Typology 13

Proliferation Financing /// DPRK IT Workers Fraud - TCSP & Crypto

Financial Intelligence Unit - Jersey

Democratic People's Republic of Korea (DPRK) IT Workers Fraud

Background:

Company X, a regulated Jersey Trust Company Service Provider (TCSP), has provided administrative services to Company Y. Company Y, a crypto-currency trading platform, was registered in a non-sanctioned and well-regulated jurisdiction. It was identified that trades executed by Company Y, involved sanctioned wallets connected to Democratic People's Republic of Korea (DPRK) IT workers.

The DPRK IT workers had used stolen or borrowed identities to secure remote work positions and utilised Virtual Private Networks (VPNs), Virtual Private Servers (VPSs), and Remote Desktop applications to obscure their true locations, making it appear as though they were based in non-sanctioned jurisdictions.

These methods helped bypass traditional banking systems and reduced the risk of detection. Funds were transferred through multiple accounts and jurisdictions, involving offshore finance centres, to further obscure their origins. Shell companies and front entities were used to facilitate these transactions, making it difficult to trace the money back to North Korea.

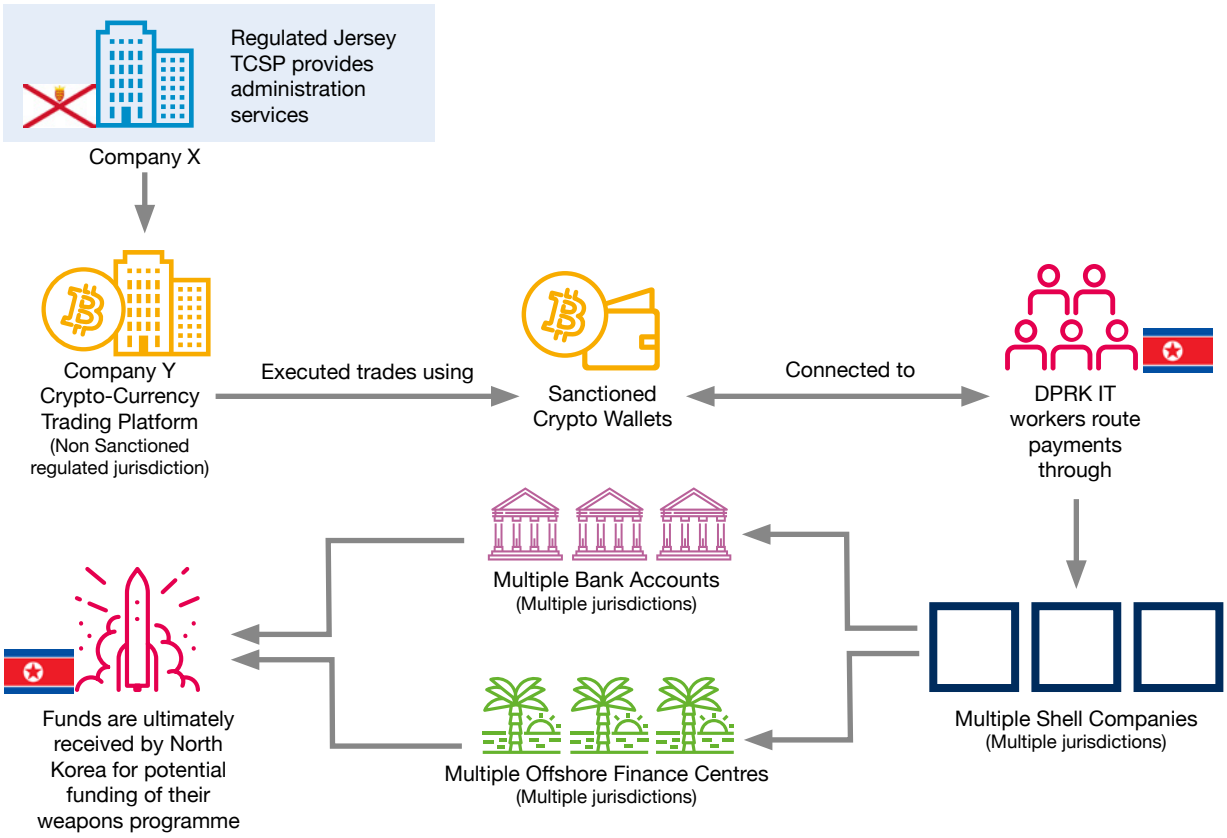
DPRK IT workers, posing as freelance third-country nationals, are employed by companies worldwide, including those in the UK and the US. These workers generate significant revenue for the North Korean regime, which is then laundered through complex financial networks to evade international sanctions.

Indicators:

- False identities and remote work.
- Frequent logins into one account from various IP addresses are often associated with different countries.
- Use of VPNs/VPSs and Remote Desktop applications to obscure true locations.
- Discrepancies in personal information provided during the on-boarding process, such as mismatched names, addresses, or contact details.
- Involvement of complex financial networks makes it difficult to trace the money back to its source origin.
- Funds are transferred through multiple accounts and jurisdictions, often involving offshore finance centres.
- A complex web of transactions involving shell companies and front entities to further obscure the origins of the funds.

Suspicious Activity:

- Alternative payment methods.
- Receiving payments through electronic money institutions and money service businesses instead of traditional banking systems.



- Frequent use of crypto-currency exchanges for receiving payments, which can be harder to trace.
- Multiple logins into one account from various IP addresses in a short period of time.
- Circular – money is usually layered via Jersey and eventually ends up with the person who generated it.

FIU Actions:

- The FIU reviews all submissions, and Proliferation Financing (PF) / Terrorist Financing (TF) related cases will always be prioritised.
- All FIU staff have a sound knowledge and understanding of PF / TF, and on this occasion, was allocated to an FIU officer with specific advanced-level PF / TF knowledge.
- The submission, including any accompanying documentation, was analysed using a wide range of sources available to the FIU.
- Intelligence shares were made with the relevant overseas jurisdictions, including onward sharing with Office of Financial Sanctions Implementation (OFSI) / Office of Foreign Assets Control (OFAC), and the Island's regulator, the Jersey Financial Services Commission (JFSC) as appropriate.
- Identifying links and indicators that include transactions connected with designated individuals, entities, or countries of proliferation concern.
- Engagement locally with the Public-Private Partnership (PPP) Jersey Financial Intelligence Network (JFIN), as well as internationally in matters relating to sanctions, PF and counter-terrorism units to share findings or to request further information from the relevant stakeholders.
- Engagement with international partners.

Outcomes:

- Activity was immediately stopped until the FIU conducted a complete analysis.
- It was highlighted that the wallets were linked to IT workers in DPRK, a high-risk jurisdiction known for PF.
- The sector is not regulated but is supervised.
- Potential failure and missed red flags on the part of the due diligence process were risk assessed as low.
- IT workers are using illicit employment gains to purchase crypto, which is harder to detect and assists with deflecting the money trail.

FIU Comment:

- IT workers infiltrate international companies and secure remote positions under false identities. These operatives not only violate international sanctions but also pose severe cyber-security threats, engaging in fraud and data theft and potentially disrupting legitimate business operations.
- Looking to gain access to the IFC sector and launder illicit funds, which would significantly risk the island's reputation as a well-regulated International Financial Centre (IFC).
- The illicit funds are often routed through crypto-currencies or shadow banking systems, making it harder to follow without the necessary tools and partnerships that FIUs have.
- Institutions should look for reused phone numbers, spelling mistakes in names, repeated email addresses, and typos in application forms, and conduct a deep dive into a subject's employment history using Open Source Intelligence (OSINT).

- Institutions should incorporate indicators into Know Your Customer (KYC) / Client Due Diligence (CDD) procedures, transaction monitoring screening systems and suspicious activity investigations connected to trade finance operations.
- Firms in Jersey must ensure strict compliance with international sanctions, including those targeting North Korea. Failure to do so could result in severe penalties and damage their own organisation and the jurisdictions credibility.
- By pro-actively addressing these risks, Jersey can maintain its standing as a well regulated and threat aware IFC while effectively countering the threats posed by DPRK IT workers.
- The FIU continues to share information effectively with PPPs and international organisations to highlight awareness and identify future typologies.
- The FIU is an important contributor to the Jersey National Risk Assessment (NRA) for PF.

FEEDBACK

Tell us what you think?

We continually strive to enhance the quality of the products we produce. However, we can only improve if you share your feedback with us. This is your chance and we appreciate it. Visit the link below or scan the QR code opposite. Thank you.

go.fiu.je/feedback-product

PolSAR Online Reporting Portal

Have a suspicion about a financial transaction? Submit a Suspicious Activity Report (SAR) via the PolSAR Portal. Access the portal via a web browser and the following url:

go.fiu.je/SAR

Typology 13 **Proliferation Financing** /// DPRK IT Workers Fraud - TCSP & Crypto

Financial Intelligence Unit - Jersey

Maritime House
La Route du Port Elizabeth
St Helier
Jersey JE1 1HB

Tel: +44 1534 612250
Email: fiu.admin@jersey.police.je
Follow us on social media:

WWW.
fiu.je

20251001_1080_V2