Fraud by False Representation

The Isle of Man Financial Intelligence Unit (FIU) is producing monthly typologies as part of its strategic objective to improve the regulated sectors understanding of various financial crime risks. Typologies produced by the FIU support the Island's international obligations under FATF recommendation 29, which requires Financial Intelligence Units to develop and disseminate information that helps identify and assess threats related to money laundering (ML) and associated predicate offences.

The typologies and indicators presented here are based on:

⇒ Analysis of suspicious activity reports (SARs) received by the FIU,

⇒ Open-source intelligence (OSINT).

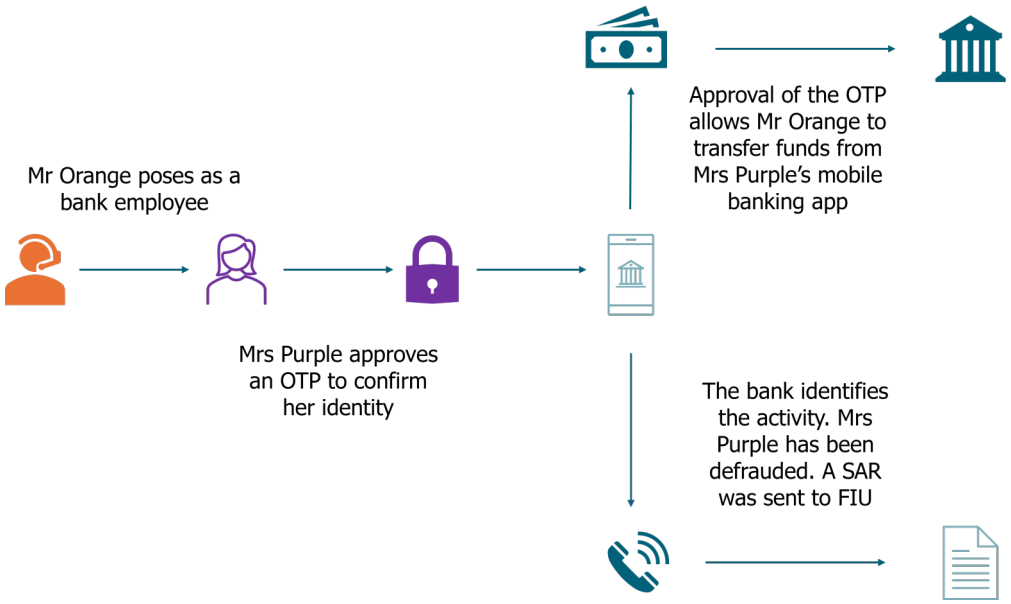
The below example is fictional and particularly relevant to professionals working in the banking sector.

Blue Bank received an internal notification that an unusually large payment of GBP 25,000.00 had been paid to a third party by Mrs Purple using her banking app. Blue Bank called Mrs Purple and established she had no knowledge of this payment.

Mrs Purple stated she had been contacted by Mr Orange, who stated he worked for Blue Bank. Mr Orange called Mrs Purple stating the bank wished to check she had made a number of recent payments. Mrs Purple stated Mr Orange asked her to approve a One Time Passcode (OTP) that was sent to her mobile device, to confirm her identity before proceeding. Mrs Purple stated Mr Orange had details of previous transactions she had made.

Blue Bank suspected Mrs Purple's banking app had been compromised. They surmised Mr Orange had committed fraud by false representation by posing as a bank employee in order to get Mrs Purple to approve an OTP code. Mr Orange was then able to send a large payment and defraud Mrs Purple. Blue Bank identified that recent login IP information for Mrs Purple's banking application showed logins from another jurisdiction, which matched the sort code for the bank account, where the funds were sent.

A SAR was submitted to the FIU.



Red Flags

- An unusually large payment or series of payments is made, which does not match the customers usual activity
- The device ID for online/ banking applications or IP location for the customer suddenly changes without explanation
- Out of character payments are made for goods/services in a country where the customer is not located / has no links

February 2026

Bribery and Corruption

The Isle of Man Financial Intelligence Unit (FIU) is producing monthly typologies as part of its strategic objective to improve the regulated sectors understanding of various financial crime risks. Typologies produced by the FIU support the Island's international obligations under FATF recommendation 29, which requires Financial Intelligence Units to develop and disseminate information that helps identify and assess threats related to money laundering (ML) and associated predicate offences.

The typologies and indicators presented here are based on:

⇒ Analysis of suspicious activity reports (SARs) received by the FIU,

⇒ Open-source intelligence (OSINT).

The below example is fictional and particularly relevant to professionals working in the TCSP sector.

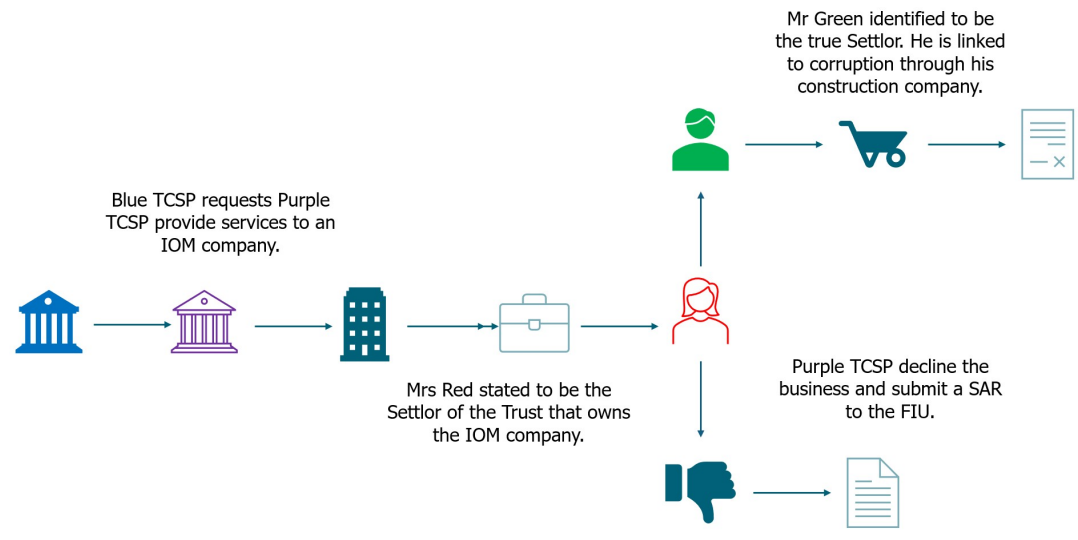
Purple TCSP is an Isle of Man based Trust and Corporate Service Provider. Purple TCSP were approached by Blue TCSP, located in another jurisdiction. Purple TCSP were asked to provide administrative services to an Isle of Man company, that owns a UK property. This company was previously administered by another Isle of Man TCSP. Blue TCSP were evasive when asked to confirm the reason services were terminated, stating it was due to a fee dispute when pressed.

The company is ultimately owned through a Trust in another jurisdiction. Purple TCSP requested that Blue TCSP provide due diligence for the ownership structure.

Mrs Red was initially stated by Blue TCSP to be the Settlor of the Trust. Purple TCSP identified from the documentation provided that the Trust was settled using an interest free loan provided by her father Mr Green. Blue TCSP were evasive when asked to provide detailed source of wealth documentation for Mr Green.

Purple TCSP conducted OSINT on Mr Green and identified that he is the owner of a construction contracting company in another jurisdiction that is undertaking work for a large government contract. Mr Green was identified to be a commercially exposed person (CEP). Further OSINT showed this contract was awarded directly by a politician linked heavily to international corruption offences. Social media accounts identified that Mr Green was associated with this politician outside of a commercial environment.

Purple TCSP declined the business. Purple TCSP suspected Mr Green may have bribed a foreign politician to acquire a lucrative government contract for his company. Purple TCSP further suspected the assets of the Trust had been purchased or tainted with the proceeds of corruption. Purple TCSP submitted a Suspicious Activity Report to the FIU.



Red Flags

- Evasion when asked for the reasons services were terminated by another TCSP.
- Attempting to conceal or failure to provide SOF/SOW documentation.
- Presence of a CEP within ownership structure.
- Adverse media linking Settlor to an individual associated with corruption.

March 2026

Use of Synthetic Accounts

The Isle of Man Financial Intelligence Unit (FIU) is producing monthly typologies as part of its strategic objective to improve the regulated sectors understanding of various financial crime risks. Typologies produced by the FIU support the Island's international obligations under FATF recommendation 29, which requires Financial Intelligence Units to develop and disseminate information that helps identify and assess threats related to money laundering (ML) and associated predicate offences.

The typologies and indicators presented here are based on:

⇒ Analysis of suspicious activity reports (SARs) received by the FIU,

⇒ Open-source intelligence (OSINT).

The below example is fictional and particularly relevant to professionals working in the Life Insurance Sector.

An Isle of Man life insurance company (the "Life Company") received an application to open a Portfolio Bond (a life insurance wrapper) to be held by two joint policyholders, Mr. and Mrs. Burgundy, purported residents of Jurisdiction X, introduced via an Independent Financial Adviser (IFA).

The IFA submitted customer due diligence documentation (CDD), including certified passports, proof of address, source of funds and origin of wealth information, which initially appeared satisfactory. The initial premium was received from a bank account held in Mr & Mrs Burgundy's name in Jurisdiction X and the portfolio bond was issued.

Within two years of the account being opened, the Life Company received a request to fully surrender the portfolio bond, well before the policy's maturity date. This early surrender would trigger substantial charges and result in a loss against the original premium. Despite being informed of the financial impact, Mr. and Mrs. Burgundy were dismissive of the consequences and remained intent on proceeding.

The client's behaviour and early surrender raised a red flag to the Life Company, prompting a full review of their client's policy.

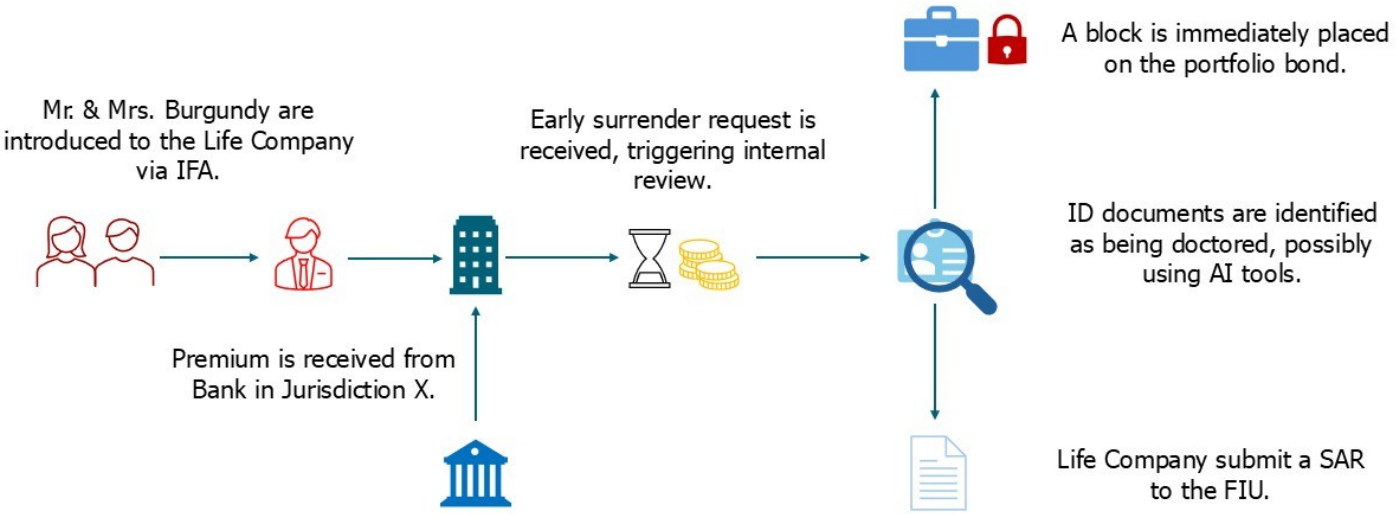
During their review, the company performed re-verification checks for Mr Burgundy's CDD documentation, which identified subtle anomalies within the identity document.

These included inconsistencies in font and format, alongside indicators of digital manipulation inconsistent with genuine documents. A review of other documents identified similar discrepancies, suggesting a coordinated pattern, with images showing characteristics consistent with AI-generated or altered content.

Attempts to independently verify the applicants were unsuccessful. The individuals could not be corroborated through reliable sources and had minimal digital footprint.

The combination of plausible personal data with manipulated identity elements indicated the likely construction of false identities designed to bypass due diligence controls.

The Life Company developed a suspicion that the portfolio bond had been used to establish a synthetic account using falsified documentation to obscure their true identities and facilitate the laundering of criminal proceeds. As a result, an immediate block was placed on the policy and a Suspicious Activity Report (SAR) was submitted to the Isle of Man Financial Intelligence Unit.



Red Flags

- Early Surrender of a long-term investment product, incurring significant charges.
- Dismissive behaviour of customer when informed of potential losses.
- Subtle inconsistencies in identity documents, including font, spacing and alignment anomalies
- Evidence of digital manipulation within passport photographs (e.g. blending, distortion)
- Images displaying characteristics consistent with AI-generated or synthetically altered faces
- Similar document discrepancies identified across multiple related parties (pattern rather than isolated issue)
- Inability to independently verify individuals through reliable public or proprietary data sources
- Lack of credible digital, financial, or public footprint for the applicants
- Combination of plausible personal data (e.g. real addresses) with fabricated or manipulated identity elements
- Use of advanced technologies (e.g. generative AI) to enhance the realism of fraudulent documents

April 2026

Sanctions Evasion

The Isle of Man Financial Intelligence Unit (FIU) is producing monthly typologies as part of its strategic objective to improve the regulated sectors understanding of various financial crime risks. Typologies produced by the FIU support the Island's international obligations under FATF recommendation 29, which requires Financial Intelligence Units to develop and disseminate information that helps identify and assess threats related to money laundering (ML) and associated predicate offences.

The typologies and indicators presented here are based on:

⇒ Analysis of suspicious activity reports (SARs) received by the FIU,

⇒ Open-source intelligence (OSINT).

The below example is fictional and particularly relevant to professionals working in the Legal Sector.

Orange Law Firm, an Isle of Man law firm qualified to undertake conveyancing in a neighbouring jurisdiction (Jurisdiction A), was approached by Black Company, an Isle of Man-registered entity, in relation to the acquisition of a large, high-value residential property in Jurisdiction A.

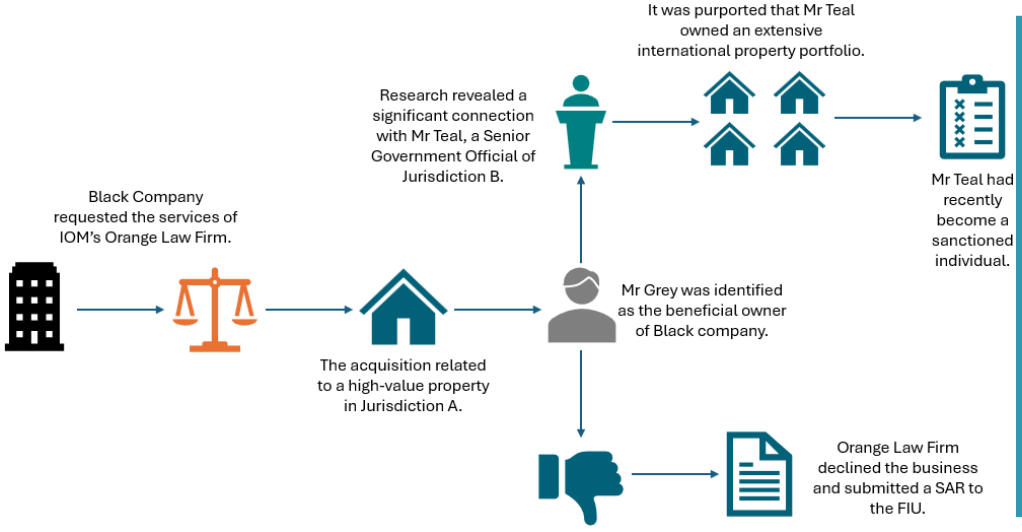
Company documentation provided by Black Company identified Mr Grey as the beneficial owner. Mr Grey was a national of Jurisdiction B, a region marked as high risk for money laundering and terrorist financing. Mr Grey's reason for the property purchase was to provide accommodation for the several days he spends working in Jurisdiction A per year.

Prior to accepting the instruction, Orange Law Firm conducted open-source research on Mr Grey. Searches of Jurisdiction A's property register revealed that Mr Grey had recently acquired several residential properties, through multiple companies, in close proximity to the proposed purchase. It became clear that Mr Grey's known and verifiable income was not commensurate with the acquisition of the properties in Jurisdiction A.

Further media checks uncovered articles describing Mr Grey as a trusted associate of an individual called Mr Teal. Orange Law Firm established that Mr Teal was a Senior Government Official of Jurisdiction B, who had recently been sanctioned over national security concerns. It was purported that Mr Teal holds an extensive international property portfolio.

Further investigation by Orange Law Firm confirmed that Mr Grey and Mr Teal shared the directorship of a company in Jurisdiction B, indicating a close business relationship.

Upon discovering this information, Orange Law Firm declined the business. Orange Law Firm suspected that Mr Grey was a professional enabler, attempting to acquire the property on Mr Teal's behalf and bypassing the sanctions against him. Orange Law Firm submitted a Suspicious Activity Report to the FIU.



Red Flags

- The type of property does not match the intended purpose proposed.
- Beneficial owner is a national of a high-risk jurisdiction with media linking them to a sanctioned individual.
- Use of multiple corporate vehicles to hold property may indicate concealment of true ownership.
- The purchase was disproportional to the known and verifiable income.

Isle of Man
Financial Intelligence Unit
Ellan Vannin Unnid Tushtag Argidoil

May 2026

Cyber-enabled Fraud and TF

The Isle of Man Financial Intelligence Unit (FIU) is producing monthly typologies as part of its strategic objective to improve the regulated sectors understanding of various financial crime risks. Typologies produced by the FIU support the Island's international obligations under FATF recommendation 29, which requires Financial Intelligence Units to develop and disseminate information that helps identify and assess threats related to money laundering (ML) and associated predicate offences.

The typologies and indicators presented here are based on:

⇒ Analysis of suspicious activity reports (SARs) received by the FIU,

⇒ Open-source intelligence (OSINT).

The below example is fictional and particularly relevant to professionals working in the banking sector.

Yellow Bank identified that an account held by Mr Green had received numerous low-value payments from unrelated individuals. Payment references related to mobile phones and other goods. Mr Green was employed in construction and the activity did not match the expected use of his personal account.

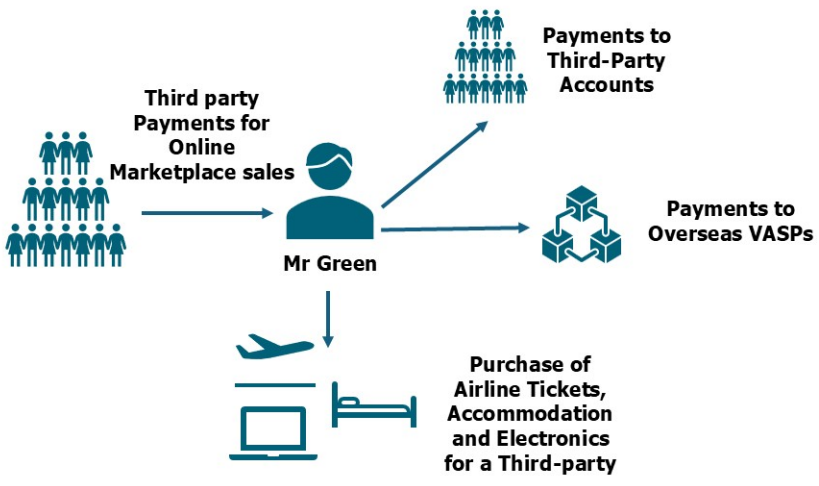
Mr Green stated that he had recently started selling goods through online marketplaces and provided screenshots of customer orders. Yellow Bank initially considered the activity indicative of an undeclared online business.

Yellow Bank subsequently received notifications that several payments had been reported as fraudulent. Customers had purchased goods advertised through different seller profiles, but the goods were never delivered. Mr Green's screenshots contained different seller names, repeated product photographs and inconsistent order information. The seller contact details could not be independently verified.

Funds were rapidly dispersed to third-party accounts and an overseas Virtual Asset Service Provider (VASP). Further review identified payments for airline tickets, accommodation and electronic equipment. Open-source intelligence linked one recipient of the transferred funds, Mr Orange, to online content supporting a terrorist organisation. He had recently travelled to a high-risk jurisdiction neighbouring an area of conflict.

Individually, the payments appeared consistent with ordinary online marketplace fraud. However, the multiple seller profiles, rapid movement of funds, transfers to Mr Orange and adverse information presented a wider pattern of concern.

Yellow Bank suspected Mr Green had used online marketplaces to commit cyber-enabled fraud and further suspected that some of the proceeds had been used to fund the travel and living costs of an individual associated with terrorism. A Suspicious Activity Report was submitted to the FIU under ATCA.



Red Flags

- Multiple low-value payments are received from unrelated individuals,.
- Multiple seller profiles use repeated product photographs, inconsistent information or contact details that cannot be independently verified.
- Funds are rapidly transferred to third-party accounts or overseas VASPs shortly after receipt.
- Payments for travel and accommodation suspected to be to a high-risk country neighbouring an area of conflict.

June 2026

Fraud / Theft and TF

The Isle of Man Financial Intelligence Unit (FIU) is producing monthly typologies as part of its strategic objective to improve the regulated sectors understanding of various financial crime risks. Typologies produced by the FIU support the Island's international obligations under FATF recommendation 29, which requires Financial Intelligence Units to develop and disseminate information that helps identify and assess threats related to money laundering (ML) and associated predicate offences.

The typologies and indicators presented here are based on:

⇒ Analysis of suspicious activity reports (SARs) received by the FIU,

⇒ Open-source intelligence (OSINT).

The below example is fictional and particularly relevant to professionals working in the banking/lending sectors.

Blue Bank received an application from Mr Lilac for a GBP 20,000 loan for a car. He stated that he was employed as a manager and provided payslips supporting the application. The loan was approved and credited into his current account.

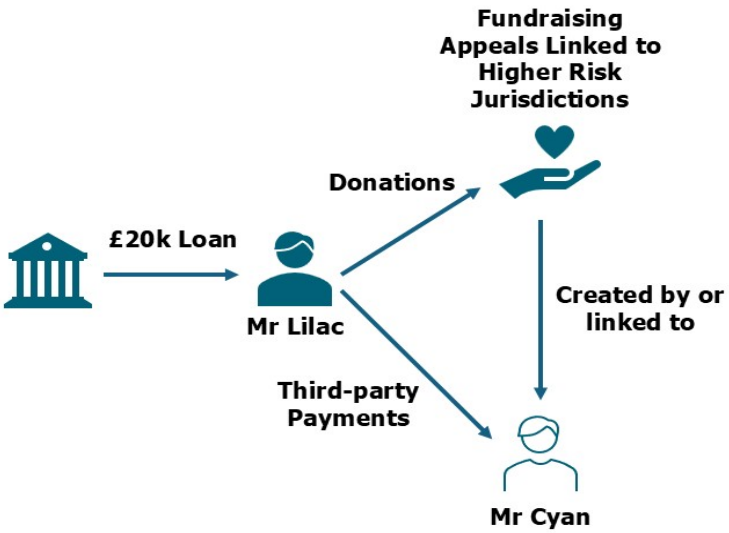
Within several weeks, most of the loan had been divided into smaller payments and transferred to a third party, Mr Cyan, and several fundraising appeals. The appeals purported to provide humanitarian assistance in an area of conflict. Mr Lilac failed to make the first repayment.

The unusual activity prompted Blue Bank to conduct Enhanced Due Diligence. The bank requested updated information regarding Mr Lilac's employment, source of funds and the purpose of the transactions. The information provided was inconsistent with the account activity, and the supporting documentation contained anomalies.

Further review identified that Mr Cyan had created or promoted the fundraising appeals. Although the appeals used different names, they contained common contact and beneficiary information. Open-source research linked one overseas beneficiary to a charity whose members had reportedly provided financial support to a terrorist organisation.

Taken in isolation, the false loan application and non-payment appeared to be an isolated act of fraud by misrepresentation, however, the structured payments, connection between the appeals and adverse information concerning the overseas beneficiary presented a wider pattern of concern.

Blue Bank suspected Mr Lilac had fraudulently obtained credit, transferred the proceeds through fundraising appeals controlled by Mr Cyan and further suspected that some of the funds may have been made available to support a terrorist organisation. A Suspicious Activity Report was submitted to the FIU under ATCA.



Red Flags

- The customer's declared income is inconsistent with account activity or information obtained from their employer.
- Loan funds are rapidly divided into smaller payments and transferred to third parties or online fundraising appeals.
- The customer defaults shortly after receiving the loan and shows no apparent intention or ability to repay.
- Different fundraising appeals contain common contact or beneficiary details and are connected to persons or organisations linked to terrorism or higher risk jurisdiction.

July 2026

Virtual Assets Source of Funds and Source of Wealth

The Isle of Man Financial Intelligence Unit (FIU) is producing monthly typologies as part of its strategic objective to improve the regulated sectors understanding of various financial crime risks. Typologies produced by the FIU support the Island's international obligations under FATF recommendation 29, which requires Financial Intelligence Units to develop and disseminate information that helps identify and assess threats related to money laundering (ML) and associated predicate offences.

The typologies and indicators presented here are based on:

⇒ Analysis of suspicious activity reports (SARs) received by the FIU,

⇒ Open-source intelligence (OSINT).

The below example is fictional and relevant to professionals working in any sector that deals with virtual assets.

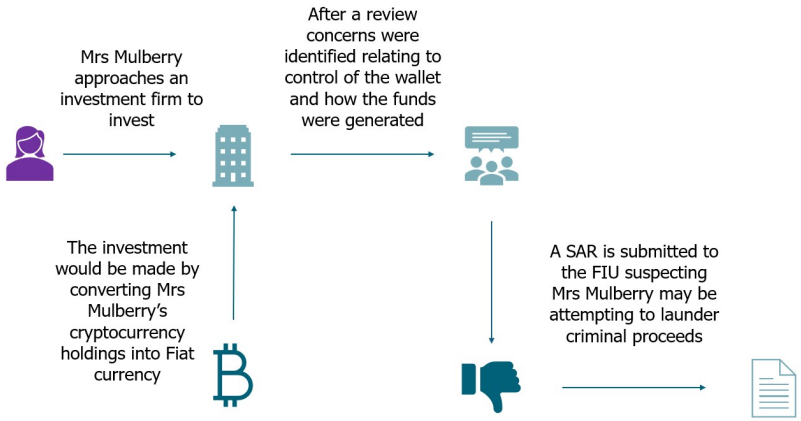
Mrs Mulberry approached an investment management firm seeking to make a large investment into their discretionary portfolio service. Mrs Mulberry stated that her funds were held in a self-hosted cryptocurrency wallet which would be converted into fiat before investment and informed that her wealth had been generated as an early investor in Bitcoin during the retail investor boom in 2017.

To verify that Mrs Mulberry controlled the wallet the investment firm requested the public address details to confirm the balance of the wallet and asked Mrs Mulberry to perform a Satoshi Test. She was asked to return a small, exact amount of cryptocurrency sent to the address by the investment firm within a specific time frame. Mrs Mulberry was able to do this, although only shortly before the deadline.

To verify Mrs Mulberry's Source of Funds and Source of Wealth, the investment firm requested transaction logs to evidence the purchase of Bitcoin and subsequent trading gains. Mrs Mulberry became evasive when asked to provide this information.

Using a cryptocurrency tracing tool the investment firm reviewed transaction history available on the public blockchain ledger. They ascertained that minimal, small value Bitcoin trading had occurred, but the address had received a large number of credits in the past six months from other addresses. These addresses had interacted with cryptocurrency mixers. Mrs Mulberry did not respond when asked to clarify the source of these credits and the investment did not go ahead.

The predicate offence was unclear, but the activity and behaviour of Mrs Mulberry caused the investment firm to become suspicious that she was attempting to launder the proceeds of crime held in a cryptocurrency wallet which may or may not be under her control. A suspicious activity report was submitted to the FIU by the investment management firm.



Red Flags

- Large delay completing the Satoshi Test highlighting the individual may not control the address.
- Stated generation of wealth on the blockchain did not match publicly available transactional activity.
- Use of cryptocurrency mixers obscuring the source of the cryptocurrency.

Isle of Man
Financial Intelligence Unit
Ellan Vannin Unnid Tushtag Argidoil