GSC
GAMBLING

PF Typology: DPRK IT Workers

Proliferation Financing Typology

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

Introduction

The following report focuses on an emerging Proliferation Financing (PF) Typology which reaches across various global sectors.

Note: Although the following typology has not been recorded directly in relation to the gambling industry, given online gambling is an IT/technology focussed industry, and regularly employs IT/software professionals, the GSC would like to make the industry aware of the following risks.

To assist stakeholders in understanding the threat picture, the GSC has summarised key insights from various reports below to highlight the emerging typologies and risks in order to support industry awareness to ensure the sector remains vigilant to evolving threats.

Remote IT workers Typology

Reports in recent years have recorded efforts by North Korea ("Democratic People's Republic of Korea", "the DPRK") to infiltrate companies outside of the DPRK to generate funds for PF. The DPRK uses various methods to finance their regime, however, this report focuses on PF in the DPRK through the exploitation of remote employment opportunities in the west. Recent PF training by the Royal United Services Institute (RUSI) undertaken by GSC staff also noted the emergence of this typology.

Chainalysis reports "*DPRK IT workers are usually deployed overseas through facilitators like Chinyong, where they apply for roles in IT companies globally.*"[1]

The United Kingdom Office of Financial Sanctions Implementation highlight in a recent alert that it is "*almost certain that UK firms are currently being targeted by Democratic People's Republic of Korea (DPRK a.k.a. North Korea) Information Technology (IT) workers disguised as freelance third-country IT workers to generate revenue for the DPRK regime.*"[2]

[1] https://www.chainalysis.com/blog/dprk-it-workers-north-korea-crypto-laundering-networks/

[2] https://assets.publishing.service.gov.uk/media/66e2ec410d913026165c3d91/OFSI_Advisory_on_North_Korean_IT_Workers.pdf

The gambling sector is inherently IT intensive and some operators may seek to outsource technical staff. A recently published report by the by the Multilateral Sanctions Monitoring Team ('MSMT') covering DPRK cyber, and IT worker activities refers to DPRK-linked actors developing gambling websites under false identities.

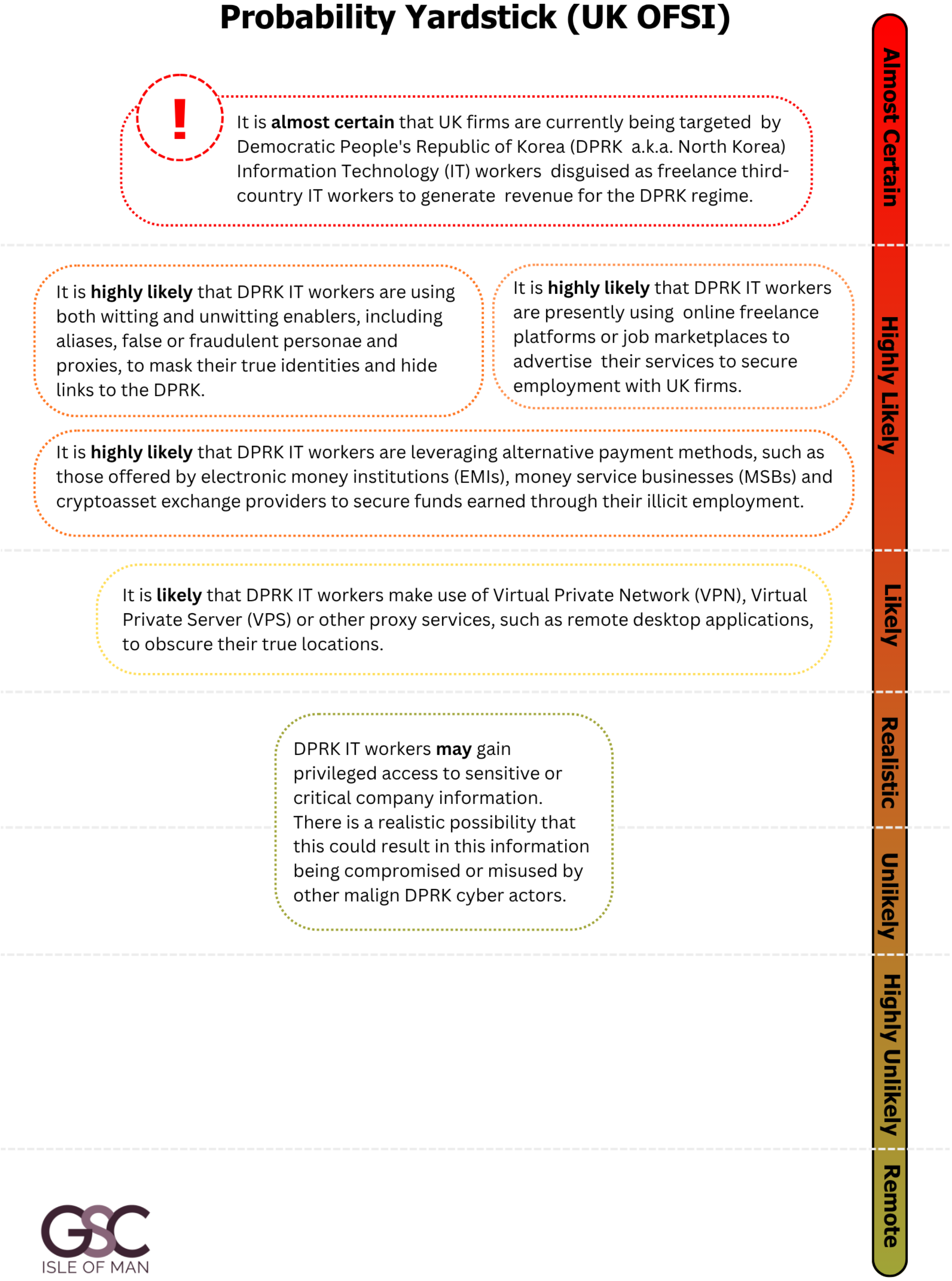
This creates a potential vulnerability that could be exploited by DPRK IT workers who can infiltrate businesses under false identities and use virtual assets as payment to evade international financial sanctions. The GSC is committed operating robust entry and integrity controls and on-going monitoring to protect the sector from exploitation by actors seeking to circumvent international financial sanctions.

Operators may also face customer-related risks, as gambling platforms can be misused to obscure the origin of illicit funds and facilitate layering of funds via in-game transactions virtual assets-linked wallets.

This publication has been produced to raise operator awareness of emerging risks associated with virtual assets and goods, including typologies such as DPRK IT worker exploitation. It outlines key risk indicators / red flags to look out for, practical risk mitigation measures and is intended to serve as a reminder of relevant reporting obligations.

This publication has been produced to make operators aware of these risks, what to look out for, how risks can be mitigated and reporting obligations.

Probability Yardstick (UK OFSI)



It is **almost certain** that UK firms are currently being targeted by Democratic People's Republic of Korea (DPRK a.k.a. North Korea) Information Technology (IT) workers disguised as freelance third-country IT workers to generate revenue for the DPRK regime.

It is **highly likely** that DPRK IT workers are using both witting and unwitting enablers, including aliases, false or fraudulent personae and proxies, to mask their true identities and hide links to the DPRK.

It is **highly likely** that DPRK IT workers are presently using online freelance platforms or job marketplaces to advertise their services to secure employment with UK firms.

It is **highly likely** that DPRK IT workers are leveraging alternative payment methods, such as those offered by electronic money institutions (EMIs), money service businesses (MSBs) and cryptoasset exchange providers to secure funds earned through their illicit employment.

It is **likely** that DPRK IT workers make use of Virtual Private Network (VPN), Virtual Private Server (VPS) or other proxy services, such as remote desktop applications, to obscure their true locations.

DPRK IT workers **may** gain privileged access to sensitive or critical company information. There is a realistic possibility that this could result in this information being compromised or misused by other malign DPRK cyber actors.

UK OFSI Advisory Key threats:

1. It is almost certain that UK firms are currently being targeted by Democratic People's Republic of Korea (DPRK a.k.a. North Korea) Information Technology (IT) workers disguised as freelance third-country IT workers to generate revenue for the DPRK regime;
2. It is highly likely that DPRK IT workers are presently using online freelance platforms or job marketplaces to advertise their services to secure employment with UK firms.
3. It is highly likely that DPRK IT workers are using both witting and unwitting enablers, including aliases, false or fraudulent personae and proxies, to mask their true identities and hide links to the DPRK;
4. It is likely that DPRK IT workers make use of Virtual Private Network (VPN), Virtual Private Server (VPS) or other proxy services, such as remote desktop applications, to obscure their true locations;
5. It is highly likely that DPRK IT workers are leveraging alternative payment methods, such as those offered by electronic money institutions (EMIs), money service businesses (MSBs) and crypto asset exchange providers to secure funds earned through their illicit employment; and
6. DPRK IT workers may gain privileged access to sensitive or critical company information. There is a realistic possibility that this could result in this information being compromised or misused by other malign DPRK cyber actors.

Note: Although the following typology has not been recorded directly in relation to the gambling industry, given online gambling is an IT/technology focussed industry, and regularly employs IT/software professionals, the GSC would like to make the industry aware of the following risks.

Typology Summary:

The DPRK deploys skilled IT workers abroad to fraudulently gain employment with companies in the UK, US and elsewhere, and raise revenue for the DPRK regime. These employees funnel their pay, (and in many cases, information stolen from their employers) back to the DPRK to fund PF.

"*These workers are instructed to deliberately obfuscate their identities, locations, and nationalities, typically using false personas, proxy accounts, stolen identities, and falsified or forged documentation to apply for jobs at these companies. They target employers located in* *wealthier countries, utilising a variety of mainstream and industry-specific freelance contracting, payment, and social media and networking platforms."* – United States Treasury.[3]

Multilateral Sanctions Monitoring Team ('MSMT') Report Covering DPRK Cyber and IT Worker Activities (October 22, 2025)

The report included a case study on Kyonghung Information Technology Exchange Company, a DPRK-controlled entity involved in coordinating overseas IT worker deployments and facilitating cyber operations.

DPRK workers at Kyonghung IT operate in smaller teams of four to develop gambling websites for clients, dividing tasks among themselves such as application development for monitoring and settlement of fund transfers, user account management, web services management and interface design using popular online platforms such as GitHub to share progress updates internally.

Kyonghung IT has also provided search engine optimisation services to criminal organisations to boost the visibility of their illicit gambling platforms.

They attempt to maintain an online presence on various freelance platforms including Upwork and Freelancer, as well as messaging services such as Telegram and WeChat, posing as low-cost freelance developers under falsified identities. These workers typically disguise themselves as Chinese nationals by superimposing their portraits onto images of Chinese ID cards found online, and they often track down the actual owner of the ID card through services such as LinkedIn to mimic their career and certifications in the fictionalised version of themselves.

How?

Hiding Identities

- Workers/applicants may speak good English/other languages;
- Use AI generated profile pictures, Deepfakes or avoid showing their face on video calls to hide their identities;
- Use stolen Identities to pass verification checks;
- Use social media sites (e.g. LinkedIn) and remote working services to secure employment and have excellent-looking CVs and previous work experience to be a desirable employee;

[3] https://home.treasury.gov/news/press-releases/sb0190

- Often university educated (often in China) or otherwise have IT skills relevant to the role;[4]
- It is common for them to complete tasks early or do excellent work early-on to gain initial trust within the company;
- Share information with each other to help evade detection and gain relevant skills.

Obfuscating revenue through blockchain technology[5]

- Often request payment in stablecoins (Virtual Assets), due to their consistent value.
- Once their salaries are paid, DPRK IT workers transfer cryptocurrency through a variety of different money laundering techniques.
- Chain-hopping[6] and/or token swapping[7] - leveraging smart contracts such as decentralised exchanges and bridge protocols to complicate the tracing of funds.
- They are commingled with other proceeds of crime and other DPRK IT workers, through the process of layering before they are funnelled to representatives of the regime who use false identity documents to open accounts at mainstream exchanges

Send funds to the custody of middlemen acting on behalf of the North Korean government after layering/laundering process to be converted into fiat using stolen/fake IDs.

Flags:

⚑ *Target UK industry*

Use of fake CVs and identity documents. Often very promising/too good to be true in order to gain employment and gain trust.

1. Fake CV details: The CVs are false, often look immaculate, very impressive, to ensure they are likely to be hired. Claim previous employment with UK firms to solicit employment;
2. Inconsistent or changing name spelling; nationality; location; contact information; education or work history; and online presence;
3. Failure to complete project tasks;

[4] "The DPRK maintains a workforce of thousands of highly skilled IT workers globally, primarily located in the People's Republic of China and Russia, who generate significant revenue that contributes to its WMD and ballistic missile programs." – United States Treasury Sanctions Press Release, "Sanctions Imposed on DPRK IT Workers Generating Revenue for the Kim Regime"

[5] From Chainalysis report "https://www.chainalysis.com/blog/dprk-it-workers-north-korea-crypto-laundering-networks/ "

[6] Chain-hopping refers to moving virtual assets from one blockchain to another.

[7] Token swapping is exchanging one type of virtual asset for another.

4. Refusal to appear on camera, conduct video interviews or meetings (favouring text-based chat). OR use AI deepfakes and blurred/altered backgrounds to hide identity;
5. Request prepayment but do not meet project benchmarks or attend check-in meetings;
6. Gaining Trust: At first offer to provide free services to earn trust, seeking long term contracts.

Use of online platforms

These workers often use online remote work sites and social media to find work. Or use intermediary firms for recruitment/acquisition.

1. Multiple logins into one account from various IP addresses in a short period of time;
2. Logins into multiple accounts on the same platform from a single IP address;
3. Logged into account continuously for 1+ days;
4. Multiple accounts using the same templates;
5. Multiple accounts receive high ratings from one client account in a short period of time;
6. Extensive bidding on projects but low acceptance rate;
7. Use of platform account resale services.

Use of witting enablers

Non-DPRK workers may "rent out" their identities for profit. Also provide front companies, infrastructure services, laptops or desktop computers that can be accessed remotely.

1. Biographical information does not match the applicant;
2. Inconsistencies when they appear on camera (time, location or appearance);
3. Indications of cheating on coding tests or when conducting interviews;
4. Online presence does not match the hired IT worker's CV;
5. Multiple online profiles with different pictures, or online profiles with no picture.

Use of unwitting enablers

Conceal identity and/or steal account information to verify identities on freelance work platforms, payment providers or with employers.

1. Propose collaboration on development projects with non-DPRK freelancers;
2. Ask co-workers to borrow personal information to obtain other contracts;
3. Request to borrow proxy accounts via social media;
4. Claim to be experienced an IT worker from third countries seeking higher hourly rates for freelance work;
5. Use of anglicised names or pseudonyms;

6. Offer to pay non-DPRK residents a fee for use of their proxy account, sometimes more if the resident has prior experience in the field and/or is willing to conduct calls with clients;
7. Request individuals with a native or high level of English to conduct video and phone interviews with prospective employers and/or clients on their behalf;
8. Ask to be contacted directly via social media or messaging applications.

Use of VPN/VPS/proxy services

Use of services to conceal location and identity, use of laptop farms and remote desktop applications.

1. Prefer remote working arrangements;
2. Use a single, dedicated device for each account;
3. Technical configurations linked with use of remote desktop sharing software;
4. Request hardware to be sent to an address not listed on the IT worker's ID documentation;
5. Claim to not be able to receive items at the address on ID documentation;
6. Operate outside declared business hours. Not reachable in a timely manner.

Use of Electronic Money Institutions (EMIs)/ Money Service Businesses (MSBs)

Purchase EMI or MSB accounts via third parties. Use enablers to consolidate earnings into bank accounts in earners name.

1. Request to be paid into an account using someone else's name;
2. IT worker's bank account is blocked/ deactivated or not accepting payment;
3. IT worker needs to switch bank account;
4. Different individuals (e.g., both client and IT worker) use the same EMI account to transfer/withdraw money;
5. Different EMI/MSB customers share the same device;
6. Frequent transfers of funds through payment platforms;
7. EMI/MSB customers receive funds from and deposit them to each other;
8. Payments made to China-based bank accounts.

Use of cryptocurrencies

Use virtual currency exchanges and trading platforms to manage digital payments and launder funds

1. Request to be paid in cryptocurrency;
2. Seek web3, blockchain, smart contracts and cryptocurrency projects in community chat rooms, forums, social media or freelance platforms;

Privileged access

Collaborate with or support other DPRK cyber actors.

• Exploit and/or build vulnerabilities into smart contracts to steal funds.

• Carry out small scale cryptocurrency thefts or other financially motivated criminality.

• Infiltrate company networks to maintain access for hacking and extortion schemes.

1. Threaten to release proprietary source codes if payments are not made;
2. Participate in white hat competitions and bug bounty programmes to identify vulnerabilities.

Risk and Mitigations

Staff Appointments

The GSC AML/CFT Guidance contains comprehensive information in respect of the gambling (AML/CFT) Code 2019 requirement to establish, record, maintain and operate procedures and controls to enable the operator to satisfy itself of the integrity of new officers and of all new appropriate employees (paragraph 26).

If operators employ remote workers, they may wish to consider undertaking enhanced measures to satisfy themselves in accordance with paragraph 26, and to educate staff on how to recognise the tactics used by DPRK IT workers.

Measures include (but are not limited to)[8]:

- Verifying all identification information supplied by remote workers;
- Monitoring and restricting the use and installation of remote administration tools to unverified employees;
- Prohibiting remote IT workers from using commercial VPNs to access company networks;
- Avoiding paying workers in virtual assets;
- Requiring verification of banking information corresponding to other identifying documents;
- Scrutinising requests for payments to be made into accounts with a different name than that shown-on identity documents;

[8] Deriving from Recommendation 10 of the Multilateral Sanctions Monitoring Team Report: The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities [22nd October 2025]

- Restricting access to personally identifiable information, such as the personal details of other staff;
- Avoiding granting remote IT workers access to proprietary information;
- Training internal human resources teams and contracted third-party staffing firms to identify and understand the red flags associated with and risks posed by interviewing and hiring DPRK IT workers.

Customers

There is the possibility for gambling Operators to be used by DPRK IT workers to facilitate money laundering and sanctions evasion. DPRK IT workers or their networks may deposit illicit funds or virtual assets into gambling platforms.

The GSC's AML/CFT Guidance for Online Operators includes comprehensive information in respect of Code requirements such as customer due diligence and enhanced due diligence, on-going monitoring, name screening systems and reporting procedures.

Virtual Assets

DPRK IT workers exploit virtual assets to evade international financial sanctions to fund proliferation. The GSC publishes AML/CFT Guidance for Virtual Assets for operators that accept any type of virtual asset or virtual goods, use blockchain-based products or services or offer in-house virtual goods. It also serves to benefit operators who do not accept VA deposits, but where VA is identified as a source of wealth or source of funds prior to deposit and there is a known customer link to VA use.

GSC expectations include:

- Integrating VA risk into operators' Business Risk Assessments, Customer Risk Assessments and Technology Risk Assessments;
- Ensuring Business Risk Assessments sufficiently cover PF risks, including jurisdictional risks;
- The consideration of additional checks based on a risk-based approach (e.g. matching IP address to CDD information; adverse information searches; use of blockchain analysis tools);
- Considering verification of identification under the 3,000 EUR threshold using risk-based approach;
- Extent of verification checks should vary depending on risks;
- Enhanced Due Diligence for all high-risk customers;
- Effective transaction monitoring systems which are regularly reviewed; and
- Staff dealing with VA transactions have sufficient training in VA risks, mitigating measures and typologies, including those relating to DPRK IT workers.

Obligations under the Terrorism and Other Crime (Financial Restrictions) Act 2014 ('TOCFRA')[9]

If you suspect you or others are being targeted by DPRK IT workers or are otherwise affected by the threats outlined in this document, this must be reported to the Financial Intelligence Unit. Gambling operators have a statutory obligation to report to the FIU as soon as practicable if you know or have reasonable cause to suspect that a person:

- Is a designated person;
- Has committed an offence under financial sanctions legislation.

Comprehensive sanctions guidance, including Proliferation Financing guidance can be found on the Customs & Immigration website.

Obligations under the Proceeds of Crime Act 2008 ('POCA')[10] and the Anti-Terrorism and Crime Act 2003 ('ATCA')[11]

If you know or suspect that there has been money laundering or terrorist financing activity, operators are reminded of the obligations to make reports to the FIU under POCA and ATCA. If you decide to make a report in this way you should adopt the usual mechanism for doing so i.e. through Themis. Isle of Man FIU Guidance on SARs is available here.

GSC Supervision

The GSC continues to work collaboratively in support of its key regulatory objectives to keep the sector fair and safe from financial crime. In addition to publishing guidance and alerts such as this, the GSC periodically updates its supervisory activities based on emerging risks.

As part of its ongoing review of emerging typologies and risks the GSC has, among other things:

- Undertaken a comprehensive review of its estate which will be translated into GSC supervisory processes and Outreach where appropriate;
- Enhanced legislation through GSC bill in order to improve our onboarding, monitoring and cooperation; and
- Been updating factsheets & Outreach on an ongoing basis to reflect emerging risks/typologies, including those mentioned above.

[9] Terrorism and Other Crime (Financial Restrictions) Act 2014
2014&usg=AOvVaw1WoBBQpiKDD8qam4m0WGYP&opi=89978449
[10] legislation.gov.im/cms/images/LEGISLATION/PRINCIPAL/2008/2008-0013/2008-0013_14.pdf
[11] legislation.gov.im/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0006/2003-0006_4.pdf

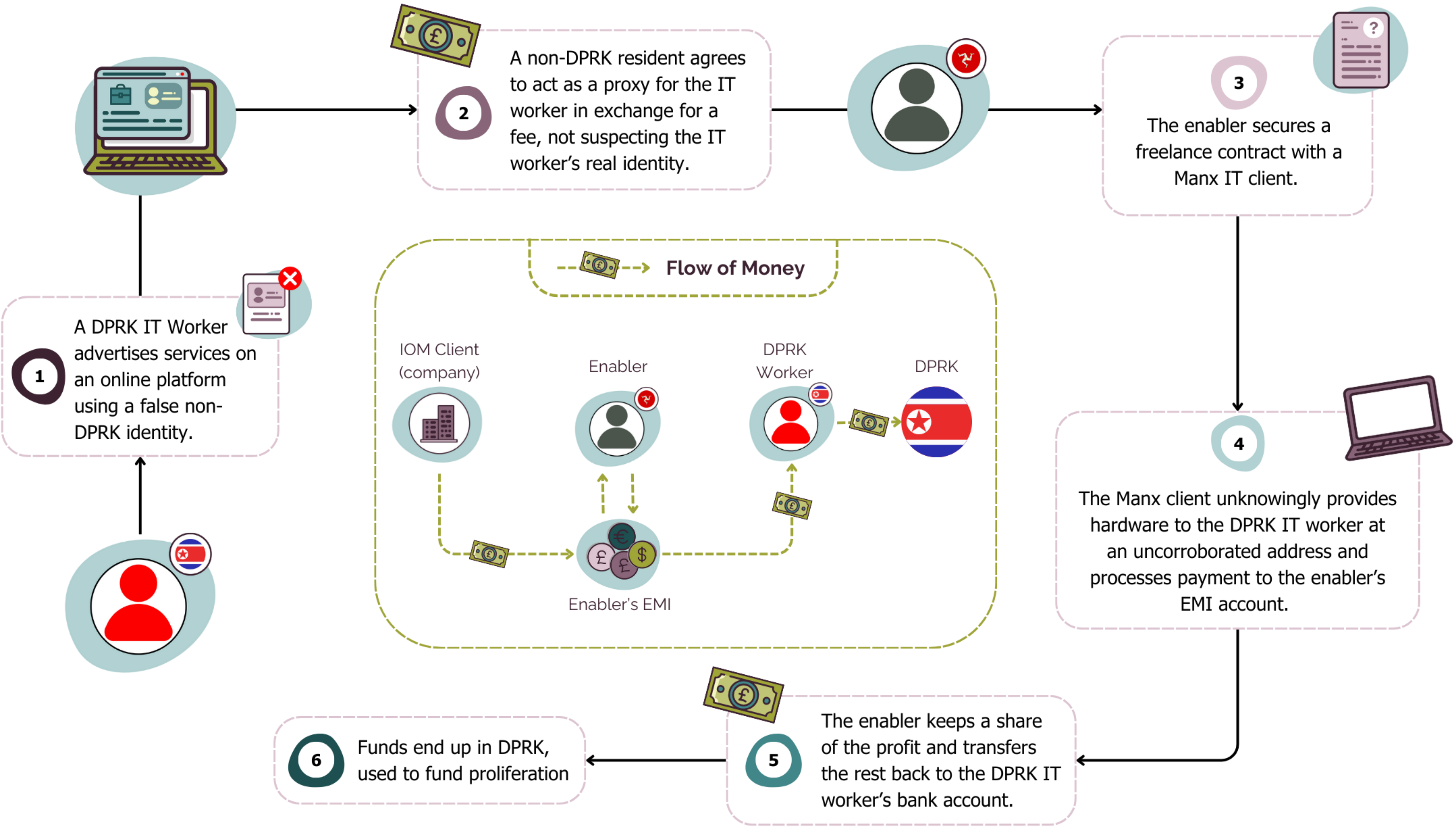
The GSC also continues to work proactively with relevant agencies and law enforcement to ensure, where necessary, actions can be undertaken swiftly and effectively to keep the Island and the global eGaming sector safe. By working together to detect and prevent illicit actors from exploiting the economy, supervisory and enforcement agencies help create a safer, more stable environment for responsible investors and operators.

Appendix: Diagrams and Further Reading

Useful Resources regarding this typology:

- https://assets.publishing.service.gov.uk/media/66e2ec410d913026165c3d91/OFSI_Advisory_on_North_Korean_IT_Workers.pdf
- https://reports.dtexsystems.com/DTEX-Exposing+DPRK+Cyber+Syndicate+and+Hidden+IT+Workforce.pdf
- https://www.bbc.co.uk/news/articles/cm2l2yn5zmxo
- https://www.chainalysis.com/blog/dprk-it-workers-north-korea-crypto-laundering-networks/
- https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html
- https://home.treasury.gov/news/press-releases/sb0190
- https://cloud.google.com/blog/topics/threat-intelligence/dprk-adopts-etherhiding

Case Study 1 Isle of Man company unknowingly hires DPRK IT Worker.



1 A DPRK IT Worker advertises services on an online platform using a false non-DPRK identity.

2 A non-DPRK resident agrees to act as a proxy for the IT worker in exchange for a fee, not suspecting the IT worker's real identity.

3 The enabler secures a freelance contract with a Manx IT client.

4 The Manx client unknowingly provides hardware to the DPRK IT worker at an uncorroborated address and processes payment to the enabler's EMI account.

5 The enabler keeps a share of the profit and transfers the rest back to the DPRK IT worker's bank account.

6 Funds end up in DPRK, used to fund proliferation

If Operators employ remote workers, they may wish to consider undertaking enhanced measures to satisfy themselves in accordance with paragraph 26 of the Code, and to educate staff on how to recognise the tactics used by North Korean IT workers.