GAMBLING

Proliferation Financing Typologies

For Gambling Operators

Updated October 2026

Gambling Supervision Commission
Ground Floor, St George's Court
Myrtle Street
Douglas
Isle of Man
IM1 1ED

Proliferation Financing

Gambling Typologies

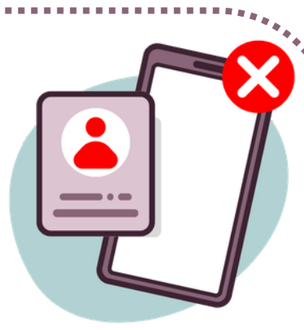
1. Mixers



A Player uses virtual assets to fund the account, which have previously passed through a cryptocurrency mixer. After minimal play, funds are transferred and further mixed before ending up in a cryptocurrency wallet, which is associated with proliferation financing activity.

Online gambling accounts can be used alongside crypto mixers, bridges, and peer-to-peer exchanges to obscure the origin of the funds, making them very difficult to track. Note: for PF (or TF), the funds need not be criminally derived illicit funds, licit funds can also be used to finance PF/TF.

2. Fake ID



Funds are deposited into an online gambling account using a false identity. The player engages in minimal gambling activity which is sufficient to make the account appear genuine. After incurring minimal losses the funds are then transferred from the gambling account to another account associated with a sanctioned state or individual.

3. Legitimate Arm



A criminal colludes with other persons who act as beneficial owners of a company which is used to obtain an online gambling licence. Illegally obtained funds collected from scam 'farms' are then co-mingled with the legitimate profits of the company and deposited in a bank account.

4. Deliberate Losses



Peer-to-peer games such as e-poker, where value transfers can occur between both electronic and human players as a result of deliberate losses, at a relatively low cost to the players. Players will make large bets on very bad hands, expecting to lose to the accomplice. This is generally known as chip-dumping and is considered to mainly pose a risk of terrorist financing.

5. Bots



Unusual / suspicious play is investigated and it is found that multiple accounts are controlled by bots which share similar IP addresses.

6. PePs & Sanctions



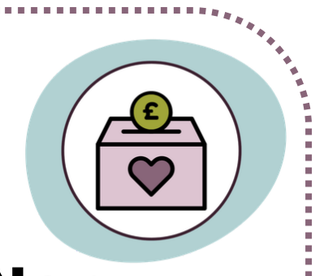
Player associated with a sanctioned state or individual.

7. Dual Use Goods



Upon taking Source of Wealth it is established that a player earns money through the international trade of 'dual use goods' with sanctioned states, such as parts for washing machines, cars and medical equipment.

8. Charities / Non-profit Organisations



The use of legitimate business to fund PF, such as gambling business using proceeds to fund PF activity by donating money to a charity that supports a war effort.

NOTE.

Regularly check adverse media and typology reports, such as UNODC reports, highlighting emerging risks. The latest NRA is available on the counteringfinancialcrime.im website.

GSC GAMBLING

Proliferation Financing

Gambling Typologies

9. Remote IT Workers



North Korean IT workers are deployed overseas through facilitators like Chinyong, where they apply for remote roles in IT companies, globally. The workers will use various obfuscation techniques (Use Fake or Stolen IDs, Deepfakes, VPNs (virtual private networks), and request payment in virtual assets) to hide their identity and location to fraudulently gain employment and funnel "paychecks" to North Korea to fund PF.

10. Reflagging Deception Practice (DPRK)



The UN Panel of Experts has highlighted how the DPRK employed reflagging as a key deception tactic to evade sanctions on petroleum imports. By frequently changing vessel flags, registrations, and nominal ownership, often through short-lived shell companies that were dissolved soon after use, DPRK-linked operators sought to obscure true control of ships involved in illicit ship-to-ship fuel transfers.

This constant reflagging created a misleading appearance of legitimate international ownership and complicated efforts by authorities to trace or seize the vessels. Combined with the use of small, non-IMO-numbered coastal ships, these practices enabled the DPRK to maintain covert supply chains and conceal its continued procurement of restricted petroleum products.

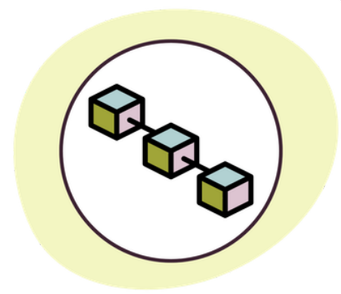
11. AI and Deepfake Technology



The exploitation and abuse of artificial intelligence (AI) The exploitation and abuse of AI introduce an emerging dimension of concern for PF risk. AI systems are increasingly used to automate sanctions evasion, including creating synthetic identities, falsifying trade documents, and operating agentic, AI-driven front companies that can autonomously conduct financial transactions, manage digital wallets, and interact with legitimate commercial entities online.

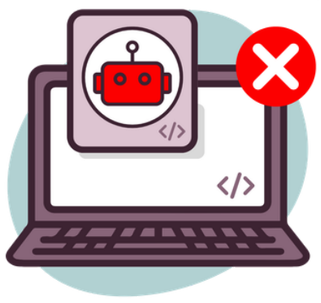
These developments significantly expand the typological landscape for PF, particularly as proliferators leverage AI to disguise the identity of DPRK IT workers, generate false corporate data, and obfuscate links to sanctioned entities. (see above)

12. Unregulated VA / VASPS



Another key typology is the use of VAs and unregulated or lightly regulated VASPs to facilitate payments, obscure transaction chains, and maintain access for sanctioned actors. Several cases showed VASPs providing services to sanctioned jurisdictions or enabling transfers involving sanctioned banks.
Even more concerning, another transaction was flagged as having links to an address associated with a DPRK state-sponsored hacking group.

13. Hacking / Theft



Cyber-criminals stealing cryptocurrency from blockchain addresses controlled by online gambling businesses. In at least one instance, the criminals concerned were acting on behalf of the DPRK. The threat of direct theft from online gambling platform accounts or blockchain addresses therefore carries an elevated PF risk. Crypto-enabled online gambling businesses need to minimise this risk through investment in appropriate ICT security.

14. Intermediary Jurisdictions



PF activity may be routed through third countries or intermediary jurisdictions to obscure links to sanctioned states, entities or end users. Operators should be alert to unusual geographic connections, payment routes or corporate structures that lack a clear commercial rationale.