Weapons of Mass Destruction (WMD) - TCSPs

Background:

Client X was born in Iran, a sanctioned high-risk country[1], including for Terrorist Financing (TF) and Proliferation Financing (PF). Client X resides in another high-risk Middle Eastern jurisdiction linked to TF risks. Client X approached a Jersey Trust Company Service provider (TCSP) to set up a discretionary trust for succession planning purposes and requested personal bank accounts be held in various currencies for proposed overseas investments.

Client X had business interests in the Middle East and owned Company A in Lebanon and Company B in the United Arab Emirates (UAE). Both companies engaged in 'general trading'[2], focusing on the physical movement of goods, encompassing a wide range of activities, including importing, exporting, and re-exporting. This sector often involves direct engagement in logistics, managing transportation, warehousing, and customs clearance.

Trade can be complex with interconnected supply chains stretching around the world. These have been seen to be exploited by Organised Criminal Groups (OCGs), Professional Money Launderers (PMLs), and TF/PF networks.

Companies A and B sold expensive silk carpets and electronic and mechanical equipment.

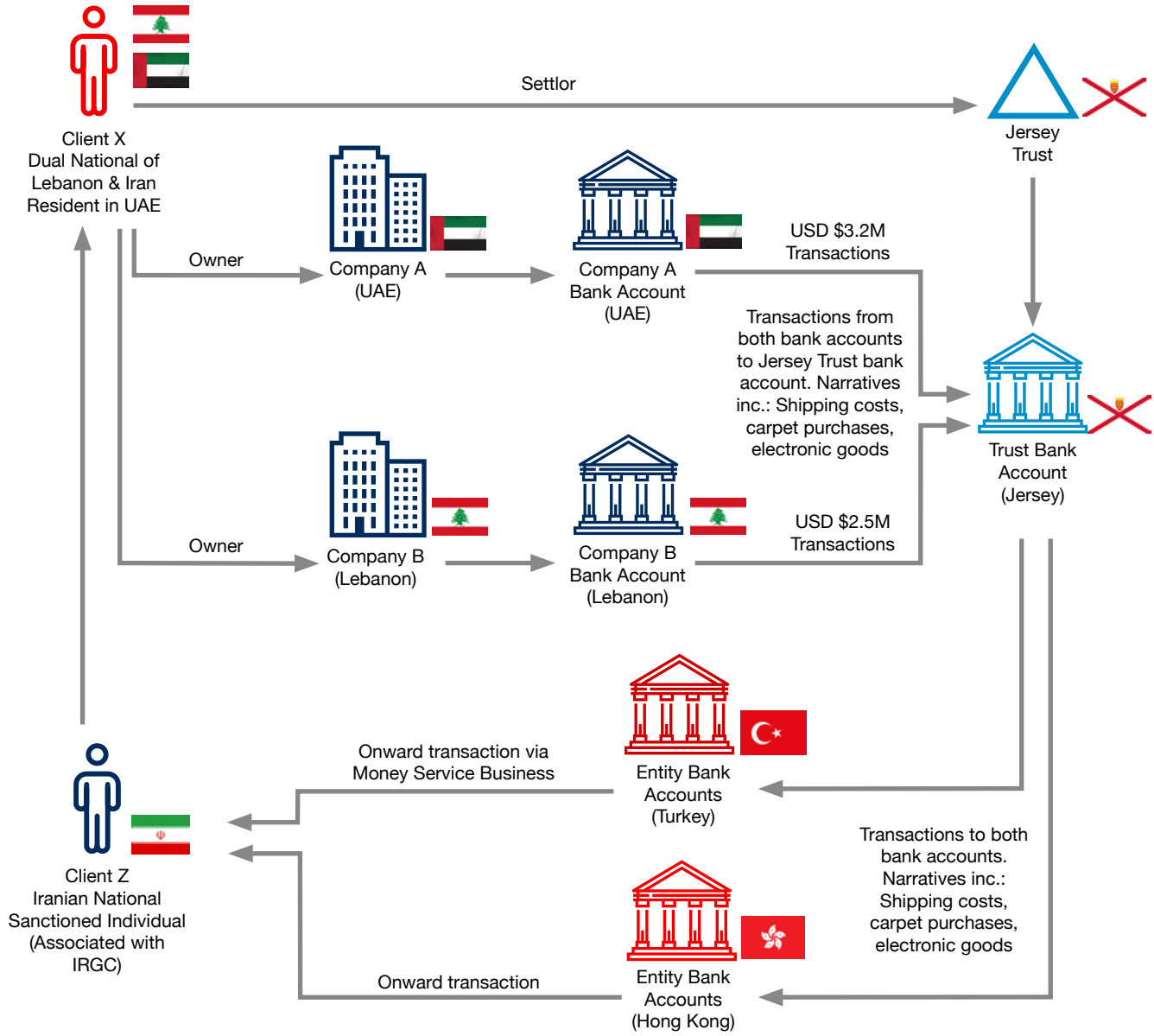
The Jersey-regulated TCSP created a discretionary trust, and personal bank accounts were opened with a Jersey-regulated financial institution.

The bank account activity operated as expected for the first three months. Subsequently, a transaction monitoring alert identified that the account was not operating in-line with expectations. The bank identified that a total of USD 2.5 million had been transferred to Jersey from Company A's bank account in Lebanon, and USD 3.2 million received from Company B in the UAE. Transaction references contained "shipping costs", "carpet purchase", and "electrical goods". The bank identified that several wire transfers were made to entities in Türkiye and Hong Kong, with similar references, usually on the same day for the same amount.

Purchases were also made for high-value cars in the Middle East, including various payments to third-party individuals resident in both jurisdictions of interest.

Open-source research indicated client X was associated with a sanctioned individual, subject 'Z,' who was linked with the Iranian Islamic Revolutionary Guard Corps (IRGC)[3] connected indirectly to an entity involved in the development and production of Weapons of Mass Destruction (WMDs) for the Iranians.

[1] https://www.fatf-gafi.org/en/countries/detail/iran.html
[2] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Trends-and-Developments.pdf
[3] https://www.bbc.co.uk/news/world-middle-east-47852262



Indicators:

- High-Risk Jurisdiction (HRJ) and sector.
- Client X was a dual national of Lebanon, however, he was born in Iran, a high-risk PF jurisdiction as identified by the Jersey Financial Services Commission (JFSC) Appendix D2 Countries list[4] and jurisdictions that are under increased monitoring[5], and assumed to have continued familial links to this jurisdiction and in Lebanon, also a HRJ[6].
- Transactions in and out of the bank accounts involved individuals or entities in foreign countries that were close to countries with proliferation concerns.
- The companies' descriptions of goods were vague, and the financial institution did not hold full beneficial ownership information for either company.
- The companies lacked an internet presence, which is normally expected from the type of business they undertake. They were newly incorporated and managed by Directors in the UAE and Lebanon.

Suspicious Activity:

- There was no information or references relating to the transfers, and the invoices supplied to the bank contained inconsistencies and were handwritten instead of typed.
- Individual wire transactions conducted in large, even USD amounts, with rapid unexplained movement of funds.
- Unusual business activity—Pass-through transactions are usually the same day, which is not normally expected from the type of business conducted.
- Transactions involved individuals or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.

FIU Actions:

- The FIU automatically prioritises PF and HRJ-related cases, and all intelligence officers have fundamental or intermediate training and awareness on PF.
- The FIU engages with domestic competent authorities and internationally with global FIU's and specialist Counter

[4] https://www.jerseyfsc.org/industry/financial-crime/amlcftcpf-handbooks/appendix-d2-countries-and-territories-identified-as-presenting-higher-risks/
[5] https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-february-2025.html
[6] https://www.knowyourcountry.com/lebanon#:~:text=FATF%20Status,having%20strategic%20AML%2FCFT%20deficiencies.

Terrorism / PF units to share intelligence and often request assistance obtaining further information.

- Intelligence shares were made with international FIUs connected to the countries of interest and on client X.
- The FIU undertook further research, including open source intelligence (OSINT) collection and exploitation of other sources and details of the relevant companies and their activities and information regarding the suspected transactions.
- The FIU undertook further Open Source Intelligence (OSINT) research to identify verified sources and details from other FIUs that supported or negated the allegations.
- The FIU will assess the risks associated with PF, identifying potential breaches, non-implementation, or evasion of targeted financial sanctions.

Outcomes:

- Consent to exit was not provided due to an ongoing investigation.
- The transactional information corroborated parts of the initial adverse media reporting identifying client X's links to subject Z, a sanctioned individual indirectly involved in proliferation activity on behalf of Iran.
- The above indicators gave context to the transactions conducted by client X and various related companies and individuals to obtain illicit funds and layer them through Jersey.
- Freezes were placed over the accounts by the financial institution.

FIU Comment:

- Institutions should seek to distinguish the extent of the different risks and similarities between PF, Money Laundering (ML) and TF[7], even if indicators may appear similar. This helps ensure information relating to PF is clearly identified, helping businesses understand their vulnerabilities against different threats.
- Institutions should verify the identities and backgrounds of their clients, understand the intended use of purchased/sold goods, and monitor for any suspicious activity or inconsistencies. Additionally, institutions should utilise red flag indicators and have knowledge of or use reference material to check against dual-use goods[8] which may indicate potential evasions of export controls and sanctions. By identifying and acting on these red flags, institutions can help mitigate the risk of illicit procurement efforts.
- Public-Private Partnerships (PPPs) support effective communication channels and intelligence sharing with partners domestically and internationally. They can also help understand and identify trends and typologies and, therefore, help enable a risk-based approach to customer relationships.
- FIU maintains ongoing public-private engagements, including the local Jersey Financial Intelligence Network (JFIN) and participation in thematic working groups such as Europol-led European Financial Intelligence Public Private Partnership (EFIPPP).
- PF networks can be persistent, resilient, and adaptable to pressures imposed by sanctions and other controls. Once companies are identified and sanctioned, they can disappear and operate under different aliases or names.
- The close geographic proximity between the UAE and Iran facilitates more straightforward and quicker movement of goods, people, and money, which can be exploited for illicit activities. In addition, because the UAE is a significant trade and transshipment hub, it is easier for proliferators to disguise the end destination of goods, which could be used for illicit means, including items used in WMD programmes.
- Both the IRGC and the Ministry of Defence and Armed Forces Logistics (MODAFL), along with their related entities, are listed on the following consolidated lists: Office of Financial Sanctions Implementation (OFSI), Office of Foreign Assets Control's (OFAC) Specially Designated Nationals (SDN) and Blocked Persons list, United Nations Security Council (UNSC) and Jersey Financial Sanctions Implementation Unit (FSIU), due to their involvement in the research, development, and manufacturing, including support for Iran's missile and nuclear programmes.

[7] https://www.fatf-gafi.org/en/countries/detail/iran.html
[8] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

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 14

Proliferation Financing
/// Weapons of Mass Destruction (WMD) - TCSPs

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_1081_V2