Terrorist Financing Typologies and Red Flags

May 2026

Isle of Man
Financial Intelligence Unit
Ellan Vannin Unnid Tushtag Argidoil

Contents

Introduction

The Isle of Man's status as an international finance centre (IFC), combined with a diverse and sophisticated financial services sector, brings both economic opportunity and inherent risk. While the jurisdiction has not identified a significant domestic terrorism threat, the international nature of its financial system means it may be exploited by those seeking to finance terrorism abroad.

The Isle of Man National Risk Assessment (NRA) identifies terrorist financing (TF) risks in several sectors, notably: Abuse of Non-Profit Organisations (NPOs), Misuse of Trust and Corporate Service Providers (TCSPs), Vulnerabilities in online gambling/e-gaming, Transactions with high-risk jurisdictions, Sanctions evasion and the Use of virtual assets and professional services to obscure beneficial ownership.

This report consolidates intelligence, open-source information and adapted international case studies into typologies relevant to the Isle of Man. Whilst some of the typologies detailed are based on these three areas, some are fictitious to illustrate how TF could manifest across different Isle of Man regulated sectors, including banking, TCSPs, life assurance, online gambling, virtual assets, real estate and legal/accounting services.

The typologies are intended to help industry identify and report suspicious activity to the Financial Intelligence Unit (FIU) in line with the Island's AML/CFT obligations. Red Flags and Linked Risk Areas accompany each example, referencing both IOM NRA priority risks and FATF Emerging Terrorist Financing Risks.

The IOM FIU produces typology reports in accordance with FATF Recommendation 29 to identify and raise awareness of emerging and priority financial crime threats, including terrorist financing. This report builds on the findings of the Isle of Man National Risk Assessment – Terrorist Financing (2025) and the FATF Emerging Terrorist Financing Risks report.

Whilst there have been no confirmed large-scale terrorist financing cases in the Isle of Man, the FIU recognises that even small or indirect transactions may form part of an international TF network. The purpose of this typologies document is to highlight potential indicators, sector vulnerabilities and practical examples relevant to the Isle of Man's regulated sectors.

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

The Isle of Man's Risk Context?

The Isle of Man's NRA concludes that the jurisdiction's risk from a direct terrorist event is very low. There is no evidence of an active domestic terrorism threat and the Island's geographic position, population size and security environment mean that it is unlikely to be the location of a planned or executed terrorist attack.

However, the NRA identifies that the primary terrorist financing risk to the Isle of Man arises not from domestic activity, but from its role as an IFC. The Island's well-developed and globally connected financial services sector facilitates legitimate cross-border financial activity but also presents an opportunity for misuse by those seeking to move funds internationally for terrorist financing purposes.

As an IFC, the Isle of Man routinely handles inward and outward flows of significant value, involving multiple jurisdictions and a variety of regulated sectors, including banking, TCSPs, life assurance companies, online gambling operators and virtual asset service providers (VASPs). This creates exposure to:

- Transit of funds linked to high-risk jurisdictions.
- Layering and integration through legitimate business activity and investment.
- Sanctions evasion via complex ownership structures or third-country routing.

The NRA emphasises that even when there is no direct link to domestic terrorist activity, the movement of funds through the Isle of Man's financial system can form part of a wider international terrorist financing network. As such, vigilance is required across all sectors to detect and disrupt transactions that may be intended to support terrorism overseas.

Background: Understanding Terrorist Financing

Terrorist financing refers to the provision or collection of funds, by any means, directly or indirectly, with the intention or knowledge that they will be used to fund terrorist acts or by a terrorist organisation. Unlike money laundering, TF funds may originate from both illicit and legitimate sources.

TF activities generally follow a six-stage process:

1. Raising funds – through donations (including NPO abuse), criminal activity (smuggling, drug trafficking, fraud, counterfeit goods), business operations, or online crowdfunding.

2. Moving funds – via bank transfers, money service businesses, trade-based transactions, virtual assets, cash couriers, informal value transfer systems (ie Hawala), or through the misuse of regulated sectors.

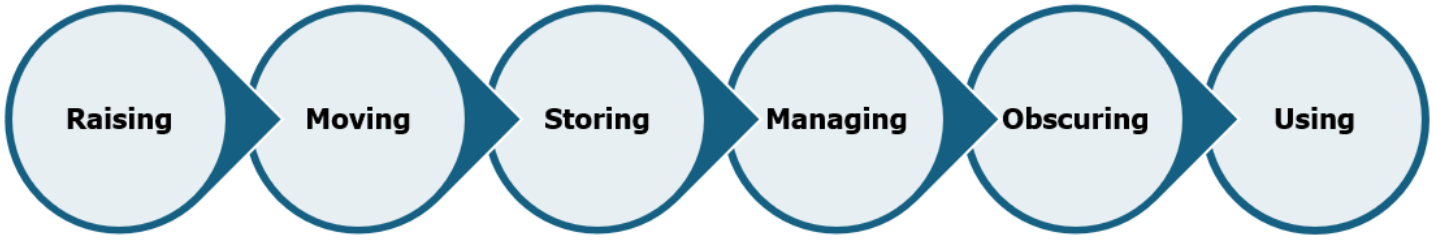
3. Storing funds – holding funds for a period of time prior to their transfer or use. Funds may be stored in personal or business bank accounts, businesses, charities, VASP-hosted Wallets, or in cash holdings controlled by individuals or facilitators.

4. Managing funds – administering, controlling, or allocating funds within a terrorist network or support structure. This may include coordinating financial support for operatives and their dependants, organising the distribution of funds across different activities, or maintaining financial oversight of resources held by facilitators or front organisations.

5. Obscuring funds – disguising the origin, destination, or purpose of funds in order to evade detection. This may involve the use of intermediaries, front companies, multiple accounts, informal value transfer systems, trade-based mechanisms, or emerging financial technologies.

6. Using funds – for operational expenses, recruitment, propaganda, weapons procurement, or supporting dependants of members.

Common global typologies include: Abuse of charities and humanitarian aid organisations; Trade-Based Money Laundering (TBML); Shell companies and complex ownership structures, Sanctions evasion using third countries or false documentation; Misuse of professional services; Virtual asset transactions and peer-to-peer exchanges; Cash smuggling and informal value transfer systems.



1. https://www.iomfsa.im/media/3259/ft-fact-sheet.pdf

Emerging TF Methods & Risks

Emerging TF Methods & Risks

Based on the IOM NRA and FATF Emerging Terrorist Financing Risks, the following are considered the most relevant emerging threats to the Isle of Man:

- Structuring smaller transactions to avoid detection.
- Exploitation of online platforms (gambling, crowdfunding, social media) to move or raise funds.
- Misuse of virtual assets, including privacy coins, mixers and decentralised exchanges.
- Use of lower risk jurisdictions adjoining high risk jurisdictions to disguise the true destination of funds.
- Multi-layered ownership structures to obscure true beneficial ownership.
- Cash courier activity between the Isle of Man and UK/EU, exploiting ferry and air links.
- Property and business acquisitions as a means of integrating TF funds.

Methodology

The typologies in this report are drawn from:
- Suspicious Activity Reports (SARs) received by the FIU.
- Open-source intelligence and adverse media.
- Adaptations of relevant international case studies, tailored to the Isle of Man's sectors.
- FATF and other FIU publications highlighting emerging TF methodologies.
- Consultation with industry stakeholders, regulators and law enforcement.

UK/IOM Proscribed Organisations and TF Sanctions

Under the Terrorism Act 2000, the UK Government may proscribe organisations that are concerned in terrorism. Proscription makes it a criminal offence to belong to, invite support for, arrange meetings for, or display support for a listed organisation. The official and most up-to-date list of proscribed terrorist organisations is maintained by the Home Office and is available at:

https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2

This list should be incorporated into customer and counterparty screening processes, including checks against known aliases and alternative spellings.

Terrorist financing sanctions operate alongside proscription and impose asset freezes and prohibitions on making funds or economic resources available to designated persons. In the UK, these measures are implemented under the Terrorist Asset-Freezing etc. Act 2010 and the Sanctions and Anti-Money Laundering Act 2018, giving effect to both UN-mandated and UK autonomous regimes.

The authoritative and consolidated source for financial sanctions designations is the UK Sanctions List, available at:

https://www.gov.uk/government/publications/the-uk-sanctions-list

This list includes individuals and entities subject to asset freezes and other financial restrictions. Regulated firms are required to screen customers, beneficial owners and transactions against this list, freeze assets without delay where a match is confirmed and report to the Office of Financial Sanctions Implementation (OFSI) where required.

Together, the UK proscribed organisations list and the UK Sanctions List form core reference points for counter-terrorist financing compliance and should be embedded within wider AML/CFT controls, including enhanced due diligence and transaction monitoring.

https://www.fiu.im/sanctions/

Regulated entities in the Isle of Man are also required to report known or suspected breaches of financial sanctions to the IOM FIU without delay. The primary mechanism for submitting sanctions-related disclosures is via the FIU's online reporting system, THEMIS. Entities registered on THEMIS should submit reports using the "Sanctions" option within the relevant legislation dropdown menu.

Where a matter involves individuals or entities designated under the Office of Foreign Assets Control (OFAC) sanctions regime, disclosures should be made using the Section 24 reporting option within THEMIS. For those not registered on THEMIS, please contact the FIU via email at fiu@gov.im in the first instance, or via telephone on 01624 686000.

Extreme Right Wing Terrorism / Right Wing Extremism

The UK Government has described the above criminality type as: "those involved in Extreme Right-Wing activity who use violence in furtherance of their ideology. These ideologies can be broadly characterised as Cultural Nationalism, White Nationalism and White Supremacism. Individuals and groups may subscribe to ideological tenets and ideas from more than one category." https://www.gov.uk/government/publications/prevent-duty-guidance/glossary-of-terms

Categories of Symbols Used in Right-Wing Extremism

Right-wing extremist (RWE) movements rely heavily on symbolism to communicate ideology, reinforce identity and signal affiliation. These symbols range from overt historic extremist insignia to more ambiguous cultural or digital imagery that has been repurposed for ideological use. While their meanings vary in clarity, they can broadly be grouped into six categories.

Historic extremist symbols

These include insignia directly associated with 20th-century fascist and National Socialist movements, such as the swastika and SS insignia. Although some of these symbols have ancient origins, their modern political use in Western contexts is overwhelmingly linked to neo-Nazism and white supremacism. In political, organisational, or fundraising contexts, they are generally high-confidence indicators of extremist alignment.

Adapted religious or cultural symbols

Includes imagery such as stylised Celtic crosses or sun wheel motifs. These symbols may have legitimate Christian, pagan, or heritage meanings, but have also been adopted by white supremacist movements. Interpretation requires contextual assessment, particularly where such symbols are displayed alongside supremacist rhetoric or coded messaging.

Numeric codes and alphanumeric shorthand

These are frequently used to communicate ideology covertly. Examples include:

"14" (referencing the "Fourteen Words" slogan)

"88" (representing "HH" or "Heil Hitler")

"1488" (a combination of both)

These codes may appear in usernames, tattoos, merchandise branding, company names, cryptocurrency wallets, or payment references. Numbers alone are not determinative, but repetition and contextual alignment may elevate concern.

Runes and esoteric symbols

These are derived from ancient Germanic alphabets and mythological traditions. Certain runes and the "Black Sun" (Sonnenrad) have been appropriated within extremist circles to evoke ideas of ancestry, racial identity, or "blood and soil" ideology. As these symbols also exist in legitimate historical and cultural contexts, proportional analysis is essential.

Digital-native and meme-based symbolism

These have played an increasingly significant role in contemporary extremist ecosystems. Online memes, coded humour, stylised graphics and tagging conventions serve recruitment and normalisation functions, particularly among younger audiences. These symbols often evolve rapidly and may be deliberately ambiguous to provide plausible deniability.

Physical markers

Gestures, stylised salutes, tattoos, patches and branded clothing, act as visible and durable expressions of ideological commitment. These are frequently observed at activist events, music gatherings, or conferences and may signal deeper affiliation when combined with other indicators.

Taken together, these categories illustrate how symbolism functions as a layered communication system within RWE movements, balancing overt messaging with coded signalling and cultural camouflage.

2. https://www.adl.org/sites/default/files/

3. Radical-Right Symbols, Slogans and Slurs Online: Germany—Kreter, Maximilian & Hof, Tobias. (2022). Radical-Right Symbols, Slogans and Slurs Online: Germany.

4. https://wyrddesigns.wordpress.com/2021/12/14/understanding-the-symbols/

Intersection with Terrorist Financing and Financial Sector Risk

The presence of extremist symbolism does not, in itself, constitute evidence of terrorist financing (TF). However, it may act as a contextual risk indicator when assessed alongside financial behaviour, network relationships and transactional anomalies.

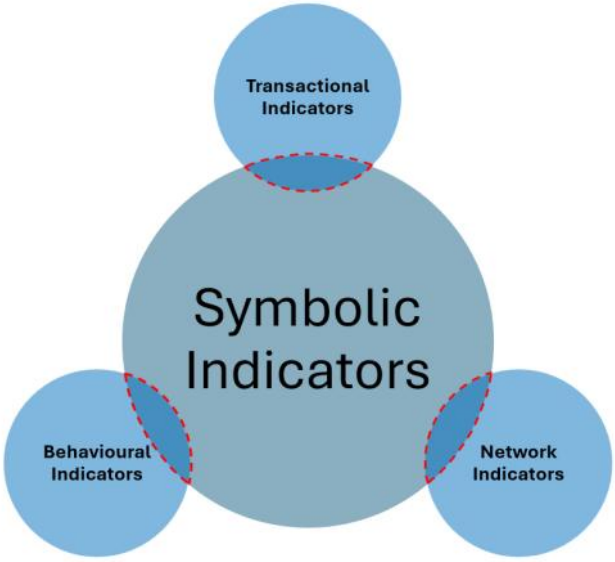
Right-wing extremist actors increasingly rely on decentralised and relatively low-value funding models. Common methods include:

- **Sale of ideologically branded merchandise.**
- **Online crowdfunding framed as activism or legal defence.**
- **Ticketed conferences, music events, or speaking engagements.**
- **Cryptocurrency donation campaigns.**
- **Peer-to-peer transfers within aligned networks.**

Within these models, symbolism functions not merely as expression but as financial infrastructure. It provides branding that attracts ideologically aligned donors, signals trust within closed communities and filters support through shared identity markers.

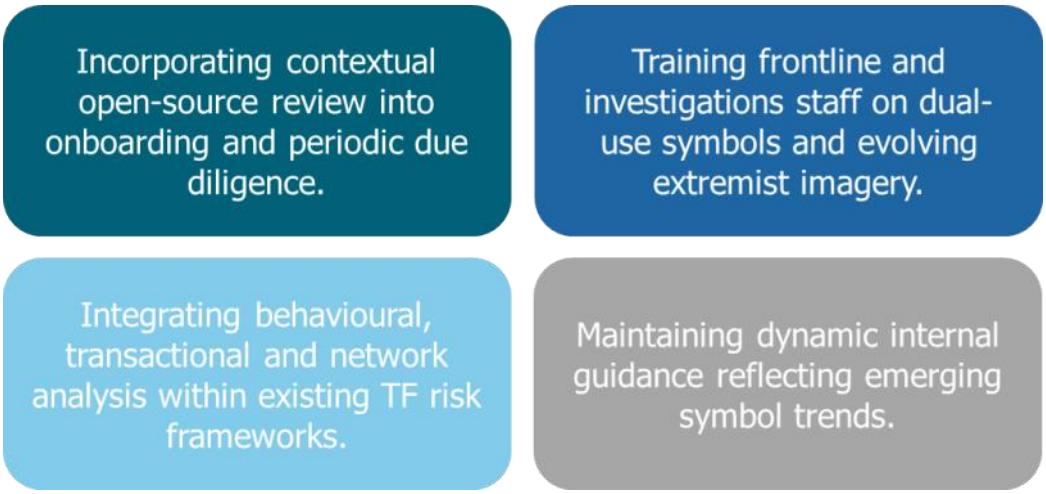
From a regulated financial institution perspective, risk may become more pronounced where symbolic indicators converge with:

- **Behavioural indicators,** such as public endorsement of extremist ideology or participation in extremist events.
- **Transactional indicators,** including rapid inflows followed by onward transfers, structured donations, cross-border transfers linked to extremist hubs, or migration to alternative payment methods following account termination.
- **Network indicators,** where individuals displaying ideological alignment share financial conduits, directorships, beneficial ownership structures, or funding pathways across interconnected entities.



The principal compliance challenge lies in proportionality. Many symbols retain legitimate cultural, religious, or historical meanings and reliance on static symbol lists may generate false positives or create civil liberties concerns. Effective mitigation therefore requires contextual, multi-factor analysis rather than symbol-only screening.

Isle of Man based financial institutions can strengthen their approach by:



In summary, right-wing extremist symbolism should neither be treated as determinative nor dismissed as irrelevant. When considered alongside financial behaviour and network activity, it may contribute meaningfully to identifying potential terrorist financing risk within the Isle of Man regulated sector.

Northern Ireland-Related Terrorism

Northern Ireland–related terrorism refers to violent activity associated with the constitutional status of Northern Ireland, historically linked to republican and loyalist paramilitary organisations during "The Troubles" (late 1960s–1998). Although the 1998 Good Friday Agreement significantly reduced large-scale violence, residual paramilitary structures and dissident groupings continue to present a security and terrorist financing risk.

Contemporary activity is primarily associated with dissident republican groups that reject the peace process and oppose the current constitutional settlement. These groups are generally smaller and less capable than their predecessors; however, they retain intent to target UK security forces, prison officers and symbolic infrastructure.

The Isle of Man's Terrorist Financing National Risk Assessment (TF NRA) recognises Northern Ireland–related terrorism as a relevant threat vector due to:

- Geographic proximity.
- The relative ease of travel and movement within the Common Travel Area.
- Historic personal and commercial links across the British Isles.

While typically assessed as lower risk than Islamist-inspired terrorism, it remains a credible threat that requires proportionate awareness within the regulated sector.

High Risk Countries:

Section 9.3 of the Terrorist Financing NRA[5] identifies jurisdictions that pose or may pose a higher risk of money laundering and terrorist financing (ML/TF). These jurisdictions are categorised into List A, List Bi and List Bii and are used by industry as a core geographic risk input within Business Risk Assessments and customer due diligence frameworks.

The Island distinguishes between jurisdictions subject to FATF countermeasures and those with strategic AML/CFT deficiencies or other elevated risk indicators. The June 2024 published lists were used for the NRA analysis.

List A – Jurisdictions Subject to FATF Countermeasures

Islamic Republic of Iran

Democratic People's Republic of Korea (DPRK)

Myanmar

List Bi – FATF-Identified Strategic AML/CFT Deficiencies

Bulgaria	Monaco	South Sudan
Burkina Faso	Mozambique	Syrian Arab Republic
Cameroon	Namibia	United Republic of Tanzania
Democratic Republic of the Congo	Nigeria	Bolivarian Republic of Venezuela
Croatia	Philippines	Vietnam
Haiti	Russian Federation	Yemen
Kenya	Senegal	
Mali	South Africa	

5. https://counteringfinancialcrime.im/media/nktj0030/iom-terrorist-financing-nra.pdf

High Risk Countries (cont.):

List Bii – Additional Jurisdictions Assessed as Higher Risk

Afghanistan	Eritrea	Pakistan
Angola	Eswatini	Sierra Leone
Belarus	Ethiopia	Solomon Islands
Plurinational State of Bolivia	Guinea	Somalia
Burundi	Guinea-Bissau	Sudan
Central African Republic	Iraq	Tajikistan
Chad	Kyrgyzstan	Togo
Comoros	Lebanon	Türkiye
Congo	Liberia	Turkmenistan
Cuba	Libya	Ukraine
Djibouti	Mauritania	Zimbabwe
Egypt	Republic of Moldova	
Equatorial Guinea	Niger	

United Nations Targeted Financial Sanctions (UNTFS)

United Nations Targeted Financial Sanctions (UNTFS) are restrictive measures imposed by the United Nations Security Council. They are binding on all Member States and implemented domestically through national legislation and regulatory frameworks.

UNTFS are a central international tool in countering terrorist financing. They require the immediate freezing of funds and economic resources belonging to designated individuals and entities and prohibit the direct or indirect provision of funds, financial services, or economic resources to those listed. Unlike broader country-based sanctions regimes, UNTFS' are targeted at specific persons or organisations identified as being involved in terrorism or its financing.

FATF Recommendation 6 requires countries to implement targeted financial sanctions regimes to give effect to United Nations Security Council Resolutions (UNSCRs) relating to the prevention and suppression of terrorism and terrorist financing. This includes UNSCR 1267 (1999) and its successor resolutions, which establish sanctions against individuals and entities associated with Al-Qaida, ISIL (Da'esh) and related groups, as well as UNSCR 1373 (2001), which requires countries to freeze without delay the assets of persons involved in terrorism and prohibit making funds or economic resources available to them.

For international finance centres such as the Isle of Man, compliance with UNTFS is critical. While the jurisdiction does not face a significant domestic terrorism threat, its globally connected financial services sector may be exposed to attempts by designated persons to retain access to assets or financial services.

Sanctions evasion commonly involves:

- **Transferring ownership or control of assets to family members or close associates.**
- **Establishing or restructuring corporate vehicles to obscure beneficial ownership.**
- **Maintaining de facto control or economic benefit despite removal from formal documentation.**

Importantly, sanctions obligations extend beyond simple name matching. The prohibition includes making funds or economic resources available indirectly, meaning that entities owned or controlled, whether formally or informally, by a designated person may present sanctions exposure.

As identified in the Isle of Man National Risk Assessment, sanctions evasion through complex structures and cross-border arrangements is a priority risk area. Effective compliance therefore requires robust screening measures, including enhanced due diligence, adverse media analysis and relational or network-based screening capable of identifying close associates and indirect control.

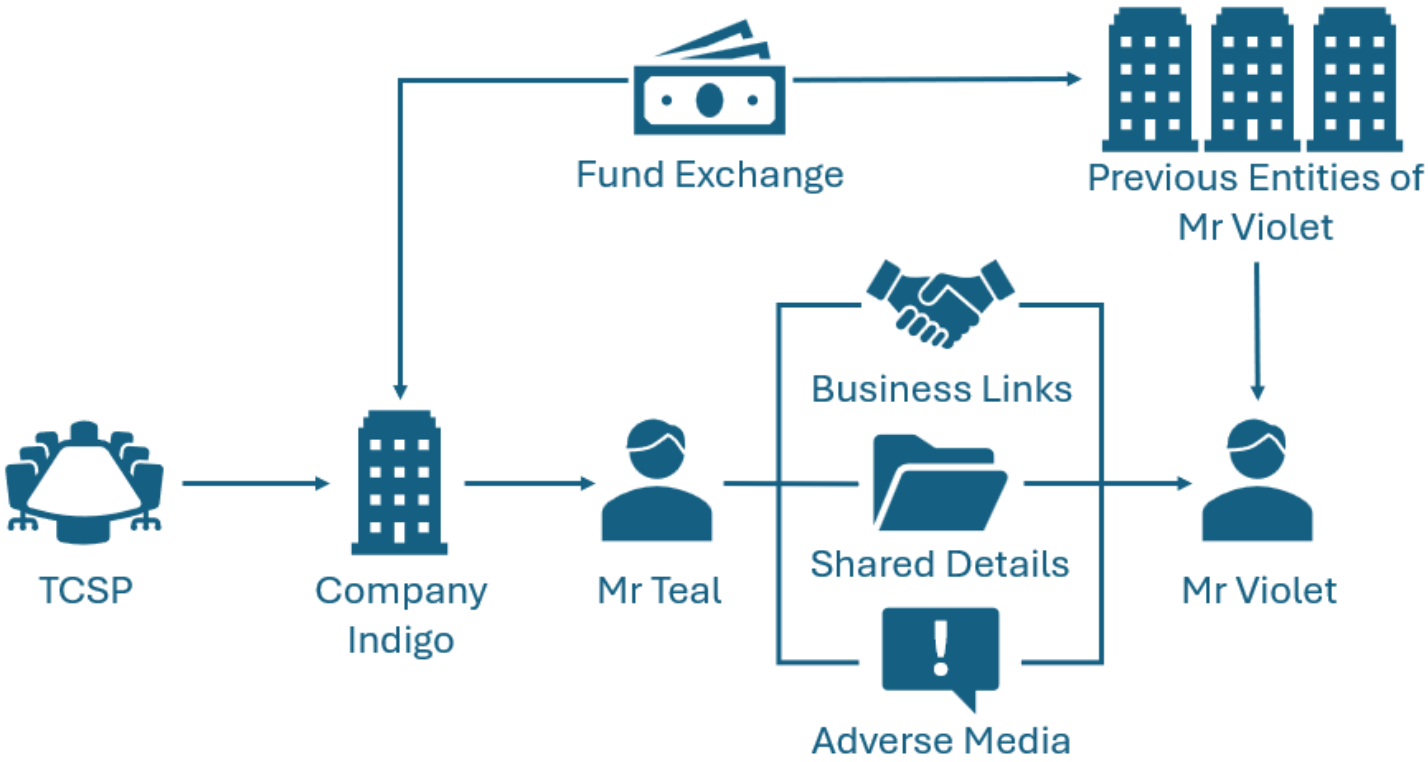
Typologies:

Typology 1:

Mr. Violet was listed under a United Nations sanctions regime for financing a terrorist group operating abroad. Several months later, an Isle of Man based TCSP incorporated Company Indigo on behalf of Mr. Violet's long-standing business associate, Mr. Teal.
Mr. Teal was declared as the sole beneficial owner and director. He stated the company would provide consultancy services in the logistics sector. Initial due diligence did not identify any sanctions matches against Mr. Teal.
However, enhanced sanctions screening incorporating relational and network analysis identified:

- **Extensive historic business links between Mr. Teal and Mr. Violet.**
- **Shared addresses and contact details in previous files.**
- **Adverse media describing Mr. Teal as a "trusted adviser" to Mr. Violet.**
- **Financial transfers between entities previously owned by Mr. Violet and Company Indigo.**

Although Mr. Teal was not designated, intelligence suggested he may have been acting as a proxy to preserve Mr. Violet's access to financial services.



Red Flags

⇒ **Newly incorporated entity controlled by a close associate of a sanctioned individual.**

⇒ **Associate with limited independent business profile but strong historic ties to designated person.**

⇒ **Shared addresses, contact details, or corporate history.**

⇒ **Ongoing financial flows between legacy entities and new structures.**

⇒ **Adverse media identifying the associate as a close confidant or facilitator.**

Typology 2: Charitable Organisation Used to channel TF Proceeds

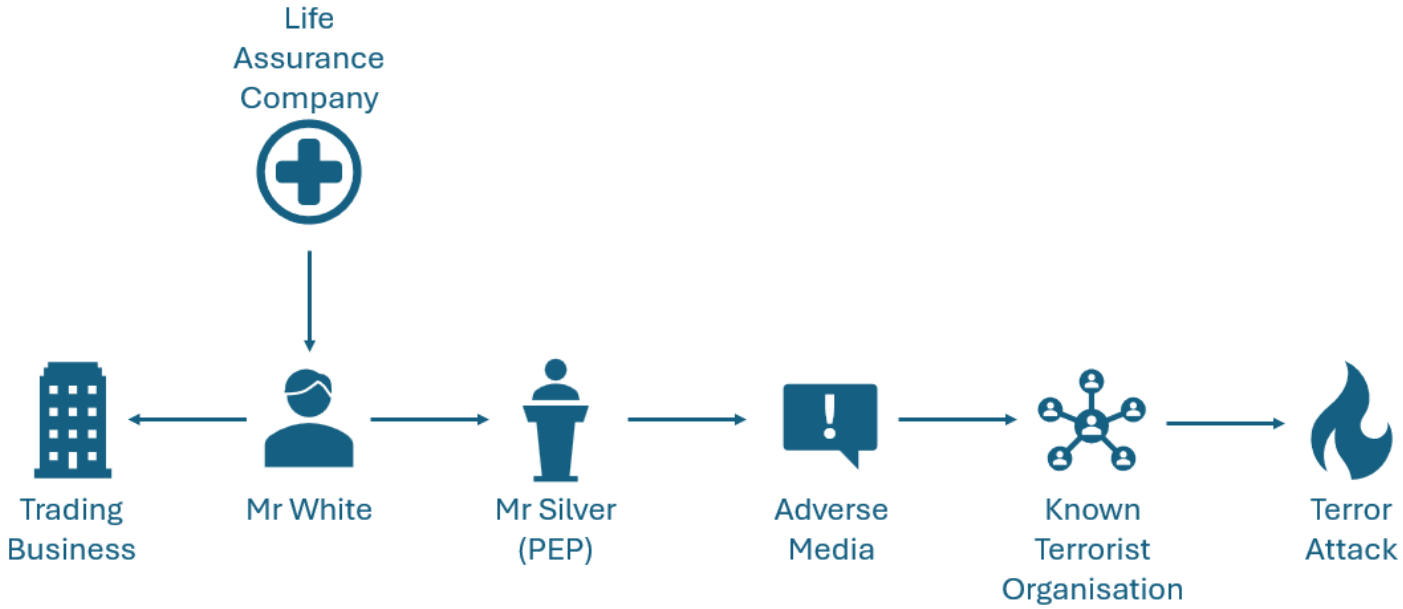
Mrs. Green established a newly registered Isle of Man charity providing educational materials to children in a Middle Eastern conflict zone. Over 12 months, the charity raised £65,000, much of it in cash. Funds were transferred in small tranches to a personal account in a neighbouring jurisdiction, where the 'project partner' was based.

Red Flags

- ⇒ **High proportion of cash donations without donor records.**
- ⇒ **Transfers to personal accounts abroad.**
- ⇒ **Beneficiary in a jurisdiction with known terrorist activity.**

Typology 3: PEP Relative Identified in Life Assurance Screening

Mr. White held a policy with an Isle of Man regulated Life Assurance Company. He resided in Country Z, where he operated a successful trading business. Routine screening found Mr. White was a close relative of Mr. Silver, a former high-ranking official in Country X linked via open-source intelligence to a known terrorist organisation and an alleged terrorist-backed attack on a State Embassy.



Red Flags

- ⇒ **Customer is a close associate or relative of an individual linked to terrorist activity.**
- ⇒ **Adverse media linking a PEP to terrorist organisations.**
- ⇒ **Indirect exposure to TF risk despite absence of direct transactional links.**

Typology 4: Complex NPO Grant Disbursement Chain

Charity Blue, registered in the Isle of Man, received significant funding from a European donor organisation for humanitarian relief in Country P. Funds were disbursed via two intermediary NGOs before reaching the intended programme. One intermediary had connections to a sanctioned TF entity and structured transfers to avoid detection.

Red Flags

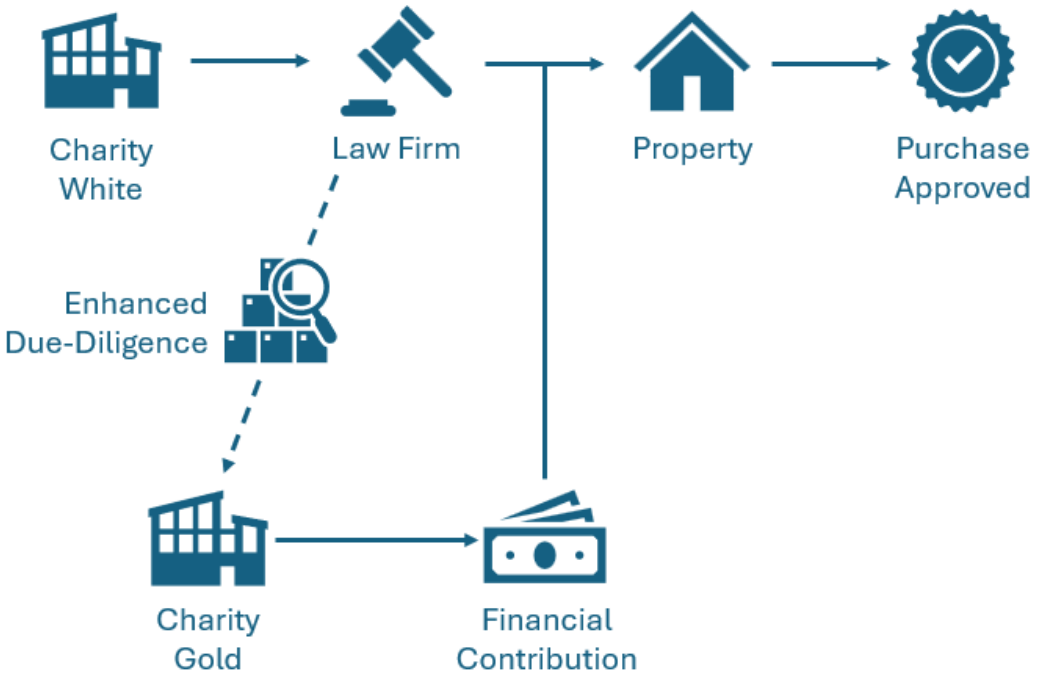
⇒ **Multi-jurisdictional disbursement chain reducing transparency.**

⇒ **Intermediary entity linked to designated persons.**

Typology 5: Charity Property Purchase Potentially Linked to Terrorist-Associated Donors

An Isle of Man based law firm acted for Charity White in purchasing property. Part of the funds came from Charity Gold, a UK-registered charity resembling an organisation alleged to front terrorist activities in Countries Q and P.

Following enhanced due diligence checks it was confirmed that there was no connection to the alleged terrorist activities in countries Q and P, and therefore the transaction progressed.



Red Flags

⇒ **Donations from an entity resembling a terrorist-front organisation.**

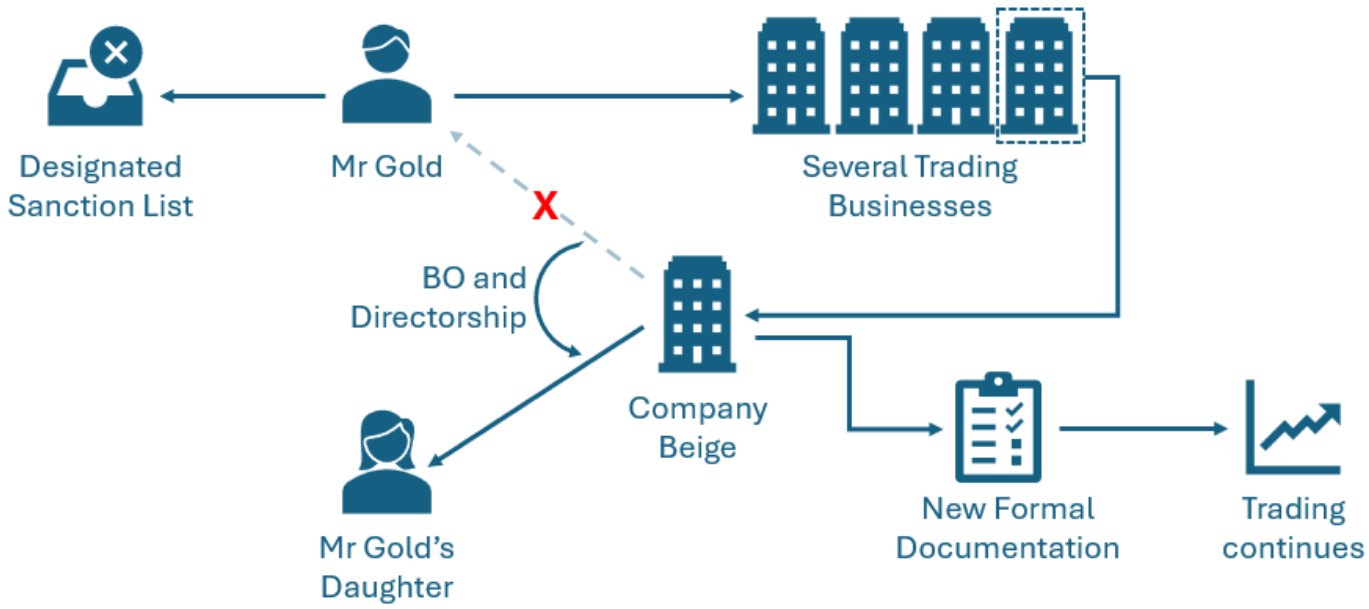
⇒ **Incoming funds from high-risk jurisdictions.**

Typology 6:

Mr Gold was designated under a United Nations sanctions regime for providing financial support to a terrorist organisation operating in a conflict-affected region. Prior to designation, Mr Gold had beneficial ownership of several trading entities operating internationally.
Within weeks of the designation, an Isle of Man incorporated company, Company Beige, underwent a change in beneficial ownership. Mr Gold's adult daughter was registered as the sole beneficial owner and director. The company's business activities and banking arrangements continued largely unchanged.
Enhanced due diligence identified that:

- **The daughter had limited independent income or business experience.**
- **Company Beige continued to transact with counterparties historically linked to Mr Gold.**
- **Email correspondence and contractual negotiations appeared to be directed by an individual using Mr Gold's known contact details.**
- **The company's source of funds originated from jurisdictions previously associated with Mr Gold's business network.**

Although Mr Gold no longer appeared in formal documentation, intelligence suggested he continued to exercise de facto control and benefit economically from the structure.



Red Flags

- ⇒ **Transfer of beneficial ownership to an immediate family member shortly after sanctions designation.**
- ⇒ **Newly appointed beneficial owner lacking independent source of wealth.**
- ⇒ **Continuity of business operations despite ownership change.**
- ⇒ **Ongoing transactional links to counterparties previously associated with the sanctioned individual.**
- ⇒ **Evidence of indirect control (shared contact details, advisory role, informal decision-making).**

Typology 7: Cross-Border Transfer Concealing Destination in High-Risk Jurisdiction

Mrs. Pink held an account with an Isle of Man regulated bank and requested a transfer to Company Bronze in Country X, which borders high-risk Country Z. Enhanced due diligence revealed Company Bronze used a false address and was registered in Country Z, raising TF/PF concerns.

Red Flags

- ⇒ **False address to disguise location in a high-risk jurisdiction.**
- ⇒ **EDD triggered by geographic risk.**
- ⇒ **Potential sanctions circumvention.**

Typology 8: Use of Online Gambling to Transfer TF Funds

Mr. Red and Mr. Black, in different countries, maintained accounts on the same Isle of Man–licensed poker platform. They repeatedly played together, with one deliberately losing high-value games to the other. The winner withdrew funds to a cryptocurrency wallet later linked to a sanctioned terrorist organisation.

Red Flags

- ⇒ **Repeated interaction between same accounts.**
- ⇒ **Unusual gameplay suggesting deliberate loss .**
- ⇒ **Withdrawals to high-risk cryptocurrency addresses.**

Typology 9: Attempted Real Estate Purchase by High-Risk Entity

Company Sapphire, incorporated in Country X, approached an Isle of Man estate agent to arrange the purchase of a property in the Isle of Man with an approximate value of GBP 800,000. The estate agency obtained KYC documentation relating to Company Sapphire and its ultimate beneficial owner, Mr. Red. Subsequent OSINT checks identified that Mr. Red was linked to a designated terrorist organisation. Upon identifying this adverse information, the estate agent declined the business relationship and submitted a SAR to the FIU.

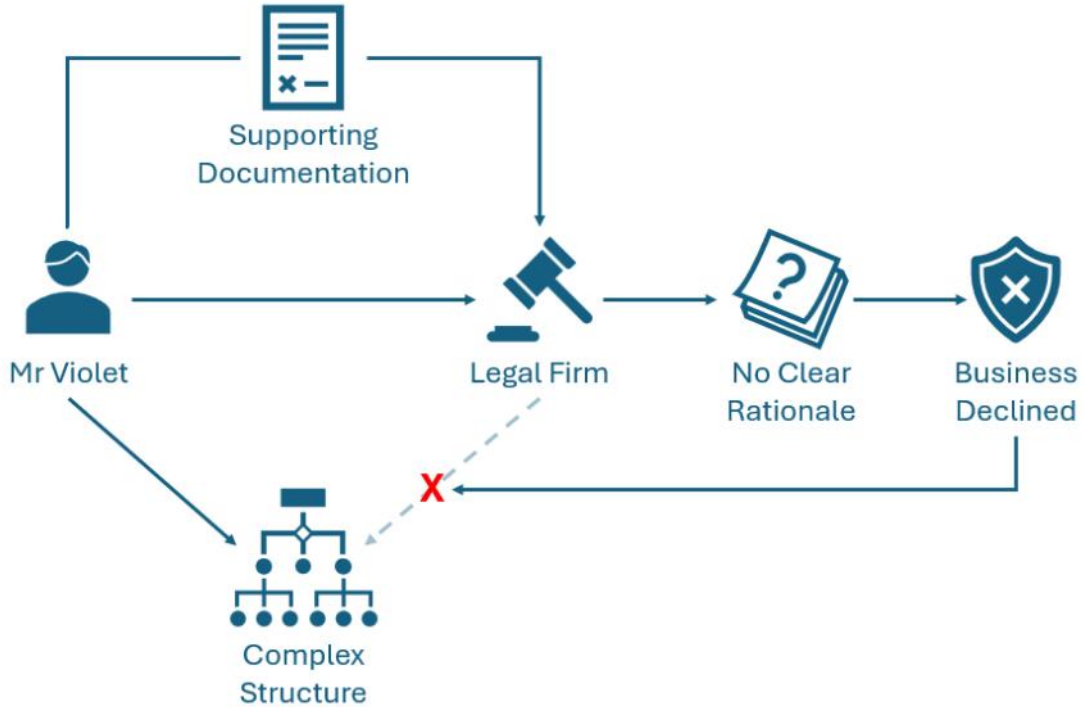
Red Flags

⇒ **High-value property purchase by entity with high-risk jurisdictional links.**

⇒ **Beneficial owner linked to designated persons.**

Typology 10: Misuse of Legal and Accounting Services for Complex Structures

Mr. Violet, an international client, engaged an Isle of Man legal firm to create a multi-tier structure involving trusts, companies, and nominee directors across three jurisdictions. Despite the legal firm requesting further supporting documents to understand the working relationship, they were unable to identify a legitimate commercial purpose. Open source intelligence linked Mr. Violet to a UN-sanctioned TF organisation. The business was declined and a SAR was reported to the FIU.



Red Flags

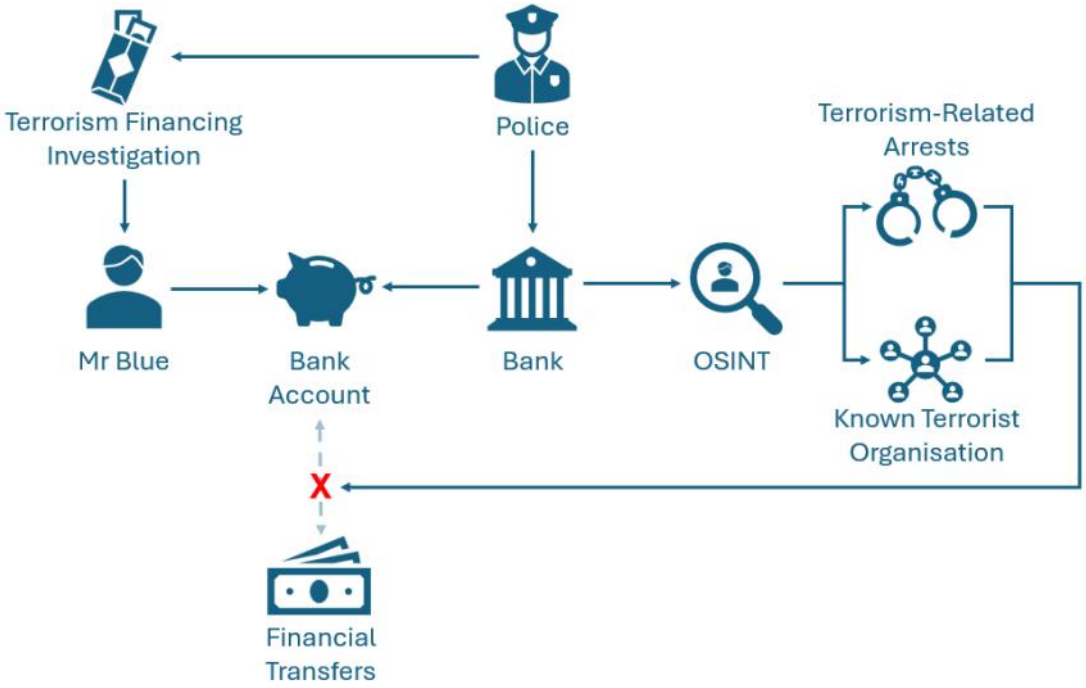
⇒ **Multi-layered structure with no discernible commercial activity.**

⇒ **Use of multiple jurisdictions to fragment oversight.**

⇒ **Ultimate owner linked to sanctioned organisation.**

Typology 11: Bank Account Holder Under Police Investigation for TF

Mr. Blue, an Isle of Man resident, held an account with an Isle of Man regulated bank. The bank received a police notification stating that Mr. Blue was under investigation in connection with terrorist financing.
Subsequent open-source intelligence checks identified prior arrests for terrorism-related offences, as well as attendance at meetings in support of a prescribed organisation. The account displayed limited transactional activity and while no transactions could be directly linked to terrorist financing, this possibility could not be discounted. In light of the information received, an immediate block was placed on the account and a Suspicious Activity Report (SAR) was submitted to the Financial Intelligence Unit (FIU).



Red Flags

- ⇒ **Police notification of TF investigation.**
- ⇒ **Prior arrests for terrorism offences.**
- ⇒ **No direct links to TF but could not discount that funds could have been used for TF purposes.**

Typology 12: Sanctioned Terrorist Organisation Member Identified in Online Gambling Account

Mrs. Purple held an account with an Isle of Man–based online gambling company. Routine screening identified her as sanctioned by the UK, EU, US, and UN for membership in two known terrorist organisations. Open-source checks confirmed a 12-year prison sentence for terrorist offences. The account displayed only minor free-play activity with no monetary transactions. It remains unclear whether the account's purpose was legitimate or criminal. The account was immediately frozen and reported to the FIU.

Red Flags

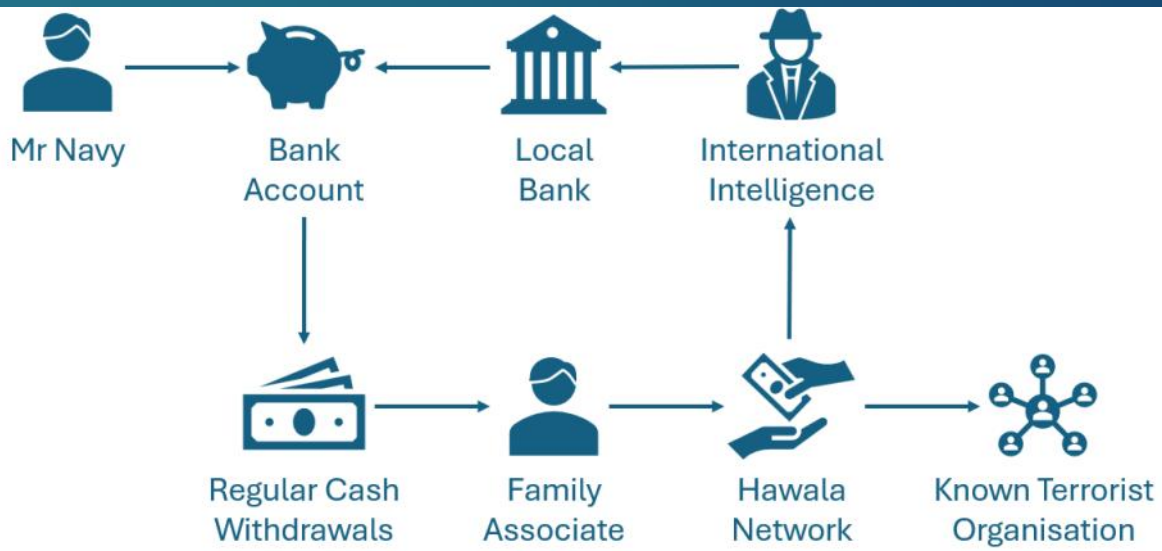
- ⇒ **Multiple sanctions designations.**
- ⇒ **Prior conviction for terrorist activity.**
- ⇒ **No transactional activity despite account opening.**

Typology 13: Use of Hawala Networks to Finance Terrorist Activity

Mr Navy, an Isle of Man resident, maintained a personal account with a local bank. Over several months, he made repeated and regular cash withdrawals.

During a business trip abroad, Mr Navy provided these funds to a family associate in Country X, where Hawala networks are widely used. The associate deposited the money with a Hawaladar, who arranged for an equivalent amount to be made available in Country Y, a jurisdiction with links to a designated terrorist organisation.

The original funds left the Isle of Man banking system through ordinary withdrawals, creating little suspicion. Only later, through international intelligence sharing, was it identified that the Isle of Man sourced funds had entered a Hawala network used to support extremist groups.



Red Flags

⇒ **Frequent cash withdrawals inconsistent with customer profile.**

⇒ **Transfers or dealings linked to jurisdictions where Hawala is prevalent.**

Typology 14: Payments Linked to Turkey / Syria Nexus

Mr Umber, a foreign national residing in the Isle of Man, held a personal account with a local bank. Over the course of three months, he instructed multiple low-value transfers to a beneficiary account in Turkey. The stated purpose of the transfers was "family support."
Routine transaction monitoring did not immediately raise suspicion, as the payments were of a relatively low value and appeared consistent with expected account activity. However, subsequent intelligence sharing revealed that the Turkish beneficiary was acting as a conduit, forwarding equivalent sums to individuals in Syria associated with a designated terrorist organisation.
The Isle of Man-originated payments, though small in value, formed part of a wider international chain facilitating terrorist financing across the Turkey–Syria nexus.

Red Flags

⇒ **Outbound transfers to Turkey or neighbouring jurisdictions with links to conflict zones.**

⇒ **Customers citing vague purposes such as "family support" with no corroborating evidence.**

⇒ **Chains of transfers involving multiple jurisdictions before reaching the final recipient.**

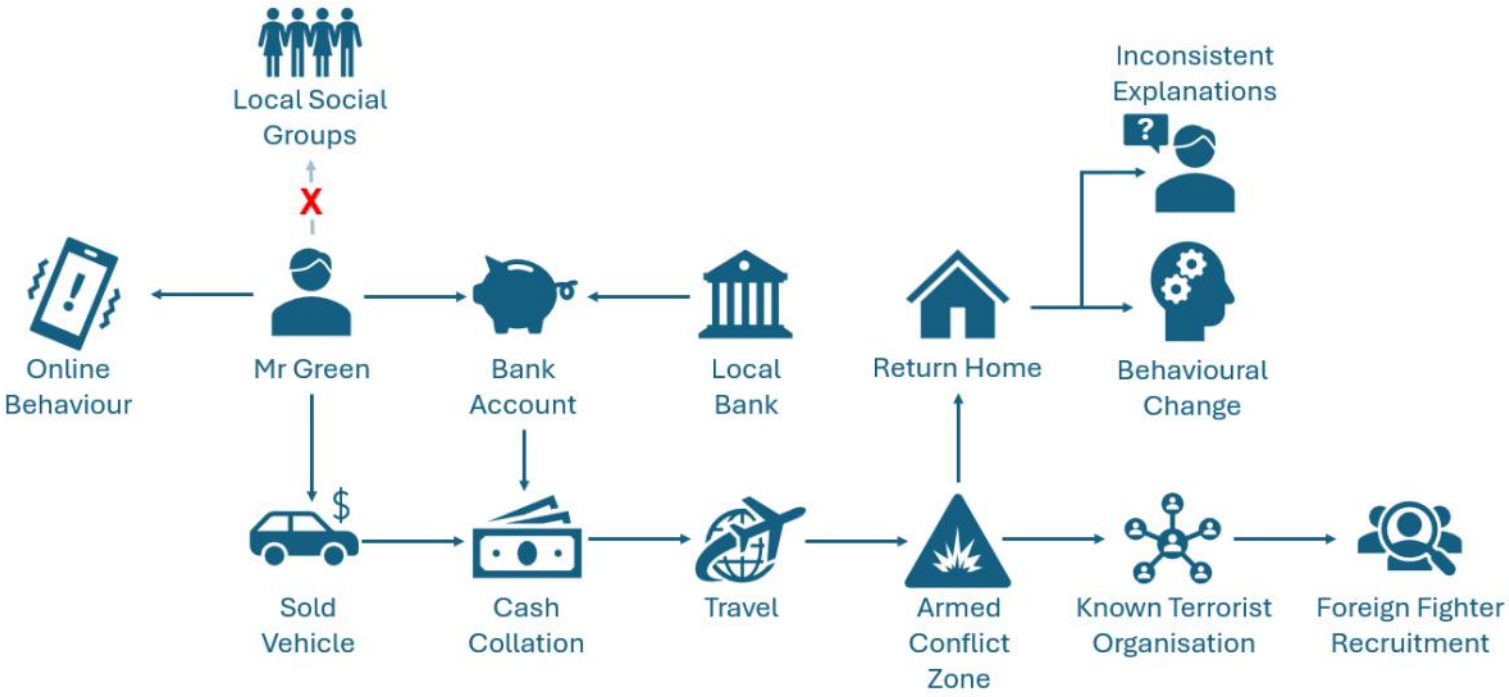
⇒ **Beneficiaries linked through intelligence or adverse media to individuals or**

Typology 15: Travel to a Conflict Zone for Fighting / Military Training

Mr Green, a resident in the UK, maintained a personal relationship with a group of overseas contacts who shared ideological views. Over a six-month period, he depleted savings held in his Isle of Man Bank account, sold a vehicle, and made a number of cash withdrawals. He purchased a low-cost airline ticket to a neighbouring country and, after a short stopover, travelled onward overland into a region affected by armed conflict where an organisation with known links to terrorism was active.

Prior to travel, Mr Green became progressively more isolated from local social groups, increased his use of encrypted messaging apps, and posted increasingly ideological material on private social media channels. On return to the UK several months later he exhibited changes in demeanour and provided inconsistent explanations about his activities abroad. Publicly available reporting and subsequent intelligence indicated that individuals associated with the group operating in the conflict zone had been recruiting and training foreign fighters.

Although no single action conclusively proves intent to fight, Mr Green's pattern of behaviour, financial depletion, structured travel, use of informal contacts abroad and corroborating intelligence, indicated a credible risk that funds and travel were being used to travel for fighting or training.



Red Flags

⇒ **Travel itineraries that include stopovers in neighbouring countries en route to a conflict zone.**

⇒ **Sudden and unexplained depletion of personal funds (large cash withdrawals, sale of assets).**

⇒ **Purchase of one-way tickets or travel arrangements that avoid conventional routes and documentation.**

⇒ **Use of cash or informal payment methods to fund travel and accommodation abroad.**

Red Flags Cont.

⇒ **Increased use of encrypted or private messaging platforms and closed social media groups discussing travel to conflict areas.**

⇒ **Social or family disclosures of intent to travel for ideological/religious reasons without credible supporting rationale.**

⇒ **Links or communications with individuals or groups known to operate in conflict zones or associated with extremist ideologies.**

⇒ **Unexplained absence from employment or education that coincides with travel.**

⇒ **Return with inconsistent accounts of activities, or possession of material (photos, messages) indicating paramilitary training or association.**

Conclusion

The typologies presented demonstrate the diversity of potential terrorist financing methodologies relevant to the Isle of Man. Whilst the jurisdiction's regulatory framework is robust, TF risks persist due to the complexity of international financial transactions, the adaptability of terrorist organisations to exploit legitimate sectors, and the increasing use of virtual assets and online platforms.

The FIU encourages all regulated entities to maintain awareness of TF indicators and sector-specific vulnerabilities, to undertake robust customer due diligence and enhanced due diligence where required, and promptly report suspicious activity to the FIU.

Even low-value or indirect transactions may form part of a wider TF network, therefore continued vigilance, intelligence sharing, and industry collaboration remain essential to protecting the Isle of Man's financial system from abuse.

Contacting the FIU

If you have queries in relation to this typology report, or wish to discuss matters arising from its content, you may contact the FIU for guidance. The FIU can be contacted by telephone on +44 (0)1624 686000 or by email at fiu@gov.im. General information, guidance and access to the online reporting system (THEMIS) are available via the FIU website at www.fiu.im.

Where a person or business knows, suspects, or has reasonable grounds to suspect that a terrorist financing offence is being committed, or that funds are linked to terrorism, they must make a disclosure under the Anti-Terrorism and Crime Act 2003 (ATCA). In urgent or live situations, reporters are encouraged to telephone the FIU without delay in advance of, or in parallel with, submitting a disclosure via THEMIS.

Suspicious activity relating to money laundering or suspected criminal property must be reported under the Proceeds of Crime Act 2008 (POCA), using the appropriate reporting option within THEMIS. Where the same matter has been reported to another jurisdiction, this should be clearly stated within the disclosure narrative.

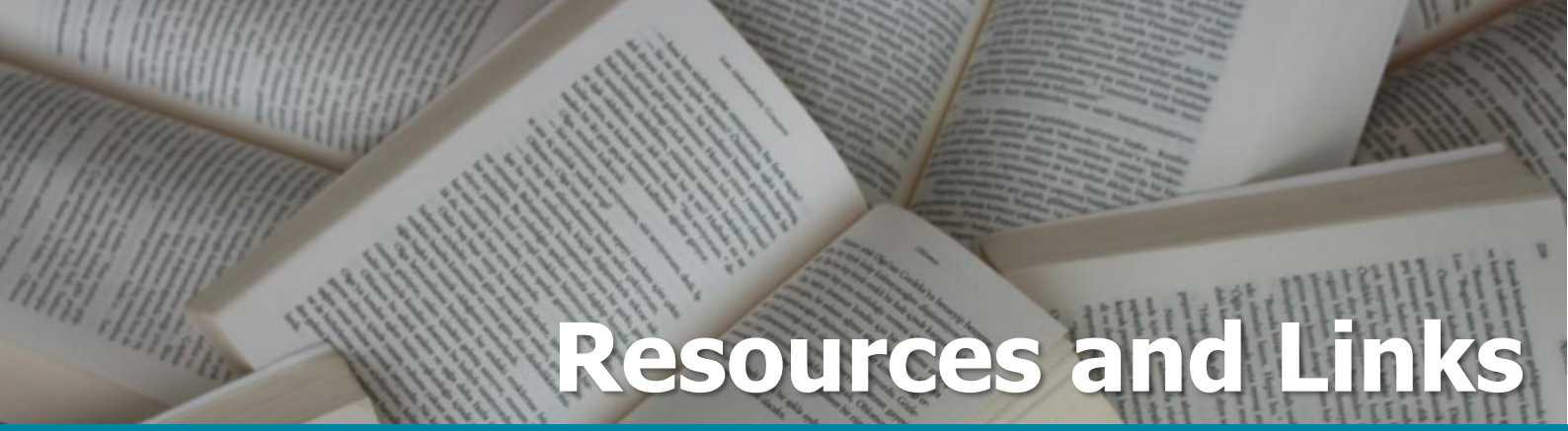
Suspected breaches of Isle of Man or United Kingdom targeted financial sanctions (including dealings with designated persons or frozen assets) must be reported to the FIU as soon as practicable. Where relevant, disclosures should include designation details, unique identifier references, date and time assets frozen, and information concerning ownership and control.

Information relating to other sanctions regimes, such as OFAC designations, or intelligence of relevance to the FIU where no suspicion has yet been formed, may be disclosed under Section 24 of the Financial Intelligence Unit Act 2016. Section 24 disclosures may be made by any person for the purpose of assisting the FIU in exercising its statutory functions, noting that suspicious activity from the regulated sector must still be reported under POCA and/or ATCA as appropriate.

The FIU encourages early engagement where uncertainty exists regarding reporting obligations and reminds all sectors that timely, accurate, and high-quality disclosures are essential to protecting the integrity of the Isle of Man's financial system.

Glossary

AML	Anti-Money Laundering
ATCA	Anti-Terrorism and Crime Act
CFT	Countering the Financing of Terrorism
EMIs	Electronic Money Institutions
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IVTS	Informal Value Transfer Systems
NRA	National Risk Assessment
NPOs	Non-Profit Organisations
OFAC	Office of Foreign Assets Control
OFSI	Office of Financial Sanctions Implementation
POCA	Proceeds of Crime Act
SAR	Suspicious Activity Report
SDN	Specially Designated National
TBML	Trade-Based Money Laundering
TCSPs	Trust and Corporate Service Providers
TF	Terrorist Financing
UNTFS	United Nations Targeted Financial Sanctions
UNSCRs	United Nations Security Council Resolutions
VASPs	Virtual Asset Service Providers
JIMLIT+	Joint Money Laundering Intelligence Taskforce
IRGC	Islamic Revolutionary Guards Corp
PSP	Payment Service Provider
SDN	Specially Designated National
IVTs	Informal Value Transfer Systems



Resources and Links

1. **https://www.iomfsa.im/media/3259/ft-fact-sheet.pdf**
2. **https://www.adl.org/sites/default/files/**
3. **Radical-Right Symbols, Slogans and Slurs Online: Germany—Kreter, Maximilian & Hof, Tobias. (2022). Radical-Right Symbols, Slogans and Slurs Online: Germany.**
4. **https://wyrddesigns.wordpress.com/2021/12/14/understanding-the-symbols/**
5. **https://counteringfinancialcrime.im/media/a2fnlfi0/money-laundering-nra-march26v3.pdf**
6. **https://counteringfinancialcrime.im/media/nktj0030/iom-terrorist-financing-nra.pdf**