industry to raise and strengthen industry PF risk awareness and understanding;
- Monitoring for compliance and taking proportionate and effective enforcement action.

Maintaining strong cooperation at the national and international levels

7.2 Given that proliferators would be quick to exploit weaknesses within a jurisdiction's counter-proliferation and CPF regime and jurisdictions with weak regimes, Singapore will continue our strong interagency cooperation and coordination through the IMC-EC working together with the AML/CFT Steering Committee, with the RTIG as the main operational body responsible for identifying and monitoring PF risks. We will also continue to collaborate with our international partners at the FATF and bilaterally via the sharing and exchange of best practices, information and intelligence, as well as engaging in joint counter-proliferation operations to keep abreast of emerging PF typologies and facilitate the development of cases to weed out identified proliferators.

Remaining alert to the ever-evolving PF risk environment

7.3 To detect emerging PF risks, Singapore will continue to proactively carry out our surveillance efforts, for instance, via MAS' dedicated risk surveillance team[77] and the ACIP Risk Surveillance WG (whose mandate is to monitor for emerging risks and alert fellow ACIP banks as necessary)[78]. Singapore will also continue to leverage the interagency RTIG platform to share and exchange information on emerging risks that should be watched closely.

Keeping our regulatory instruments up-to-date and compliant with the relevant UNSCRs

7.4 As a responsible UN Member State, Singapore is committed to implementing all relevant UNSCRs. Singapore will continue to monitor for updates to the UNSC sanctions regimes, and incorporate any updates in the relevant Regulations. The sector supervisors will also continue to alert FIs and DNFBPs as and when there are changes to the Regulations so that FIs and DNFBPs can review and adapt their CPF policies, procedures and controls as necessary.

Engaging industry to raise and strengthen industry PF risk awareness and understanding

7.5 As a well-informed, alert and vigilant ecosystem of players is key to an effective CPF regime, Singapore will continue to use industry platforms such as ACIP to further deepen industry's PF risk understanding through the sharing of typologies and issuance of industry-driven best practice papers. Sector supervisors will also continue to work with relevant industry bodies and their industry outreach efforts and supervisory engagements to ensure that PF risks remain on the radar of FIs and DNFBPs.

[77] MAS has an AML Risk Surveillance Division, which (among others) identifies and monitors ML/TF/PF risks by applying data analytics and risk surveillance tools to a spectrum of data points and intelligence.
[78] Please see paragraph 2.5 of this report for more information on ACIP.

Monitoring for compliance and taking proportionate and effective enforcement action

7.6 The sector supervisors will continue to monitor FIs' and DNFBPs' compliance with the relevant Regulations, and law enforcement agencies (CAD and Customs) will continue to investigate potential breaches of the relevant domestic legislation. Should breaches of our laws be uncovered, Singapore authorities will not hesitate to take swift, proportionate and effective action against non-compliant individuals and entities.

8 CONCLUSION

8.1 PF risks related to key jurisdictions of concern remain a clear and present danger to international peace and stability. FIs and DNFBPs in Singapore, particularly banks and other sectors noted in this PF NRA, are important gatekeepers in the fight against WMD proliferation and PF. They must continue their vigilance against known and emerging sanctions circumvention methods as proliferators change and adapt their modi operandi to evade UNSC sanctions and unilateral sanctions imposed by individual jurisdictions. Sector supervisors will continue to keep tabs on the risks faced by their sectors, strengthen industry risk understanding and monitor the sectors' compliance with the relevant Regulations.

8.2 Given the increasingly volatile external environment, Singapore authorities will regularly review the CPF strategy and PF NRA, and will continue to collaborate with one another, the private sector and international partners to ensure that our defences against WMD proliferation and PF remain sound, robust and effective.