اللجنة الوطنية لمكافحة
غسل الأموال وتمويل الإرهاب
NATIONAL COMMITTEE
FOR AML & CFT

Typologies of Proliferation Financing

State of Kuwait

August 2025

PF context for Kuwait

1. Kuwait has not had any PF related cases or TFS sanction evasion cases in the past but contextual factors suggest that some PF risks related to the DPRK exist and thus that Kuwait does have some risk exposure in this regard.

2. Kuwait's ties with the DPRK are very limited but exist. The DPRK maintains an embassy in Kuwait City. Kuwait has no embassy in Pyongyang. In the past, Kuwait hosted a significant number of North Korean laborers, primarily in the construction sector, with remittances from these workers contributing to DPRK's finances. In 2019, the UN imposed a ban on overseas North Korean workers under UN Security Council Resolution 2397 (2017), which Kuwait complied with by repatriating all North Korean laborers. This step closed a critical channel of funds for DPRK.

3. Some very limited commercial trade continues to taken place between Kuwait and DPRK, with a total volume of commodities worth USD 28.000 of imports by Kuwait from the DPRKs and of USD 17.600 of exports from Kuwait to the DPRK in 2023. Exports related mostly to used vehicles, and imports involved goods mostly in the categories of eletronic equipment and essential oils/cosmetics/toiletries.

4. Kuwait has no DPRK financial institutions licensed in the country and no Kuwaiti financial institutions have a branch in DPRK. An analysis of CBK funds flow data for the years 2021, 2022 and 2023 revealed that no funds transfers to/from DPRK through the Kuwaiti banking system or through formal money transfer services have taken place. No work applications from citizens of the DPRK have been recorded in Kuwait.

5. Kuwait's location at the crossroads of major shipping routes that connect Europe, Africa, and Asia makes its ports and airports important logistical hubs for international trade. This harbors a certain risk for Kuwait to be used as a conduit for Proliferation Financing -related transactions and trade, especially through maritime routes that are difficult to monitor comprehensively. Goods, including dual-use items (those with both civilian and military applications), may be misdeclared or transhipped through Kuwait to obscure their final destination, entailing the possibility for its financial system to inadvertently facilitate Proliferation Financing -related transactions.

6. Businesses in Kuwait, particularly in the shipping and logistics sectors, may find it difficult to trace the end-users of the goods they are financing or facilitating, thereby increasing the risk of inadvertently supporting proliferation activities. The smuggling of goods across the desert border with Iraq also remains a Proliferation Financing concern for Kuwaiti authorities.

7. Kuwait's financial institutions, which include commercial banks and money service providers, engage in a significant volume of cross-border and international trade related transactions, especially with countries in the Middle East, Africa, and Asia. Kuwait's extensive network of suppliers and contractors in industries related to petrochemicals, machinery, and transport may unknowingly facilitate the trade of dual-use goods or technologies linked to proliferation. International trade financing mechanisms, such as letters of credit or documentary collections, may be used to facilitate the shipment of dual-use goods with an associated underlying proliferation financing risk.

8. The below cases discuss techniques and methods used by those engaging in proliferation financing and sanctions evasion related to the activities covered are those falling under targeted financial sanctions regimes relating to the financing of proliferation of weapons of mass destruction under UNSC resolutions **1718**, **1874, 2087**, **2094**, **2270**, **2321**, **2356, 2231**.

9. The typologies are compiled from:

- The 2008 FATF Proliferation Financing Report Typologies Report on Proliferation Financing
- UNSC Panel of Experts report - S/2016/157;
- UNSC Panel of Experts report - S/2017/742;
- UNSC Panel of Experts report - S/2018/171;
- RUSI 2018 publication – Underwriting Proliferation: Sanctions Evasion, Proliferation Finance and the Insurance Industry;
- United States' 2022 National Proliferation Financing Risk Assessment and The 2024 Asia/Pacific Group on money Laundering (APG) Typologies Report.

10. The cases described involve many different sectors worldwide, including the financial, trade and shipping sectors.

Proliferation Financing Typologies

Typology 1 – Accessing the global financial system

11. Due to the sanctions framework in place, the DPRK's proliferation financing efforts often involve the use of networks of front companies, nominees, and unusually structured transactions in several jurisdictions.

Case Study 1: Pan Systems and Glocom

Pan Systems Pyongyang (Pan Systems) and its front companies used an extensive network of individuals, companies, and offshore bank accounts to procure and market arms and related material. One of these front companies is Glocom, which claims to sell battlefield radio equipment and accessories, but is said to be operated by the Reconnaissance General Bureau (RGB) – a DPRK intelligence agency that manages the DPRK's clandestine operations. The global network consisted of individuals, companies, and bank accounts in China, Indonesia, Malaysia, Singapore, and the Middle East.

Since 1998, Pan Systems and International Global Systems (a Malaysian company with connections to Glocom) have used foreign currency accounts (in USD and Euros) at Daedong Credit Bank (a DPRK Bank) to in turn gain access to the international financial system through bank accounts in other jurisdictions (e.g., China).

These accounts were used to transfer funds to a supply chain of more than 20 companies located primarily on the Chinese mainland, in Hong Kong, and Singapore. In recent years, this has shifted almost entirely to

companies in China and Hong Kong. Most of these companies supplied electronic products, radio components, and casings consistent with Glocom's advertised military communications equipment, while others were transport companies. The network also made regular transfers to various facilitators with Chinese, Korean, foreign, and code names working in China, Indonesia, Malaysia, and the Middle East.

Case Study 2: Financial operations of Glocom in Malaysia

In addition to its four bank accounts with the Daedong Credit Bank in Pyongyang, Glocom and its network of related entities controlled at least 10 accounts in four other countries between 2012 and 2017, through Malaysia-based front companies. These multiple overseas accounts allowed Glocom to continuously move funds between accounts it controlled in different banks and countries in the course of its illicit trade.

Kim Chang Hyok, the representative of Glocom in Malaysia, held the sole signing authority for the accounts of the front companies he directed – namely International Golden Services and International Global System. In contrast to other cases in which nationals of the DPRK sought to conceal their links to the country on official documentation, the onboarding paperwork at a Malaysian bank used by Kim showed the bank was fully aware that these accounts were controlled by the DPRK. Kim Chang Hyok declared himself to be a national of the DPRK, indicated that the country was also the source of the funds and that he intended to open a factory in Malaysia.

Alongside the front company accounts he controlled, Kim Chang Hyok also maintained four personal accounts in a Malaysian bank. His day-to-day expenditure was conducted almost exclusively using his credit card, including frequent maximum daily cash withdrawals from ATMs. The cash withdrawals were split between his accounts, further limiting the bank's view of the nature of his activity. There was also the presence of periodic bulk cash injections or large in-house cheque deposits that replenished those accounts.

Case Study 3: Maintaining Representative Offices and Agents Abroad

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

The representative in Dalian of DCB and DCB Finance undertook transactions in US Dollars, with single transactions occasionally exceeding the $1 million mark. He also facilitated payments and loans between companies linked to DCB and exchanged large quantities of bulk cash transferred to China from the DPRK into US Dollar notes of higher denomination. Additionally, the representative also undertook foreign exchanges between US Dollars and Euros, transferring balances between DCB and its shareholder

(mainly Korea Daesong Bank). When DCB established representative offices in Shenyang in late 2012, and Dandong in 2014, the three offices cooperated in managing the activities of foreign exchanges, transfers, bulk cash exchanges and loans.

Typology 2 – Use of ledgers to evade financial sanctions

12. One particular method of sanctions evasion is through the use of a ledger system, which helps avoid transferring funds directly through sanctioned entities. A pertinent example can be found in the way through which Glocom paid its suppliers and made transfers through its network.

Case Study 4: Glocom paying suppliers

First, a national of the DPRK would make a bulk cash deposit into one of the Glocom accounts in Pyongyang. This deposit would be reconciled by ledger with accounts controlled by Kim Chol Sam, the then-representative of the Daedong Credit Bank in China. On the same or the next day, Kim Chol Sam would initiate a transfer to the intended recipient in Malaysia or Singapore for the same amount.

To do so, actual funds would flow from the account where the deposit had been recorded to a DPRK-controlled front company in Hong Kong, less transfer fees and a commission for middlemen. The front company would then in turn remit funds to the intended recipient. As a result, the receiving financial institution in Malaysia or Singapore would see only an incoming payment from the Hong Kong front company, rather than one from International Global System or Pan Systems — the actual holders of the accounts with the Daedong Credit Bank. The same was true of correspondent banks processing the transactions, including those in New York, which would have little insight into the origin or beneficiaries of the transaction. In addition to paying suppliers in this fashion, Glocom used the same method to move money within its own network, specifically between its front company accounts in Pyongyang and those in Malaysia.

Glocom clients were instructed not to directly remit funds to Pan Systems or International Golden Services accounts, but rather to pay other accounts in the names of Hong Kong front companies. Through Daedong Credit Bank, Glocom used accounts in the names of Malaysian and Singaporean front companies as well as Pan Systems to receive remittances from Hong Kong front companies. Kim Chang Hyok (a.k.a. James Jin or James Kim), representative of Pan Systems in Malaysia, established multiple accounts in the country in the names of front companies on behalf of Glocom. In a series of transactions to its suppliers, Glocom transferred over $350,000 through at least seven front companies in Hong Kong in multiple transactions cleared through three New York-based and one Hong Kong-based bank. Records show that payment for a single invoice was often done through a series of instalments from multiple front companies, another means of hiding the identity of the true parties and evading detection by authorities of illegal conduct. One Singaporean supplier to Glocom employed a business manager from the Democratic People's Republic of Korea to "source business" in the country and provide a $100,000 deposit to the company against which balances were settled in addition to transactions from front companies, all without having to transact with the Democratic People's Republic of Korea.

Daedong Credit Bank also used a ledger system for its operations in China. This system allowed Daedong Credit Bank representatives abroad to use accounts in their names or those of front companies — whose names never appeared in the transactions — to undertake transactions on behalf of entities and banks of the DPRK, including designated entities. The system kept funds in circulation outside of the DPRK by using revenues from the country's commodity sales to replenish Daedong Credit Bank's accounts abroad. All of this removed the risks of detection arising from wire transfers directly from a bank in Pyongyang.

Typology 3 – Misuse of legal entities and arrangements

13. Legal entities and arrangements can be misused in numerous ways to facilitate proliferation financing. These entities often provide a veneer of legitimacy that enables illicit financial flows, shielding the true nature of the transactions and obfuscating the involvement of sanctioned or proliferating states and individuals. Take, for instance, the use of joint ventures with the DPRK by Korea General Corporation for External Construction to generate profit.

Case Study 5: Establishing Joint Ventures to Generate Revenue

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

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

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

Typology 4- Theft and money laundering in conjunction by DPRK-backed cybercriminals

14. Cybercriminal groups with ties to the DPRK (and specifically the RGB) are a known avenue for helping facilitate the DPRK's proliferation financing programmes. The RGB in particular has fostered military hacking groups such as those going by the names Lazarus Group and Advanced Persistent Threat 38 (APT38). The following example from the US Department of Justice (the DOJ) shows the multiplicity of ways in which DPRK-connected cybercriminals steal and launder the proceeds of crimes, as well as the increasing reliance on cryptocurrency.

Case Study 6: RGB hacking financial institutions for money and cryptocurrency

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

Simultaneously with the above indictment, the DOJ also indicted Canadian citizen Ghaleb Alaumary, who agreed to plead guilty in a money laundering scheme and admitted to being a high-level money launderer for multiple criminal schemes, including a cyber-enabled bank heist orchestrated by North Korean hackers.

The schemes used by both the North Koreans and Canadian citizen included:

Cyber-enabled heists from banks: Attempts from 2015 through 2019 to steal more than $1.2 billion from banks in Vietnam, Bangladesh, Taiwan, Mexico, Malta, and Africa by hacking the banks' computer networks and sending fraudulent Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages.

Ransomware and cyber-enabled extortion: Creation of the destructive WannaCry 2.0 ransomware in May 2017, and the extortion and attempted extortion of victim companies from 2017 through 2020 involving the theft of sensitive data and deployment of other ransomware.

Creation and deployment of malicious cryptocurrency applications: Development of multiple malicious cryptocurrency applications from March 2018 through at least September 2020 – including Celas Trade Pro, WorldBit-Bot, iCryptoFx, Union Crypto Trader, Kupay Wallet, CoinGo Trade, Dorusio, CryptoNeuro Trader, and Ants2Whale – which would provide the North Korean hackers a backdoor into the victims' computers.

Targeting of cryptocurrency companies and theft of cryptocurrency: Targeting of hundreds of cryptocurrency companies and the theft of tens of millions of dollars' worth of cryptocurrency, including $75 million from a Slovenian cryptocurrency company in December 2017; $24.9 million from an Indonesian cryptocurrency company in September 2018; and $11.8 million from a financial services

company in New York in August 2020 in which the hackers used the malicious CryptoNeuro Trader application as a backdoor.

Marine chain token and initial coin offering: Development and marketing in 2017 and 2018 of the Marine Chain Token to enable investors to purchase fractional ownership interests in marine shipping vessels, supported by a blockchain, which would allow the DPRK to secretly obtain funds from investors, control interests in marine shipping vessels, and evade U.S. sanctions.

Typology 5 – Workers supporting PF activities

15. In recent years, the DPRK has made extensive use of its workers (particularly in the IT field) to support the regime's proliferation financing activities. It should be noted that DPRK workers are the subject of specific UNSCR provisions, which require all DPRK workers abroad, regardless of their visa status, be repatriated to the DPRK.

16. Similarly, countries with proliferation risks have used students studying abroad in science and engineering courses which could be used for gaining knowledge and expertise for further use in WMD programmes.

Case Study 7: IT workers involved in Proliferation Financing

The DPRK has used freelance information technology (IT) workers, who represent themselves as legitimate service providers, to generate revenue for eventual repatriation to the DPRK. In contrast to the malicious cyber actors associated with the RGB, the DPRK IT workers often are subordinate to the UN- and U.S.-designated Munitions Industry Department, which is directly responsible for overseeing the country's WMD and ballistic missile programs.
In such scenarios, DPRK IT workers are primarily dispatched to China and Russia, in addition to several other countries. They sometimes rely on tourist or student visas to obfuscate the fact they are in these countries to generate revenue for the regime, thereby evading sanctions. However, China and Russia have not pursued active enforcement of the visa prohibition along those lines – providing an avenue for such IT workers to obscure their connection to the DPRK.

Some DPRK IT workers advertise their services on freelance platforms, where they use a variety of methods to obscure their nationality or connection to DPRK state entities, modelled on the methods the Kim regime uses to access the formal financial system. These methods include false identification (including the repeated use of fraudulent credentials by multiple workers across multiple platforms) and the use of front companies in third countries to provide their services. DPRK IT workers will often deliberately seek to work through platforms with weak due diligence and sanctions compliance protocols.

Case Study 8: Known PF procurement entity sponsoring students

Voluntary information received from a Canadian intelligence agency indicated that an individual's (Individual 1) education in Canada was sponsored by a known WMD procurement entity located in Country X and that Individual 1 was possibly a procurement agent.

Analysis of FINTRAC's information revealed that Company A, located in Country X, sent Electronic Funds Transfers (EFTs) to Individual 1 as well as three other individuals (Individuals 2, 3 & 4). For some of the EFTs, the transaction was noted to be for "cost of study". All EFTs were sent to personal bank accounts and totalled about $140,000 US.
Other than all receiving funds from Company A, no apparent connections between the four individuals were identified. Individuals 1 & 2 were found to be located in two different Canadian provinces, while no address was found for either Individual 3 or Individual 4.

During the same period, a Large Cash Transaction Report (LCTR) received from a depository financial institution indicated that Individual 2 also deposited about $10,000 US into his/her personal account. The LCTR further indicated that Individual 2 was a student.
It is unknown why Company A would be funding the education of these four individuals. However, the research field in which Company A was involved indicated a possible association to a WMD program. In addition, at the time, Country X was known to sponsor students who agreed to study overseas in science and engineering programs. It was suspected that Country X's objectives were to gain knowledge and expertise in some areas that could be useful for its WMD programme.

Typology 6 – Transactions for components used in DPRK rockets

17. Components used in connection with proliferation programmes are difficult to source for countries such as the DPRK. For this reason, complex payment schemes may be used to conduct transactions involving such parts. The following example illustrates a complex circular payment scheme used by Korea Chonbok Trading Corporation (Chonbok) in Pyongyang purchased large number of pressure transmitters for use in DPRK rockets.

Case Study 9: Circular Payment Scheme used by Chonbok Trading Corporation

The scheme involved two Taipei-based companies – Royal Team Corporation (RTC) and another company (Company A) – as well as Korean International Exhibition Corporation (KIEC), a company in the DPRK. It functioned through the three companies arranging to compensate one another's creditors so that no foreign transaction was required.

Here, several of the companies held outstanding debts to others; Company A owed approximately the same amount to KIEC (for the participation of Taipei-based companies in a trade fair) as Chonbok owed to RTC. Company A transferred funds to RTC, while Chonbok paid KIEC the amount owed to RTC, in effect cancelling out the parties' debts to one another. RTC subsequently changed its explanation of the transaction by removing mention of Company A, instead stating that Chonbok had transferred cash directly in Pyongyang, which RTC had then immediately turned over to KIEC for the organization of the participation of Taipei-based companies in a fair.

RTC was unable to provide records for either of the two payment scenarios. Its managers were obliged by law to declare to the authorities the foreign currency revenue from Chonbok of €28,350. However, it would have been impossible for the regulatory authorities to detect any transaction. It appeared that RTC evaded local regulations, whether by design or omission, and consequently assisted the DPRK in evading sanctions.

Typology 7 – Proliferation financing through information-stripping

18. Singaporean authorities uncovered an extensive scheme through which a series of Singaporean companies were used to transmit and obscure the origin of funds used for the benefit of the DPRK to support specific arms-related shipments and for more general purposes.

Case Study 10: Information stripping by Chinpo Shipping Company

The Singapore Court charged Chinpo Shipping Company (Private) and its Director, Tan Cheng Hoe, with providing financial services or transferring financial assets or resources to Ocean Maritime Management Company Limited (OMM) – an entity which was sanctioned by the UNSC for its role in arranging the concealed shipment of arms from Cuba to the DPRK.

The Court found that Mr. Tan had transferred $72,016.76 to a foreign shipping agent for the shipment aboard the Chong Chon Gang in July 2013 (intercepted by Panama). Chinpo "had conducted no due diligence whatsoever" before transferring the funds on 8 July 2013. Chinpo made 605 outward remittances totalling $40 million between 2009 and 2013 on behalf of nationals of the DPRK, with Mr Tan describing himself as a "payment agent" for OMM.

Court documents indicated that, although Chinpo at one time mentioned vessel names in its outgoing remittance forms, it ceased that practice in the second half of 2010. According to Mr. Tan's statement, "more questions were asked by the bank in the United States when the vessel name was included, and some processing banks will reject the transaction after asking for more information". He then stated that the Singapore branch of Bank of China, from which Chinpo had undertaken the transaction of $72,016.76, "had advised [Chinpo] to leave out the vessel name in transactions, that bank was aware that the remittances were being conducted on the behest of Democratic People's Republic of Korea entities".

Apparently, as a result of that advice, Mr. Tan began to remove vessel names from the payment details. Chinpo similarly advised entities of the DPRK on multiple occasions not to include such names in inward remittances, further assisting sanctions evasion. An employee stated that she had been instructed to include that reminder in outgoing e-mails. Another employee elaborated that the instruction had been included "partly because Chinpo wanted to get the money, and the funds would be blocked by the US if the US knew that the transfers were made in relation to a Democratic People's Republic of Korea vessel". Such information-stripping is consistent with the evasion practices used by other OMM entities and individuals.

Typology 8 – Luxury goods

19. UNSCRs relating to the DPRK also create prohibitions on importing / exporting luxury goods, as such goods can be resold by the regime to affluent members of the DPRK's population to generate revenue for the government, which can be used for proliferation purposes. The example below set out how this prohibition has been circumvented by the DPRK and its associates.

Case Study 11: Supplying luxury goods in the DPRK

Three corporate entities were formed by Chong Hock Yen (Chong) to supply designated luxury goods (e.g., perfumes, cosmetics, watches, musical instruments) to various entities in the DPRK in breach of UN-DPRK Regulations. The activities in question took place between 27 December 2010 to 18 November 2016, in the following way:
SCN Singapore Pte Ltd (SCN) supplied luxury goods to one Bugsae Shop in the DPRK;
Sindok Trading Pte Ltd (Sindok) (known as BSS Global Pte Ltd since 5 February 2015) supplied luxury goods to New Hope Joint Venture Corporation (Pyongyang) in the DPRK;
Laurich International Pte Ltd (Laurich) (known as Gunnar Singapore Pte Ltd since 15 August 2016) supplied luxury goods to MG Corporation in the DPRK.

Between November 2011 and May 2014, transactions valued at more than $5 million were made through a Daedong Credit Bank account to SCN as well as to another unrelated company for payment for goods sold at the Bugsae Shop, as well as other expenditures. More than 10 transactions ranging from $70,000 to $150,000 were made through this account to SCN Singapore Pte Ltd to an account at Overseas-Chinese Banking Corporation Limited Singapore.

Goods were indirectly sent to the DPRK – generally via shipment through China, with payment being made through front companies incorporated in countries such as Hong Kong, the British Virgin Islands, and Anguilla. It was also noted that many of the trades took place during a period where the DRPK conducted an increasing number of missile and nuclear tests.

Typology 9 – Re-naming and re-registering vessels following designation (a.k.a. vessel identity laundering)

20. The DPRK uses sophisticated and elaborate techniques to provide laundered identities for direct delivery vessels delivering refined petroleum to it or its vessels. This is in contrast with the simpler form of digital tampering or spoofing of a vessel's automatic identification system (AIS) profile that can usually be detected on maritime databases.

21. As these vacated AIS profiles are no longer attached to an actual physical ship, more than one vessel can utilize the digital profiles. Vacated identifiers have been used by stateless direct delivery vessels. The example of the New Konk below shows how this can happen in practice.

Case Study 12: The New Konk as F. Lonline

The New Konk was a feeder tanker that conducted a ship-to-ship transfer with the Vifine (now known as the DPRK-flagged Un Hung), with the latter then delivering refined petroleum to the DPRK. Shared ownership, management and corporate registry associations between the two vessels, indicating similar entities linked to sanctions-related activity was identified. The New Konk itself subsequently began delivering illicit cargo directly to the port of Nampo on a repeated basis, leading to its recommendation for designation. To continue its illicit deliveries, the vessel then adopted different laundered vessel identifiers, occasionally sailing in 2020 as the M0uson56 and as the F. Lonline.

Further investigations into the F. Lonline suggested another case of complex vessel identity laundering involving the former Thailand-flagged Smooth Sea 3, which resulted in the creation of a fraudulent digital identity – the F. Lonline – used by suspect vessels such as the New Konk to swap into. This case of identity laundering also involved the same entities and shipyards/dockyards for laundering the identities.

To further enhance its disguise following its identity launder, the New Konk was observed docked during the first half of 2021 at a shipyard owned by Fujian Yihe Shipbuilding Industry Co. Ltd and painted a different colour.

The management and ownership history of the F. Lonline is connected to other vessels that have likewise laundered their identity. While currently listed as owned and managed by Hong Kong-incorporated Brilliant Trade International since October 2019, the F. Lonline was owned and operated by Smooth Sea Co. Ltd., sailing as the Smooth Sea 3 from June 2004 to June 2019, before it was transferred to Rui He HK Marine Co. Ltd., to sail under a different flag and ship name. The vessel was passed on a month later to Cheng Xin Shipping Ltd., reflagged under Belize and renamed the F. Lonline three months later. The Hong Kong-incorporated Cheng Xin Shipping Ltd. has been associated with the Smooth Sea in a case of suspected vessel identity laundering. The New Konk, the Mouson and the Hai Zhou 16868 all visited the Fujian Yihe shipyard and departed transmitting fraudulent new digital identities.

Typology 10 – Maritime insurance and sanctions evasion

22. Insurance products relating to the maritime sector may be used by designated persons to evade international sanctions. However, rather than being used for directly raising funds for proliferation, insurance is typically utilised for facilitating other proliferation-connected activities. This can be illustrated through the case of the ships *Lighthouse Winmore* and *Billions No. 18*.

Case Study 13: Lighthouse Winmore, Billions No. 18 and the insurance scam

Ship-to-Ship transfers have become a frequent means of sanctions evasion, with frequency and value seeing unprecedented increases since 2018. The UN Panel of Experts' investigation of petroleum transfers showcased a very sophisticated example of DPRK-related vessel identity fraud, highlighting new sanction evasion techniques that defeated the due diligence efforts of the region's leading commodity trader, as well as the United States and Singaporean banks that facilitated the fuel payments and a leading United

Kingdom insurer that provided protection and indemnity cover to one of the vessels involved. The same case underlines the extremely poor reporting, oversight, monitoring, and control over the vessels exercised by the flag-of-convenience States under whose jurisdiction they apparently sail and the lack of implementation of freezing sanctions.

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

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

Investigations into the Lighthouse Winmore highlighted that the tanker was chartered shortly before the ship-to-ship transfer by Oceanic Enterprise Ltd, a Marshall Islands company, via a Singapore-based broker.

Typology 11 – Sanction Evasion Case

23. In many instances, sanction evasion cases relate to the procurement of perfectly legal dual-use goods that are utilized in a manner that is contrary to the DPRK sanctions regime. In the below example it is not the goods in isolation that is the issue, but the provision of those goods to individuals and companies designated under the DPRK regime.

Case Study 14: Contravening Sanctions Laws

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