

Complex Proliferation Financing and Sanctions Evasion Schemes

Complex proliferation financing (PF) and sanctions evasion schemes are major threats to the international financial system. These schemes include the evasion of **PF Targeted Financial Sanctions (PFTFS)** related to the Democratic People's Republic of Korea (DPRK) and other sanctioned jurisdictions, which are covered under Recommendation 7 of the Financial Action Task Force (FATF) Standards ('R.7') and evasion of **other sanctions regimes (such as national and supranational sanctions)**, which are not covered under R.7.

The FATF defines **PF risk** as the potential breach, non-implementation or evasion of the TFS obligations referred to in R.7. Based on this narrow definition of PF risk, the main threat actors identified include the **DPRK** and the state actors, individuals, and entities supporting or working with the DPRK to evade UN sanctions. Many countries have also identified **Iran** and the **Russian Federation** as current PF threats though they are not subject to UN PF-related sanctions or covered under the FATF's definition of PF risk.

4 Major Typologies used in Complex Evasion Schemes

- 1. ENLISTING INTERMEDIARIES TO EVADE SANCTIONS**
 - ❖ **Use of Front and Shell Companies** to access financial systems, facilitate payments and contracts, import or export goods under false pretenses and obscure connections to sanctioned entities.
 - ❖ **Transit through 3rd Countries** to leverage globalized supply chains and international trade.
 - ❖ **Using Bank Accounts and 3rd Country Financing** by routing payments through multiple financial institutions across several countries and taking advantage of jurisdictional differences in 3rd countries
- 2. OBSCURING BENEFICIAL OWNERSHIP INFORMATION (BOI) TO ACCESS FINANCIAL SYSTEMS**
 - ❖ **Third-party Facilitators Supporting DPRK's Access to Financial Access** - use of DPRK citizens such as diplomats and foreign nationals to finance proliferation activity.
 - ❖ **Networks of Unlicensed Financial Facilitators Support Sanctions Evasion** including unlicensed Trust and Corporate Service Providers (TCSPs) and Money Services Businesses (MSBs), which are also used to move funds for individuals acting on behalf of terrorist groups.
 - ❖ **Using Different Types of Legal Persons** such as subsidiaries, to cloud beneficial owner information.
 - ❖ **Exploitation of Credit and Debit Cards by the DPRK** - numerous illegally obtained UnionPay debit cards issued by major China-based commercial banks, in the names of hundreds of domestic account holders to conduct local currency payments.
- 3. USING VIRTUAL ASSETS (VA) AND OTHER TECHNOLOGIES**
 - ❖ **Regulatory Challenges** - exploiting weaknesses in regulatory requirements for Virtual Assets (VAs) and (Virtual Asset Service Providers) VASPs.
 - ❖ **Using VAs to Move Funds** - VAs offer a higher level of anonymity to users and are capable of being transferred across borders instantaneously.
 - ❖ **VAs and Generation of Funds** - theft of VAs and cyberattacks are used to raise funds globally.
 - ❖ **Foreign Entities and Individuals Supporting DPRK Information Technology (IT) Workers** - these persons commit fraud to hide lucrative businesses with DPRK IT workers.
- 4. EXPLOITING THE MARITIME AND SHIPPING SECTORS**
 - ❖ **Altering Vessel ID** - physically altering merchant vessels to obscure their identities by painting over vessel names, using alias flags, and altering unique IMO ship identification numbers.
 - ❖ **Ship-to-ship Transfers** - goods (often cash) are moved between vessels in open waters.
 - ❖ **Disabling Automatic Identification System (AIS) Broadcast** - manipulating AIS broadcasts by altering vessel names, IMO numbers, or other unique identifying information, to conceal a vessel's voyage.
 - ❖ **Falsifying Documents** - use of false documentation when transporting commodities especially for exports of dual-use goods.

Case Study 1

Evasion of PF-TFS related to the DPRK

Exploiting maritime sector to supply gasoil to the DPRK



In late 2019, an individual allegedly conspired with five (5) other individuals abroad to supply approximately 12,260 metric tons of gasoil to the DPRK using the vessel, MT Courageous, on seven (7) occasions. The supplies were facilitated through **ship-to-ship transfers** on the first six (6) occasions, with the final transfer occurring at the Nampo Port in the DPRK. The alleged actions were in violation of Singapore's UN DPRK Regulations and the UNSCR 1718 Sanctions Regime. To facilitate payments for the purchase and supply of gasoil to the DPRK, the individual was accused of utilizing the **bank account** of a company, of which he was a director, on four (4) occasions. The individual also allegedly **falsified documents** belonging to the company on two (2) occasions, and allegedly utilized the bank account of another company under his control to receive payments for the prohibited supply of gasoil to the DPRK, on five (5) occasions.

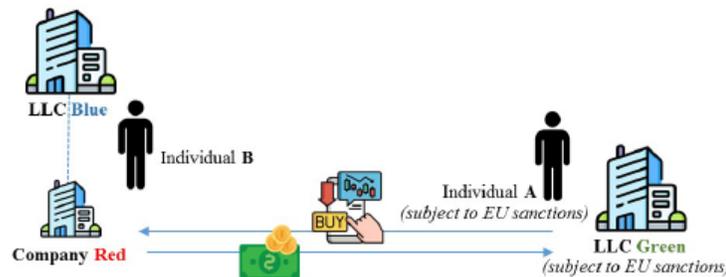
Furthermore, the accused allegedly lied to the investigation officer, disposed of evidence and failed to inform the police about the supply of gasoil to the DPRK by another vessel in February 2019. Consequently, the accused faced multiple charges, including supplying prohibited items to the DPRK, falsifying accounts, acquiring benefits from criminal conduct, obstructing justice and failing to disclose a prohibited transaction. Additionally, the first company, of which the accused was a director, has been charged with four (4) counts of transferring financial assets that may contribute to a prohibited activity in contravention of Singapore's UN DPRK Regulations. The second company faced five (5) counts of acquiring benefits from criminal conduct. Court proceedings are ongoing.

Case Study 2

Evasion of other sanctions regimes (such as national and supranational sanctions)

Complex scheme to evade EU Sanctions

Individual A, who is subject to EU sanctions, coordinated a complex scheme with Individual B to facilitate the evasion of sanctions. First, Individual B, owner of Limited Liability Company (LLC) Blue, established a subsidiary called Company Red. Second, Individual B used Company Red to acquire Individual A's share in LLC Green. Although LLC Green owned 28.5 million shares in a European company, those shares were frozen because LLC Green was controlled by Individual A. Thus, when Company Red acquired Individual A's share of LLC Green, it also acquired the frozen shares of the European company. In exchange for the sale of LLC Green, Individual A received an equivalent economic benefit. Individual B facilitated the evasion of sanctions because he and the Russia-based companies (LLC Blue, Company Red, and LLC Green) used this scheme to **sell a non-EU company controlled by a listed individual** and owning frozen shares of an EU company with the sole purpose to lift the freezing of those shares in the European Union.



Good Practices for Detecting PF and Sanctions Evasion:

- 1) Use of SARs/STRs.
- 2) Automated sanctions screening tools.
- 3) Sharing cross-border intelligence.
- 4) Interagency coordination.
- 5) International cooperation.
- 6) Monitoring tools (open-source intelligence and blockchain analysis)

Mitigating Risks Related to PF and Sanctions Evasion:

- 1) Sanctions screening tools.
- 2) Ongoing monitoring that may lead to the filing of SARs/STRs.
- 3) Customer due diligence.
- 4) Comprehensive assessment of risks.
- 5) Training employees.
- 6) Establishing policies and procedures.
- 7) Negative news screening.
- 8) Enhanced due diligence (EDD).
- 9) Real-time alerts.



References:

FATF Report: Complex Proliferation Financing and Sanctions Evasion Schemes (June 2025).