Terrorist Financing Red Flags

Strengthening CFT Compliance: Recognising Terrorist Financing Red Flags in the Virgin Islands

Strengthening CFT Compliance: Recognising Terrorist Financing Red Flags in the Virgin Islands (VI)

These red flag indicators have been developed to assist Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) in identifying potential signs of Terrorist Financing. They build upon red flag guidance previously issued by the competent authorities in the Virgin Islands, including the BVI Financial Services Commission (FSC) and the Financial Investigation Agency (FIA).

Earlier guidance, which outlines general suspicious activity indicators for money laundering and related financial crimes, can be accessed on the **FSC's website**.

Terrorist Financing (TF) is the collection or movement of funds to support terrorist activities, whether directly or indirectly. These funds may be derived from legitimate or illicit sources, but the key feature is their intended use to support terrorism.

As an international finance centre, the Virgin Islands (VI) remains at an elevated risk for TF as identified in the **Virgin Islands 2025 TF Risk Assessment**. The TF Risk Assessment found that the products and services provided by FIs and DNFBPs, were vulnerable to misuse for TF purposes. As such, FIs and DNFBPs must remain acutely aware of the vulnerabilities posed by these products and services and aid in identifying any unusual activities.

The following red flags have been provided to highlight activities and behaviors that may indicate TF risk. However, the presence of a red flag does not necessarily confirm TF. Instead, it signals the need for further due diligence, monitoring, and reporting.

Obscuring Beneficial Ownership (BO)

RED FLAG: Beneficial ownership of legal person or legal arrangements is unclear or buried under multiple layers of ownership.

Why this is a red flag: Terrorist financiers may hide behind complex structures to move funds and disguise who is truly in control.

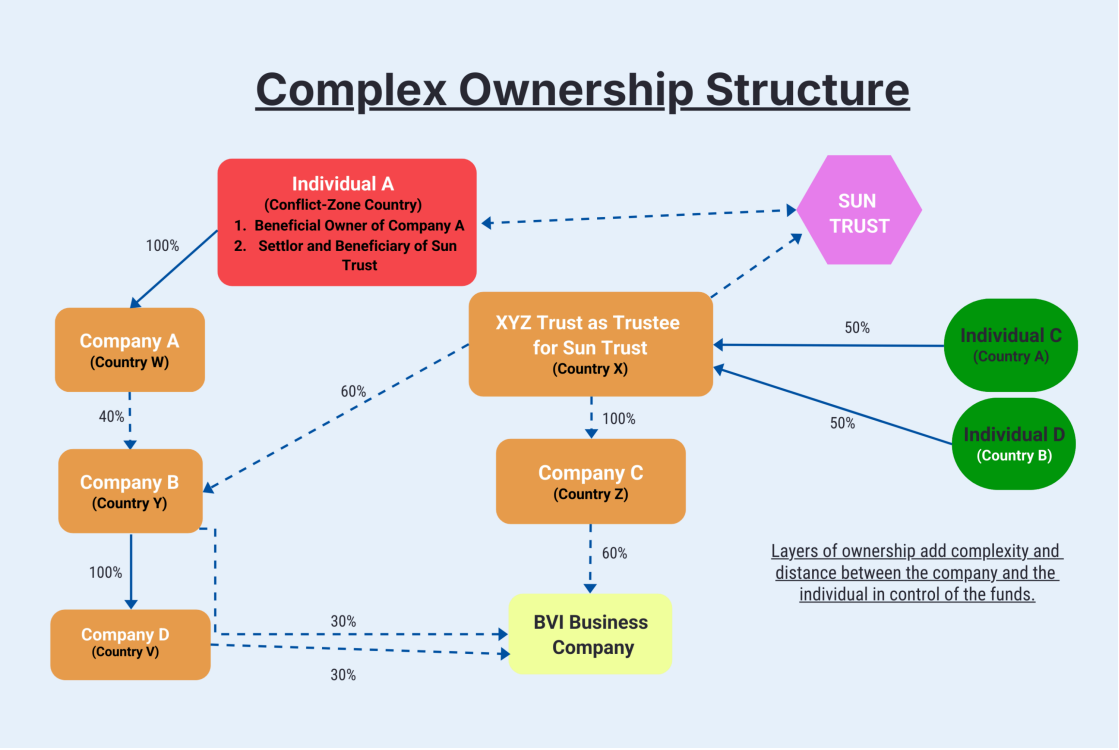
Examples of suspicious activity:

Corporate structures that involve multiple layers where beneficial ownership is difficult to determine. For example:

Individual A is the sole beneficial owner of Company A, which holds 40% shares in Company B. Company B has direct ownership in the BVIBC through its 30% shareholding. Company B also has indirect ownership of the BVIBC through its ownership of Company D.

Individual A is also the settlor and beneficiary of Sun Trust whose trustee, XYZ Trust, owns Company C, which holds 60% of the shares in the BVI Business company.

The shareholders of XYZ Trust are Individuals C and D, who are the sons of Individual A.



These layers of ownership of the BVI entity — add a level of complexity and distance between the company and the individual in control of the funds.

The use of multiple jurisdictions makes it more difficult to trace the source of funds or verify the legitimacy of the ultimate beneficial owner.

Other examples of suspicious activity:

1. Clients refuse, delay, or provide inconsistent information about beneficial ownership.
2. Changes, sudden or otherwise, in ownership that have no clear rationale or economic value.

Misuse of BVI Legal Persons and Legal Arrangements

RED FLAG: A BVI Business company (BVIBC), other legal person (e.g., limited partnership), or legal arrangement (e.g., trust) is used in a way that does not make commercial sense or executes transactions with unusual financial patterns.

Why this is a red flag: Terrorist financiers may exploit BVIBCs, other legal persons and legal arrangements to conceal ownership, control, or the movement of funds that do not align with an entity's stated business purpose. This might indicate that the entity is being exploited to disguise the movement of terrorist funds.

Examples of suspicious activity:

A dormant company suddenly begins wiring large sums to overseas accounts in high risk jurisdictions.

Related companies suddenly engage in frequent transfers with no documented business reason.

Companies start engaging in high-value transactions inconsistent with their stated business.

Inadequate Oversight of Non-Profit Organisations (NPOs)

RED FLAG: An NPO receives or moves funds in ways that do not match its stated purpose.

Why this is a red flag: NPOs can be used or misused to collect or transfer money under the appearance of legitimate activity.

Examples of suspicious activity:

Transfers of funds to high-risk jurisdictions or regions currently experiencing armed conflict and/or political instability on the guise of providing humanitarian aid but the funds are diverted to support terrorist groups operating in that area.

An NPO regularly receives donations from individuals in conflict zones without explanation.

Charitable funds are transferred to accounts held by private businesses unrelated to the NPO's stated purpose.

Numerous small cash deposits made by unrelated third parties, inconsistent with typical local fundraising.

Payments made to individuals abroad that cannot be linked to any documented project or programme.

Attempts to Circumvent Targeted Financial Sanctions (TFS)

RED FLAG: Transactions involve sanctioned persons, jurisdictions, or goods.

Why this is a red flag: Circumventing Targeted Financial Sanctions can allow terrorists or their supporters to move or access funds despite restrictions.

Background: Sanctions are legal measures that restrict dealings with individuals, entities, or countries linked to terrorism, terrorist financing or other illicit activity.

Targeted Financial Sanctions require FIs and DNFBPs to freeze the assets of listed persons and prohibit any financial activity with them.

To comply, FIs and DNFBPs must carry out sanctions screening – checking client names and counterparties against official sanctions lists (such as those issued by the UN, UK or under Virgin Islands legislation) to ensure they are not dealing with a sanction party.

Examples of suspicious activity:

1. A client makes payments to an entity with a name similar to one on a sanctions list.
2. Funds are routed through multiple banks or intermediaries before reaching a sanctioned jurisdiction.
3. Customer attempts to withdraw or transfer funds or other assets just prior to or immediately following the publication of updated sanctions lists.
4. Purchase orders referencing restricted dual-use goods without a clear business need.

Suspicious Use of Cash

RED FLAG: Customers rely heavily on cash transactions.

Why this is a red flag: Cash transactions are difficult to trace and can indicate an attempt to conceal the movement of funds linked to terrorist financing.

Examples of suspicious activity:

1. A customer with a modest income regularly deposits large amounts of cash that exceed their expected earnings.
2. Repeated cash transactions just below the VI's reporting threshold (e.g., $9,800, $9,900).
3. Cash is taken out from different branches or ATMs, possibly to move funds for terroristic purposes.

Use of Informal or Alternative Money Transfer Systems

RED FLAG: Customers use informal or unregulated transfer systems instead of formal banking channels.

Why this is a red flag: The use of informal money transfer systems (like *hawala)* operate outside the regulated financial sector, making them hard to trace or monitor.

Examples of suspicious activity:

1. Customers frequently using money remittance services instead of their bank account to send funds to high-risk countries.
2. A client insists on using informal transfer systems despite having access to formal banking services.
3. A customer receives unexplained incoming transfers from informal systems where the customer cannot verify the origin or purpose of funds.

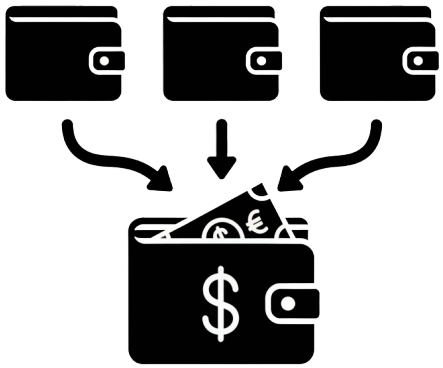
Misuse of Virtual Assets and Virtual Asset Service Providers (VASPs)

RED FLAG: Frequent or multiple virtual asset transactions to and from jurisdictions at high risk for TF.

Why this is a red flag: Virtual assets can provide anonymity and fast cross-border transfers, making them appealing for terrorist financiers.

Examples of suspicious activity:

1. A customer conducts multiple transactions using an unlicensed virtual asset exchange.
2. Large virtual asset transfers with no clear stated purpose.
3. Funds are split across multiple wallets and then consolidated into a single account before being cashed out.
4. A customer regularly converts virtual assets into cash through peer-to-peer platforms without using regulated exchanges.



Unusual or Inconsistent Customer Behavior and Transaction Patterns

RED FLAG: Customer actions or transactions do not match their normal profile

Why this is a red flag: Unusual behavior may indicate attempts to disguise the origin, purpose, or destination of funds connected to terrorist financing.

Examples of suspicious activity:

A low-income client sends frequent large international wire transfers.

Customers are evasive when asked about the origin of funds or refuse to provide documentation.

Wire transfers contain vague descriptions such as “consulting services” without supporting invoices or contracts.

A client pressures staff to process transactions immediately and insists on confidentiality.

Mitigating the Risk of Terrorist Financing (TF)

To effectively mitigate TF risks, FIs and DNFBPs should implement internal controls that enable the early detection and reporting of suspicious activity. Key measures include:

Know Your Customer (KYC)	Conduct thorough customer due diligence (CDD) and verification.
Monitor transactions	Understand transaction patterns in order to identify unusual activity or patterns that do not match a customer's profile.
Maintain adequate records	Keep accurate and up to date records of transactions and customer profiles.
Report Suspicious Activities	File Suspicious Activity Reports (SARs) promptly with the Financial Investigation Agency (FIA).
Staff Training and Awareness	Provide regular CFT training to staff to ensure they can recognise TF red flags, understand reporting obligations, ad apply CFT procedures effectively.
Independent Reviews	Conduct periodic internal audits or independent reviews to assess the effectiveness of the institution's CFT controls and make improvements where needed.

For more information on AML/ CFT requirements and guidance:
Visit the BVIFSC's website at **www.bvifsc.vg**
Contact the AML/ CFT Unit at **aml@bvifsc.vg**