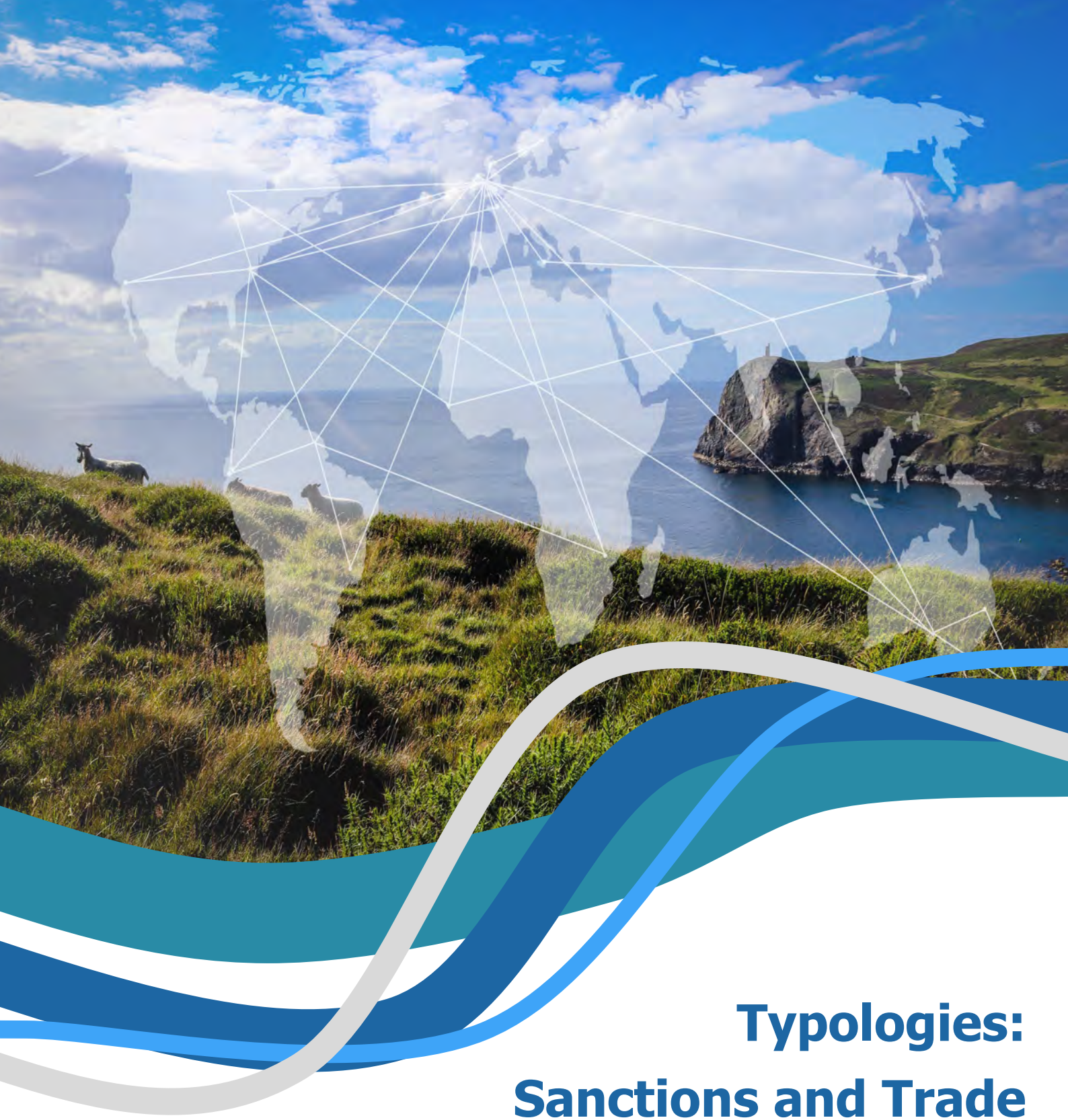


Typologies: Sanctions and Trade Based Money Laundering

February 2023

Isle of Man
Financial Intelligence Unit
Ellan Vannin Unnid Tushtag Argidoil

Contents

Introduction

> **"A typology is the study or systematic classification of types that have several characteristics or traits in common"**
> **-ECOFEL**

The project undertaken by the Isle of Man Financial Intelligence Unit (FIU) to provide typologies to industry is part of the commitment made to fulfil international obligations under Financial Action Task Force (FATF) Recommendation 29 to identify money laundering and terrorist financing related threats and vulnerabilities and as part of its general powers to provide or assist with the provision of awareness training in relation to financial crime.

The following examples are fictional scenarios, loosely based on the type of information received and analysed by the FIU and follow on from previously issued typologies to assist in highlighting areas and focus information the FIU is receiving relating to suspicions of financial crime.

It is envisaged that the following document will ensure those operating in the Isle of Man's regulated industries and those subject to financial sanctions regulations have sufficient knowledge and access to resources to identify this activity within our jurisdiction and will ultimately add value to the information submitted to the FIU.

Note: For the purposes of the examples presented in this document, the term sanctions is used to refer to financial sanctions only.

Sanctions

Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities, or particular sectors, industries or interests. They may be aimed at such people and things in a particular country or territory, or some organisation or element within them.

There are also sanctions that target people and organisations involved in terrorism.

As of 3rd April 2018 the FIU became the IOM body to whom suspicions of breaches of financial sanctions should be reported; this role was previously undertaken by Customs & Excise. The FIU also receives reports where an organisation has frozen an account where they suspect a breach of financial sanctions.

Once the decision was taken by the UK to leave the EU, the UK enacted the Sanctions and Anti-Money Laundering Act 2018 (the Sanctions Act), and UK sanctions regimes are now in force under that act. This legislation has enabled the UK to transition existing EU regimes into UK law and establish UK autonomous regimes. The Foreign, Commonwealth and Development Office (FCDO) updated the UK Sanctions List at 11pm on 31st December 2020 and from that point, it became the definitive list of all UK sanctions imposed under the Sanctions Act.

From 1st January 2021, EU sanctions no longer applied in the IOM. The UK sanctions regime took precedent and has been applied in IOM law. From that date, it became the policy of the IOM Government to maintain the implementation of international sanctions measures in the Isle of Man, in line with such measures as have effect in the United Kingdom.

Note: It is important to note that **only** breaches of UK sanctions should be reported to the FIU under the "Sanctions Breach" legislation option. Any matters relating to OFAC/EU or other sanctions regimes should be reported under POCA, ATCA or FIU Act 2016 Section 24 reports.

Types of Sanctions

Trade Sanctions - In their most extreme form, trade sanctions place a blanket ban on exports and/or imports from a certain country. They come in several different forms, including tariffs and regulations. Countries may also impose trade sanctions against particular industries, companies, or people, within a jurisdiction, rather than on an entire state. This strategy is usually adopted when the sanctioning country wishes to avoid causing extensive damage to the sanctioned country's economy, and has a specific goal in mind.

Financial sanctions - these are used to freeze the assets of certain people or organisations, so that they cannot access their assets held in foreign bank accounts.

Tariffs – these are taxes imposed on goods imported from another country or exported to that country.

Embargoes – trade restrictions that prevent a country from trading with another, e.g. a government can prevent its own citizens and businesses from providing and receiving goods or services from another country.

Non-Tariff Barriers (NTBs) – these are non-tariff restrictions on imported goods and can include licensing and packaging requirements, product standards and other requirements that are not specifically a tax.

Sanctions can be imposed unilaterally (a single country enacting the sanction) and multilaterally (a group or a bloc of countries supporting their use).

Sanctions Red Flags

Obscuring information in payment messages – Society for Worldwide Interbank Financial Telecommunication (SWIFT) payment messages are sent in a manner intended to obscure the identities of sanctioned parties. Information that would identify these individuals is either removed or replaced at the originating institution or a downstream branch. Red flags include the use of Financial Institution (FI) information rather than customer information, different payment processing for sanctioned and non-sanctioned persons, and the re-submitting of rejected payments with information removed or altered.

Misuse of cover payments – disguising the identity of customers through the use of different payments processing procedures, including the sending of wire transfers directly to individuals within the bank who service particular customer accounts. Red flags include the receipt of payment instructions from high-risk individuals, and use of different procedures for payments involving corresponding banks.

Misuse of Special Purpose Entities (SPEs) – payments are routed through SPEs, such as shell companies or investment funds that are owned or controlled by sanctioned customers. The payments appear to be coming from the SPE rather than from the sanctioned individual. Red flags include transactions involving shell companies, and multiple unrelated customers with the same physical address.

Misuse of Suspense Accounts – payments are routed from sanctioned parties through internal suspense accounts to prevent rejection or blocking by other FIs. The outgoing SWIFT messages falsely identify the originating FI, instead of the sanctioned individual, as the payment originator. Red flags include use of a suspense account where the customer is not identified and use of a suspense account where the FI is listed as the originator of the transaction.

Layered routing of payments – payments are structured in highly complicated ways (with no apparent business purpose) to conceal the involvement of sanctioned parties. Red flags include inefficient routing of payments and transactions involving the use of shell companies.

Trade Finance Violations – similar to amending wire transfer payment messages, where FIs obscure references to sanctioned customers or countries in trade finance instruments. Red flags include inconsistent terms within documentation, trade finance transactions that contain transhipments, where products referenced and destinations are vague in nature, and transactions that are inconsistent with the customer's stated normal business.

Amending information on cheques – removal or altering of references to sanctioned individuals when issuing and processing cheques. Red flags include use of handwritten notes when changing transaction terms, and missing payment information.

Use of third party financial institutions – use of unwitting banks within the payment process in order to minimise risk for branches of the originating institution. Red flags include unusual use of correspondent or other banks within the payment process, or a significant change in banking relationships coinciding with sanctions events.

Trade Based Money laundering

Trade Based Money Laundering

Trade Based Money Laundering (TBML) is a set of techniques used to disguise the nature and details of trade transactions, for a number of purposes, including to facilitate breaches of international sanctions and the movement of value (funds) generated by criminal activity (including sanctions breaches) or to finance such activity. TBML is a set of recognised techniques used by state actors and their criminal associates to facilitate the proliferation of WMD and the trade of commodities which enable the financing of such activity.

Red Flags

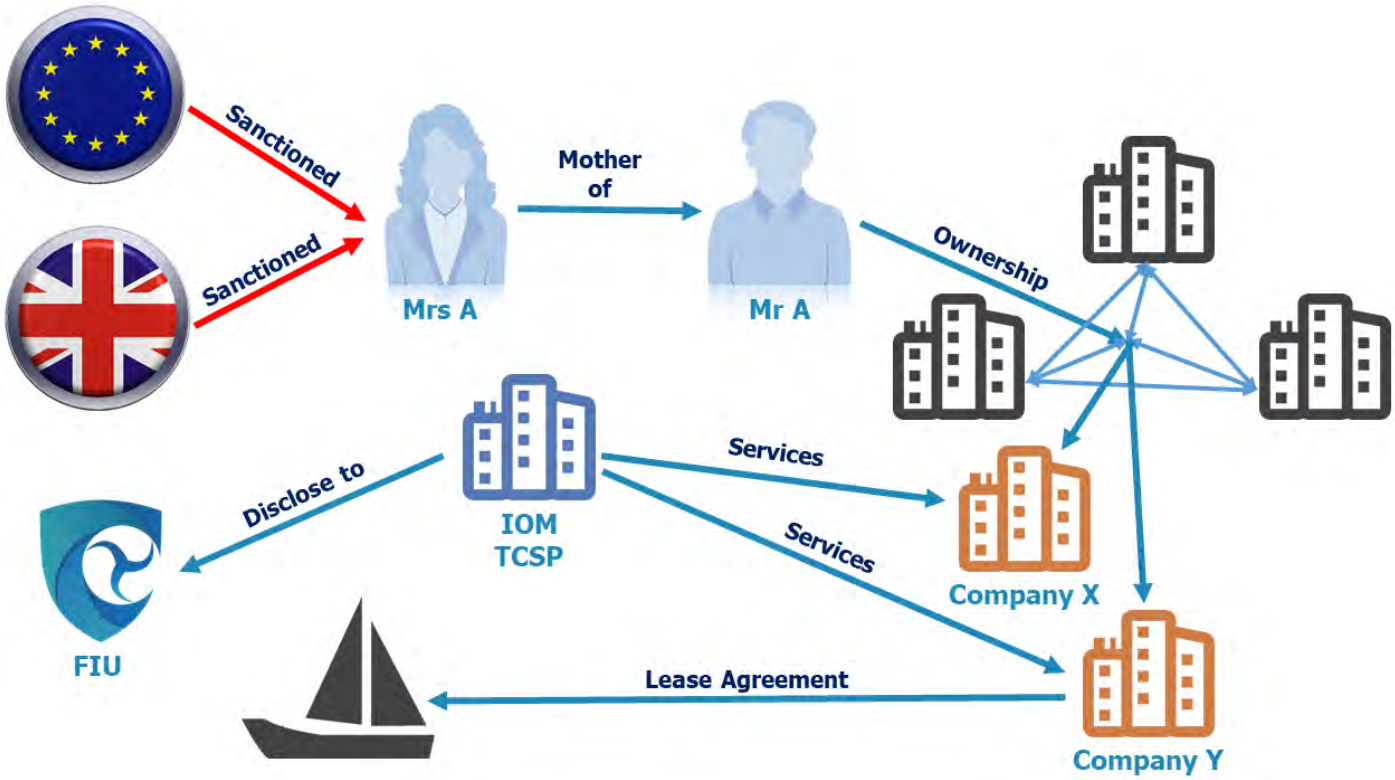
Misrepresentation of transaction details – misrepresenting the price, quality or quantity of goods being bought and sold, transported, imported, exported or otherwise traded

Bogus trading – creation of partly or wholly bogus trading arrangements, or trading patterns, in order to justify the movement of value (funds) from one party to another, often where no goods actually exist, or where no provision of services has taken place

Misrepresentation of trade details – where the ultimate origin, destination or true nature of goods is falsified, in order to facilitate the movement of actual goods, which are listed under international sanctions re-gimes, to sanctioned states, or the purchase of listed goods from sanctioned states

Note: Many of the Sanctions red flag indicators are also used to facilitate TBML

Typology 1



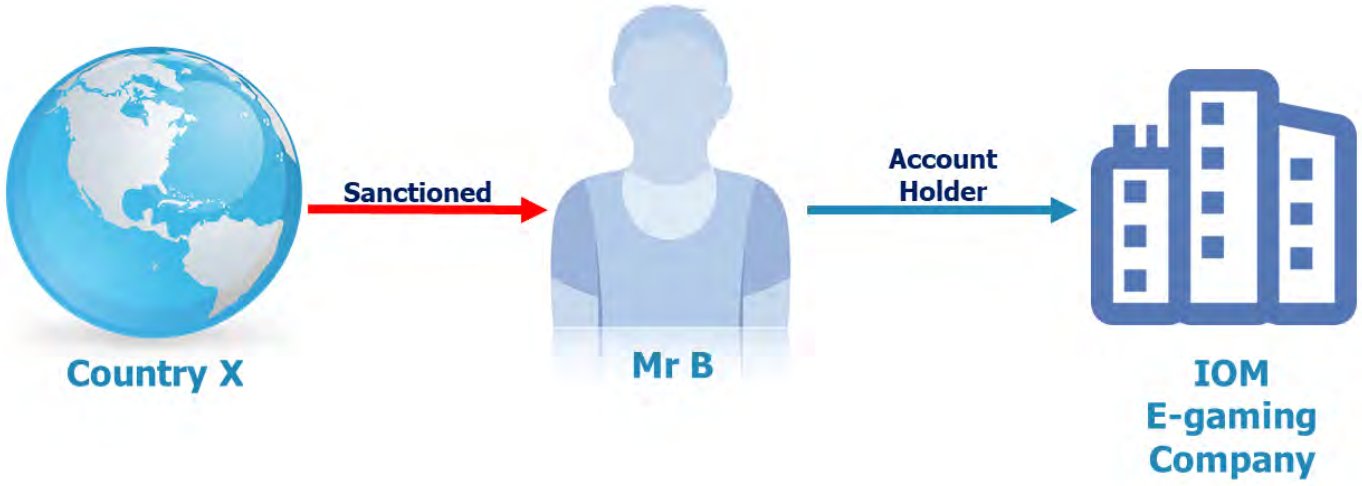
An Isle of Man registered Yacht is owned by Mr A though a complicated company structure. An Isle of Man Trust and Corporate Services Provider (TCSP) provide services to Companies X and Y, both registered in the Isle of Man. Company Y hold the lease agreement for the Yacht.

Mr A is the son of Mrs A, who was designated under EU and UK Sanctions. When the designation was identified, the Yacht was deregistered in the Isle of Man.

It is suspected that the vessel has made multiple journeys after the registration had been removed, which may constitute a possible breach of EU and UK sanctions. The TCSP therefore report the potential breach to the FIU.

In this scenario the TCSP has no operational control over the vessel, therefore would not be seen as responsible for any breach. However, this example highlights the risks associated with arrangements over which a TCSP has limited operational control.

Typology 2



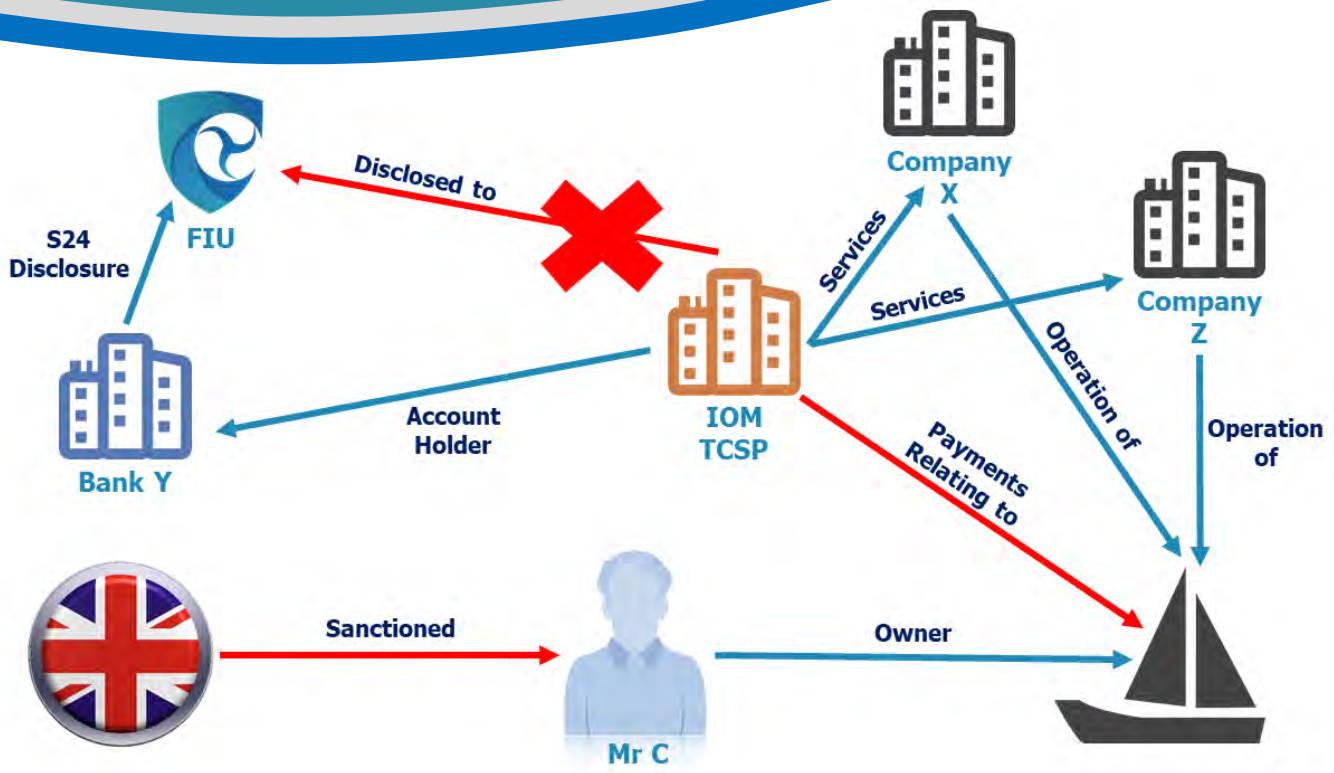
Mr B holds an account with an Isle of Man online gambling institution. The institution is alerted that Mr B had been sanctioned by an international jurisdiction.

The institution conducts searches on Mr B to identify whether he had been sanctioned by any other country. Searches confirm that Mr B is not sanctioned by any other country.

The institution review Mr B's account transactions and no gambling activity has taken place since the sanction implementation, however they still decide to make a report to the FIU under Section 24 of the FIU Act.

Whilst this example is not a sanctions breach, as Mr A was not sanctioned in the UK/IOM, information of this type is still valuable to the FIU as it may be of interest to the relevant international jurisdiction.

Typology 3



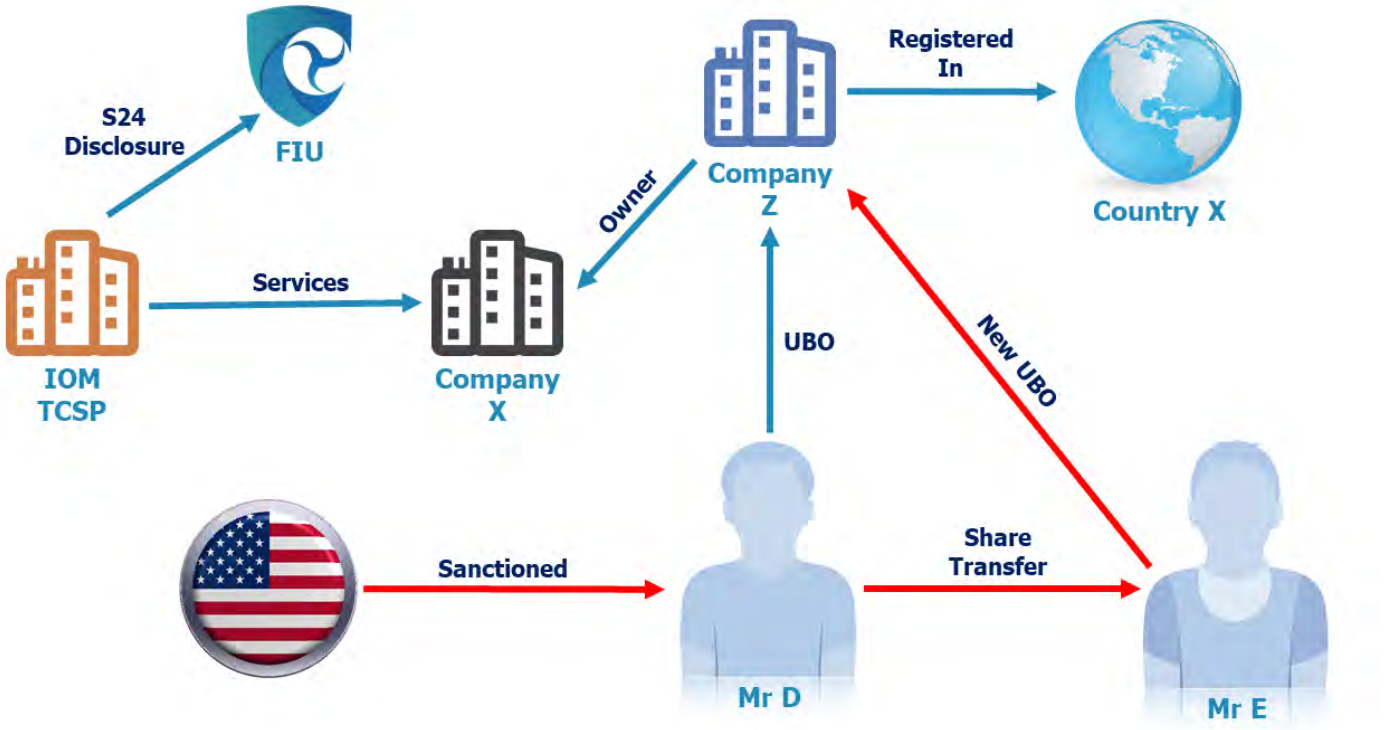
Bank Y identify payments on the accounts of an Isle of Man TCSP that relate to a yacht owned by Mr C, a sanctioned individual. The TCSP provide services to companies X and Z, which are in turn responsible for the operation of the yacht. Bank Y reports the suspected breach to the FIU.

Despite the relationship between the TCSP and the operation of a yacht related to Mr C and the sanctions against Mr C, the TCSP does not make any disclosures to the FIU in relation to the matter.

Should it be identified that the TCSP were aware of the connection to Mr C and the sanctions designations against him, this may constitute a failure to report offence.

This example highlights the importance of regular due diligence checks and timely reporting of suspicions to the FIU.

Typology 4



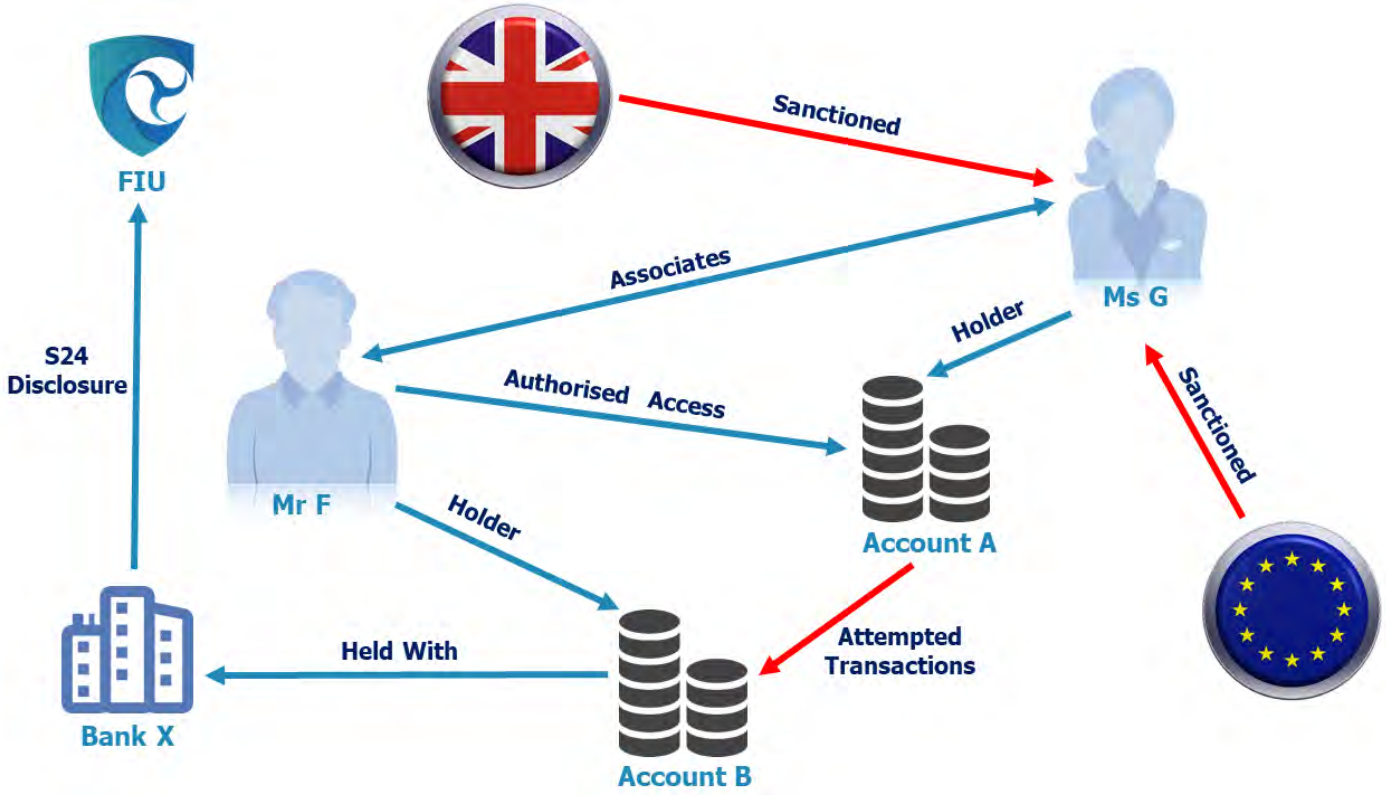
An Isle of Man TCSP provides services to an Isle of Man registered company, Company X. The sole shareholder of the company is Company Z, which is registered internationally. The ultimate beneficial owner of Company Z is Mr D.

Following Mr D becoming subject to a designation under OFAC sanctions, the shares in Company Z are all transferred to a third party, Mr E, which in turn affects the ownership of company X. Despite the changes affecting the Isle of Man company, the transfer occurrs outside of the TCSPs control. As soon as the TCSP become aware of the change in ownership, they make a disclosure to the FIU under Section 24 of the FIU Act.

The transfer of the shares would potentially constitute a breach of OFAC sanctions, however it is hard to determine without a full investigation, where the responsibility for the breach would lie.

This example highlights the complexity of company structures and the difficulty in identifying culpability for breaches in such instances.

Typology 5

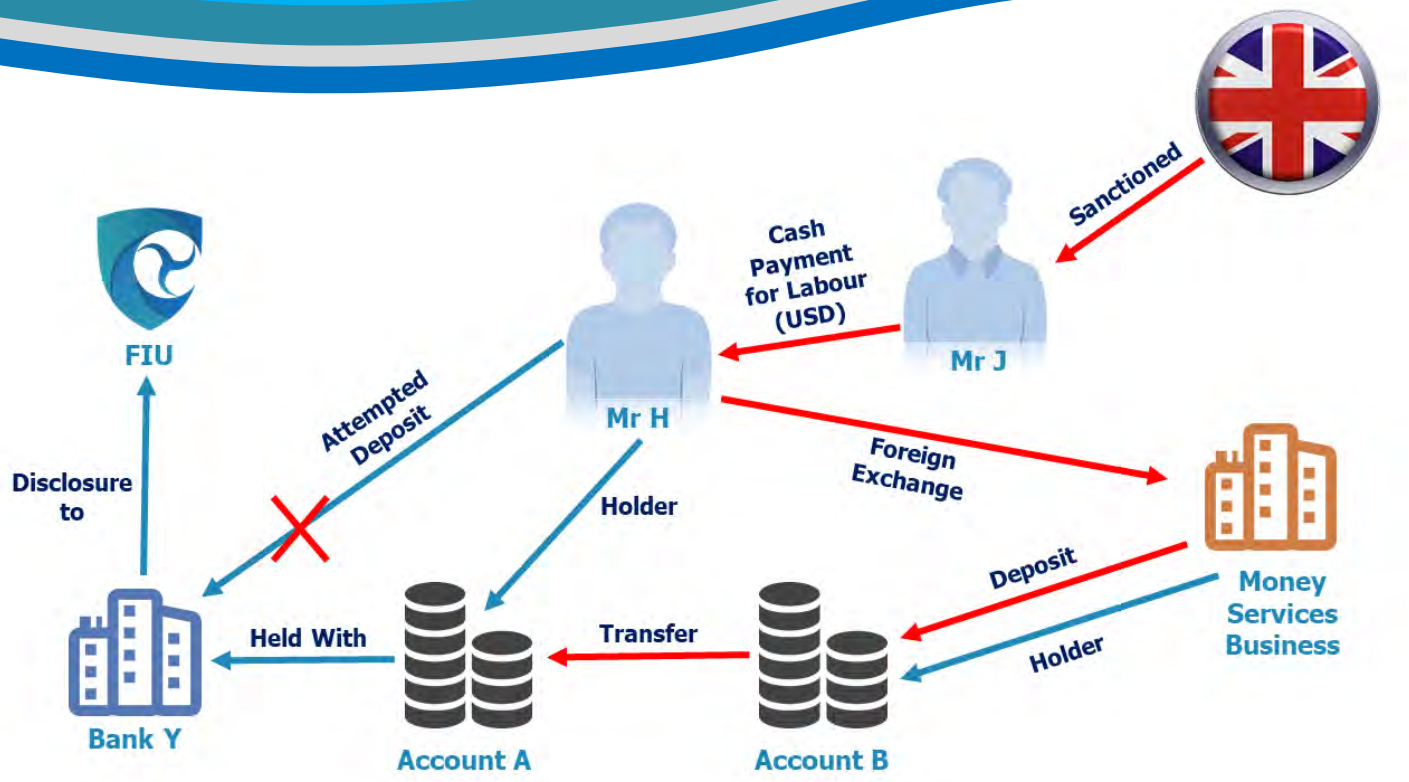


Mr F holds personal bank accounts on the Isle of Man with Bank X. Mr F is an associate of Ms G and has access to her bank accounts.

Following Ms G being designated under EU sanctions, both her and Mr F anticipate that she will also be designated shortly after by the UK. In an attempt to circumvent the incoming UK sanctions, Mr F attempts to transfer funds from the accounts of Mrs G into his personal accounts disguised as gifts. Bank X make a disclosure to the FIU under Section 24 of the FIU Act.

Whilst this example is not a breach, the actions above demonstrate an attempt to circumvent incoming sanctions and this type of information may ultimately help stop sanctioned individuals maintaining access to their funds via a third party.

Typology 6



Mr H is an Isle of Man resident who completed some labouring work for Mr J whilst off island. Mr J was a sanctioned individual and paid for the labour in foreign currency cash.

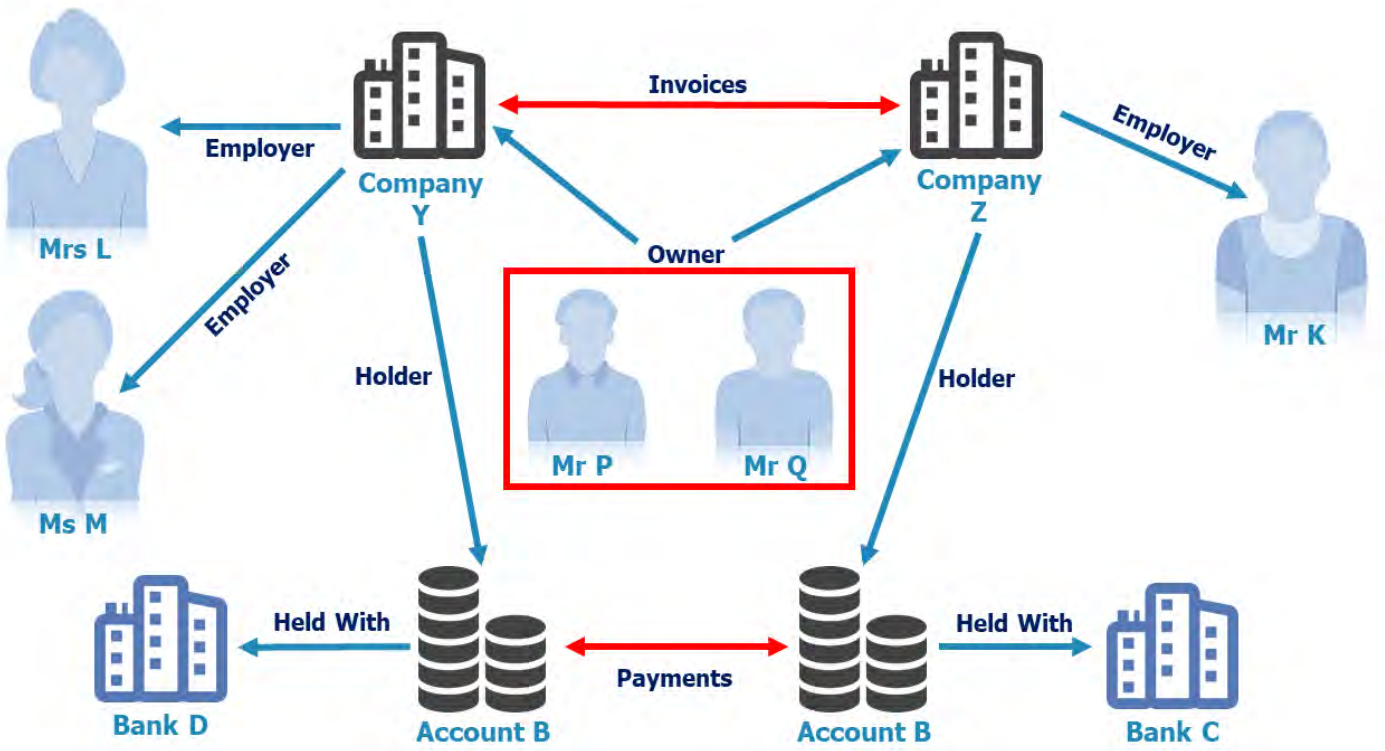
Upon returning to the Isle of Man, Mr H attempts to pay the foreign currency into his personal bank account held with Bank Y. Bank Y refuse the deposit, as the source of the funds (an invoice for the work) highlights the source as a sanctioned individual.

Mr H then takes a portion of the foreign currency to a money services business to exchange it for GBP. The money services business accepts the funds, pays them into their account and then transfers them to the personal account of Mr H with Bank Y. Bank Y then report the potential breach to the FIU, as they are aware of the original source of the funds.

As Mr H knew the origin of the funds, this would be considered a potential sanctions breach.

This example highlights the importance of questioning the source of funds when accepting cash deposits and foreign exchanges.

Typology 7



Mr K, Mrs L and Ms M all work for Companies Y and Z, which are both registered on the Isle of Man and hold Isle of Man bank accounts. The beneficial owners of both companies are Mr P and Mr Q, who manage the operations of the companies. Whilst employed at the companies Mr K, Mrs L and Ms M all become concerned that multiple inter-company invoices are being raised for services, which are not being supplied. When they express their concerns to Mr P and Mr Q, they dismiss them as nothing to worry about. This further makes them suspect that the companies are being used as a vehicle by which to launder funds.

This is an example of how trade based money laundering may present within the financial system.