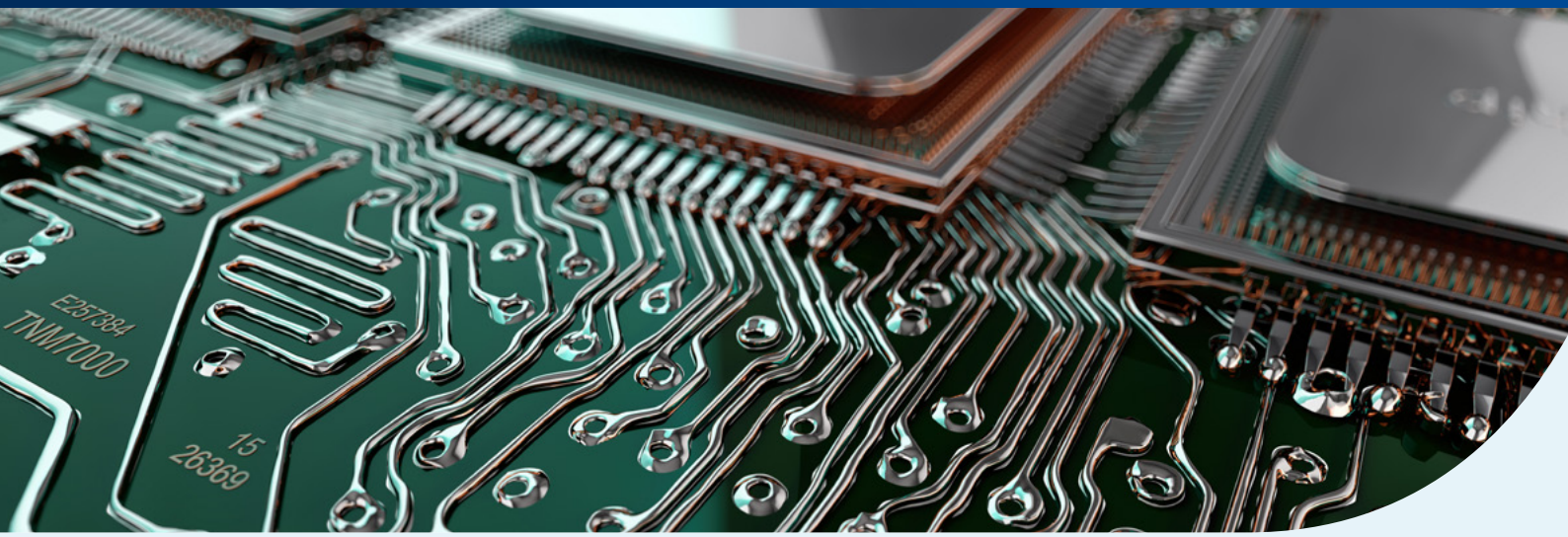
Typology 12

Proliferation Financing /// Dual-Use Goods - Banking

Financial Intelligence Unit - Jersey



Proliferation Financing - Dual-Use Goods - Banking

Background

A Jersey-regulated financial institution provided personal banking services to a Chinese national resident in Hong Kong, 'Client A'. The purpose of the account was to protect savings, save for retirement, and invest overseas. Client A was the Ultimate Beneficial Owner (UBO) of a freight forwarding and logistics company based in Hong Kong with known links to China, 'Company Z'. Client A was also a principal shareholder in another Chinese logistics supply chain entity based in China, providing e-commerce platforms, amongst other products.

A cross-border notification was received from a correspondent bank in Southeast Asia, indicating that it had been identified that Company Z had transacted with several alleged front companies that purchased goods on the global open market and ultimately forwarded them to Iran, in breach of Office of Foreign Assets Control (OFAC), Office of Financial Sanctions Implementation (OFSI), United Nations (UN), and Jersey Financial Sanctions Implementation Unit (FSIU) sanctions.

Funds from Company Z were received in Jersey from the Southeast Asian bank, which held the initial concerns regarding the links to the alleged front companies and sanctioned country. Additionally, it was identified that credits received into the account of Client A from his businesses were rapidly transferred out to either pay off loans or fund property purchases in the UK, further raising concerns.

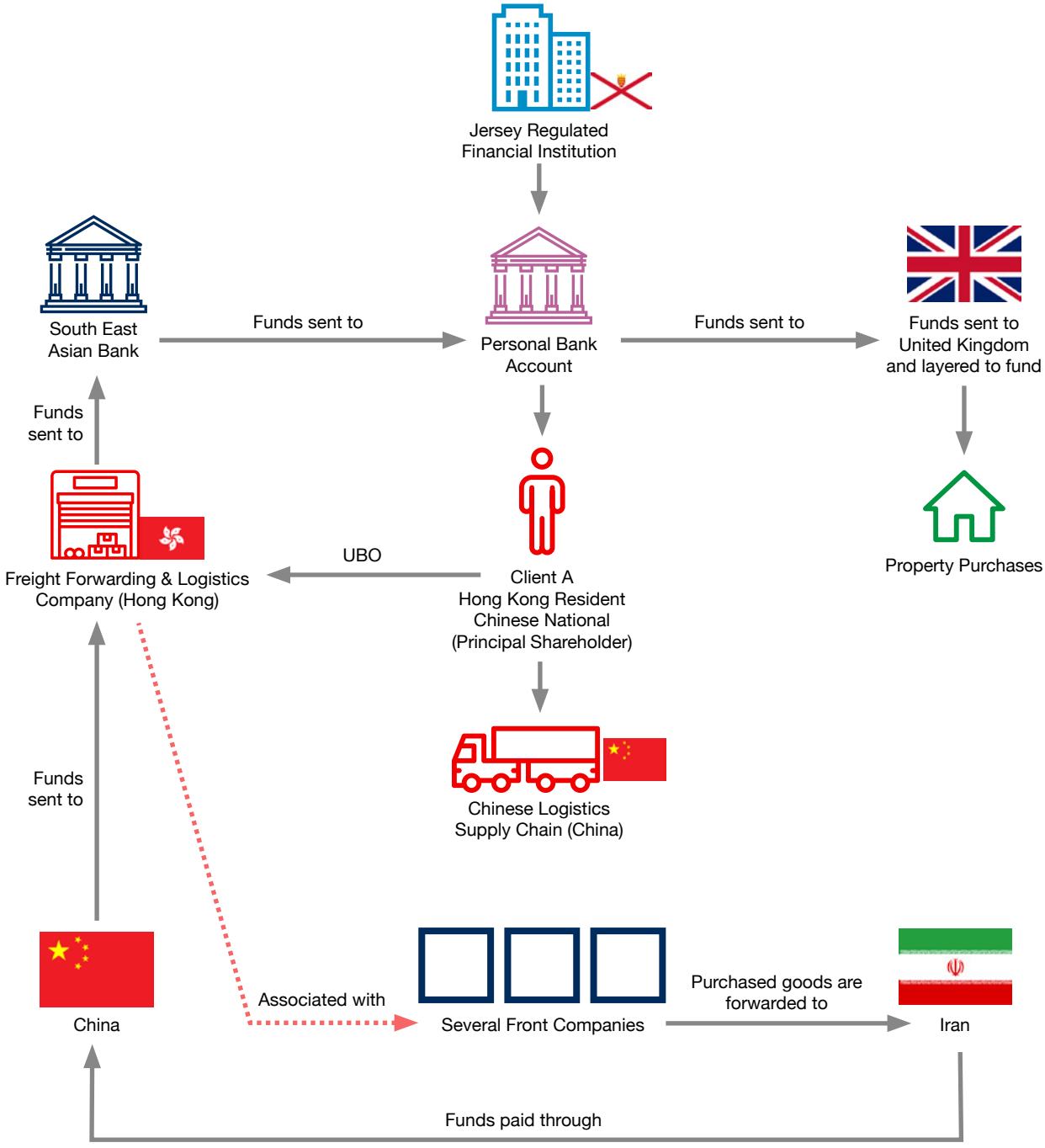
Indicators:

- The country involved falls under high-risk jurisdictions as identified by JFSC Appendix D2 Countries list High risk jurisdictions and sectors[1], including countries with close proximities to sanctioned countries and the use of front companies.
- High volume credits received from external banks are immediately used to purchase property in the UK, indicating layering.
- Cross-border activity and the use of international wire payments with limited oversight of Client Due Diligence (CDD) performed on the source of funds.
- Client A used a fake identity for employment in Southeast Asia, highlighting fraud concerns.
- The account was not assessed to be high risk on opening.
- The companies were dealing with dual-use items.

Suspicious Activity:

- Client A did not disclose that they were the Ultimate Beneficial Owner (UBO) of two logistics/supply chain companies deemed high risk. For those in the supply chain, or even people processing payments, these transactions may appear harmless, but can be a red flag for Proliferation Financing (PF) activity.
- It was a newly established account that had a rapid high turnover of funds.

[1] https://www.jerseyfsc.org/industry/financial-crime/amlcftcpf-handbooks/appendix-d2-countries-and-territories-identified-as-presenting-higher-risks/



- There were various third-party payments from high-risk jurisdictions with lax Anti-Money Laundering (AML) / PF / Terrorist Financing (TF) controls in place.
- Account activity was not in keeping with business expectations.
- The CDD did not include key information relating to the type of business activities, and ultimately, the business activity did not seek to understand the goods being shipped, the identity and jurisdiction of either buyer or seller, the shipping company or the routes.

FIU Actions:

- The submission was graded as high, prioritised, and allocated to an FIU officer with specific higher-level training in PF/TF matters.
- All FIU staff clearly understand and are trained in proliferation and PF.
- The FIU Jersey will assess the risks associated with PF, identifying potential breaches, non-implementation, or evasion of targeted financial sanctions.
- Intelligence was shared with partner agencies and international FIUs, including onward shares with Office of Foreign Assets Control (OFAC) and Office of Financial Sanctions Implementation (OFSI).
- The Bank has blocked the account.
- Matter raised at the next FIU Jersey / Financial Sanctions Implementation Unit (FSIU) meeting.
- Intelligence was shared with jurisdictions with a nexus to the case.
- Enquiries and requests for assistance were made to other International FIUs seeking further information.

Outcomes:

- Consent was not provided until full analysis was completed, with a reliance on obtaining information from other FIUs and understanding any wider international investigations
- Accounts remain blocked internally by the financial institution.
- Client A should have been rated as high risk based on the residency and nationality of the client, the business activity and the geographical location being high-risk.
- Bank to review its existing risk frameworks, including looking at its customers, geographic exposure, products, services and transaction monitoring.
- Transaction monitoring should have picked up the unusual activity if PF red flags had been included as part of the AML / Counter-Terrorist Financing (CTF) / Counter-Proliferation Financing (CPF) risk framework.

FIU Comment:

- Client A was primarily identified because of a cross-border exchange with a correspondent financial institution in Southeast Asia.
- The controls expected to be applied by the financial institution should have escalated to CDD or Enhanced Due Diligence (EDD), alongside comprehensive open-source searches and sanctions screening on the subject and the legal entities with which client A was employed.
- The Jersey financial institution should have reviewed the corresponding banking services in the AML/CTF/CPF framework. The Wolfsberg Group CBDDQ methodology is a helpful guide for this.
- The country was identified as either trading with sanctioned states or lacking sufficient visibility/transparency on traded goods linked to front companies with opaque ownership structures.
- The business activity was linked to dual-use goods and to the use of shipping companies, brokers, and agents to ship goods, often via circuitous routes inconsistent with normal geographical trade patterns.
- In many cases, PF activity primarily aims to generate access to foreign currency and the international financial system. Although it may initially appear to be a routine or innocuous transaction, it is important to understand the full transaction cycle and consider how any trade may be used to enable illicit activity.
- As an IFC, Jersey takes its obligations to ensure that legal arrangements are not abused for PF, which could cause a potential reputational risk to Jersey.
- Jersey implements both United Nations Security Council (UNSC) sanctions and autonomous UK sanctions, although it is not a UN member. The UK's membership extends to Jersey.
- Examples of dual-use items include[2]:
  - Chemicals: Used in both industrial processes and the production of chemical weapons.
  - Drones: Employed for commercial deliveries and surveillance, but also for military reconnaissance and strikes.
  - Nuclear technology: Utilised for energy production and potentially for nuclear weapons development.
- These items are subject to strict export controls to prevent their misuse in the proliferation of Weapons of Mass Destruction (WMDs) and other military applications.

[2] https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation

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

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

20250521_1079_V1