Terrorist Financing

Typology Report

2026

Prepared by: **Financial Investigation Agency (FIA)**

Report Type: **Analytical Typology Report**

Reporting Basis: **Virtual Assets Suspicious Activity Reports (VA SARs)**

Activity Period Covered: **2018 - 2025**

SAR Filing Period: **December 2024 - October 2025**

TABLE OF CONTENTS

Report Overview

EXECUTIVE SUMMARY

This report outlines key terrorist financing typologies identified through the analysis of multiple Suspicious Activity Reports (SARs), submitted by Virtual Asset Service Providers (VASPs), which are referred to as “VA SARs”. The findings highlight recurring patterns in how funds are raised, transferred, and concealed in activity linked to terrorist organisations.

Across the cases reviewed, virtual assets play a central role in facilitating value transfer. Transactions frequently involved the rapid conversion of funds into stablecoins, the use of privacy-enhancing tools, and the movement of funds across multiple jurisdictions, often with limited transparency.

The underlying activity occurred between 2018 and 2025, with VA SARs filed between December 2024 and October 2025. The temporal gap between activity and reporting reflects the evolving nature of detection, including the identification of wallets and entities subsequently linked to terrorist financing through sanctions, seizure actions, and intelligence developments.

INTRODUCTION

Terrorist financing refers to the collection and movement of funds intended to support terrorist groups or activities. These funds may come from lawful or unlawful sources but are typically routed in ways designed to hide their origin, purpose, and final destination. This report brings together VA SAR data to identify common financing methods, behavioural indicators, and weaknesses in financial systems that are being exploited.

METHODOLOGY

The findings are based on VA SARs between December 2024 and October 2025 involving individuals and entities across multiple jurisdictions. Transaction analysis relied on blockchain analytics tools such as Chainalysis, alongside open-source intelligence, to trace wallet activity and identify exposure to known terrorist financing networks. Although the reporting window is limited, many of the transactions occurred years earlier. This allowed for retrospective analysis once wallets and networks were later designated or seized.

OVERVIEW OF TRANSACTION BEHAVIOUR

Based on the methodology outlined above, the following section summarises key transaction behaviours observed across the reviewed VA SARs:

- **Rapid movement of funds:** Funds are deposited in fiat or crypto, converted quickly into stablecoins, and withdrawn with minimal delay. Accounts do not retain balances for extended periods.

- **Limited trading activity:** Accounts do not exhibit characteristics of genuine trading behaviour, such as market engagement or attempts to generate returns. Instead, they function primarily as transit points for funds.
- **Use of multiple asset types:** BTC, USDT, XRP, TRX, and Monero are commonly used. Monero appears in cases where users appear to be deliberately reducing transaction traceability.

TYPES OF EXPOSURE IDENTIFIED

- **Direct exposure:** Funds are transferred directly to wallets publicly associated with terrorist financing campaigns or identified on seizure and sanctions lists.
- **Indirect exposure:** Funds are routed through one or more intermediary wallets or exchanges before reaching a flagged destination, increasing complexity and reducing transparency.

CONTEXTUAL RISK INDICATORS AND REFERENCES

The activity observed across the VA SARs frequently involved exposure to wallets or entities identified through seizure actions, sanctions frameworks, and law enforcement advisories. This included, for example, wallets identified in national seizure orders related to terrorist financing campaigns, as well as designations under international sanctions regimes such as the OFAC Specially Designated Nationals (SDN) List.

In some cases, transactions aligned with patterns highlighted in public advisories and typology reports issued by authorities such as FinCEN and the Financial Action Task Force (FATF), particularly in relation to the misuse of virtual assets for terrorist financing and illicit value transfer.

These references provide important context for identifying higher-risk activity, particularly where transaction behaviour is consistent with known typologies or involves interaction with flagged wallets and services.

KEY TERRORIST FINANCING TYPOLOGIES

DIRECT DONATIONS TO TERRORIST WALLETS

In the cases reviewed, funds were converted into virtual assets, primarily USDT, and transferred directly to wallet addresses publicly advertised as donation points for terrorist groups, including campaigns associated with Al-Qassam. Transactions were typically low in value and, in some instances, included references indicating charitable intent.

Common indicators included same-day conversion and withdrawal activity, donation-style transaction references, repeated low-value transfers, and transfers to wallets identified in seizure actions or listed under international sanctions regimes.

INDIRECT DONATIONS USING INTERMEDIARY WALLETS

Another observed method involved routing funds through one or more intermediary wallets before reaching a final destination linked to terrorist financing. In many cases, funds were transferred to a personal or unattributed wallet, then immediately forwarded onward in similar amounts and within short timeframes.

The consistency in amounts and timing suggested no meaningful change in ownership, with intermediary wallets used primarily to create distance between the originating account and the final recipient.

Common indicators included mirrored transaction amounts, minimal time gaps between successive transfers, repeated use of the same intermediary wallets, and rapid consolidation of funds into wallets associated with known terrorist financing clusters.

USE OF MSBs & EXCHANGE FRONTS TO MOVE VALUE

Several cases involved the movement of funds through wallets linked to money service businesses (MSBs) or nested exchanges used to facilitate cross-border value transfer. In some instances, these intermediaries were subsequently linked to seizure actions or sanctions designations, indicating their involvement in illicit financial activity.

The activity pattern suggested the use of such services as conduits for moving funds across jurisdictions, rather than for legitimate remittance or trading purposes.

Common indicators included repeated transfers to wallets associated with MSB or exchange clusters, the presence of small transaction amounts alongside larger passthrough volumes, and limited economic or commercial justification for the observed activity.

PEER-TO-PEER TRADING AS COVER

In some cases, users referenced peer-to-peer (P2P) trading platforms to explain rapid movement of funds and limited counterparty transparency. Supporting documentation was often weak, relying on screenshots or unverifiable information rather than formal KYC or transactional evidence.

The use of P2P explanations appeared, in some instances, inconsistent with the underlying transaction behaviour, particularly where funds were ultimately routed to higher-risk destinations.

Common indicators included vague or unsupported explanations of P2P activity, frequent platform hopping, and continued exposure to wallets associated with terrorist financing despite claims of legitimate trading. Frequent platform hopping may indicate attempts to obscure transaction trails, as the movement of funds incurs transaction fees that reduce the value of the funds.

USE OF PRIVACY AND ANONYMITY TOOLS

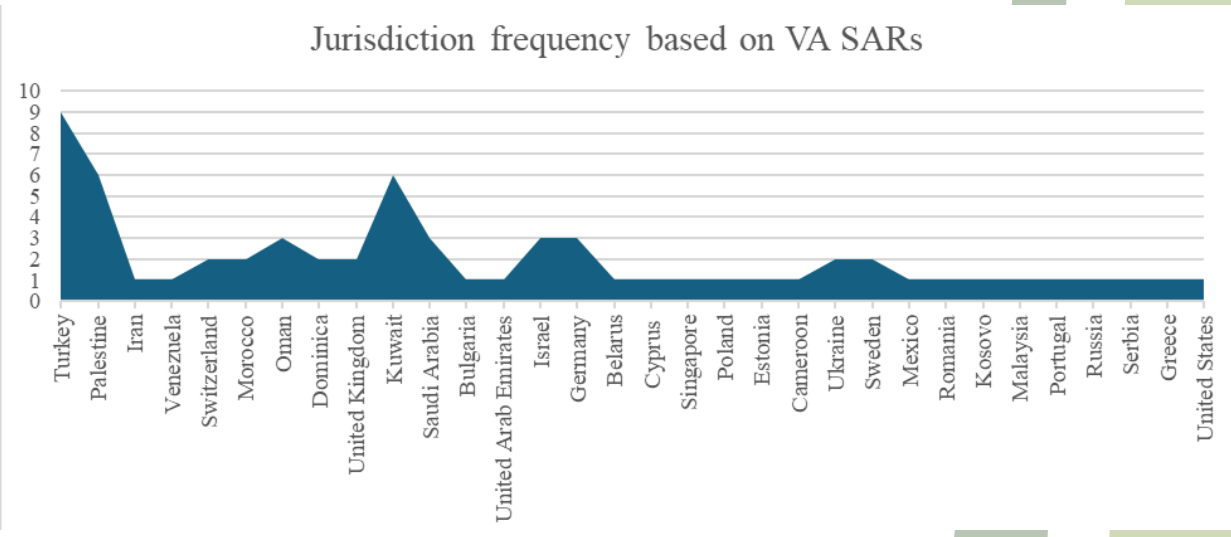
In several cases, users employed privacy-enhancing tools and anonymity-based platforms to obscure identity, location, and transaction traceability during the movement of funds. This behaviour appeared alongside rapid fund movement and limited transparency, suggesting an effort to reduce attribution and complicate detection.

Common indicators included:

- Use of VPNs or anonymised login methods to mask user location.
- Use of privacy-focused virtual assets, such as Monero, to reduce blockchain transparency.
- Interaction with non-KYC exchanges or platforms, offering anonymity and limited oversight.

GEOGRAPHIC CONCENTRATION (BASED ON VA SARS)

The table below presents the frequency of jurisdictions referenced across the reviewed VA SARs. Each count reflects the number of VA SARs in which a given jurisdiction appeared, either as the customer's location, or a destination linked to the suspicious activity.



This analysis provides additional context to the typologies identified above by highlighting recurring geographic patterns and cross-border transaction pathways observed across the reviewed VA SARs.

The distribution shows a clear concentration in a small number of jurisdictions. Turkey appears most frequently, followed by Palestine and Kuwait. These jurisdictions are commonly associated with cross-border payment corridors, informal value transfer systems, or proximity to known terrorist financing networks. Their higher frequency suggests repeated exposure rather than isolated incidents.

A second tier of jurisdictions, including Oman, Saudi Arabia, Israel, and Germany, appears with moderate frequency. These locations often function as regional financial hubs, transit points, or residence jurisdictions for account holders, rather than as final destinations for funds.

The remaining jurisdictions appear infrequently, often only once. These lower counts do not indicate lower risks on their own. Instead, they reflect the global and dispersed nature of the activity, where funds move through a wide range of countries to complicate tracing and attribution.

Overall, the table supports the typology findings that terrorist financing activity is not confined to a single region. Instead, it relies on cross-jurisdictional pathways that combine high-risk regions with established financial centers and low-visibility jurisdictions. The frequency analysis helps identify recurring geographic exposure while reinforcing the need for risk-based monitoring rather than jurisdiction-only screening.

SUPPORTING INDICATORS FROM VA SAR ANALYSIS

ACCOUNT PROFILES

The review of VA SARs identified several recurring account behaviours:

- **Individual accounts:** Frequently showed inconsistencies in KYC data, VPN use or anonymised access, and transaction volumes that did not align with the declared source of funds.
- **Corporate accounts:** In some instances, entities displayed activity consistent with informal financial intermediaries, including patterns resembling unregistered VASP operations.
- **Dormant accounts:** Several accounts remained dormant for extended periods before processing large volumes of transactions within a short timeframe.

USE OF CRYPTOCURRENCIES

The VA SARs referenced a range of virtual assets, with the following observed most frequently:

- **Bitcoin (BTC)** – used in both deposits and withdrawals, often linked to darknet marketplaces and seizure lists.
- **Tether (USDT)** – particularly on the Tron (TRX) blockchain, frequently used in transfers involving flagged or higher-risk addresses.
- **Ethereum (ETH)** – occasionally used in smaller transactions.
- **Litecoin (LTC)** – involved in multiple transfers, some flagged for suspicious flow-through activity.
- **Monero (XMR)** – observed in cases involving reduced transparency due to its privacy-enhancing features.
- **Tron (TRX)** – used both as a native asset and as the primary network for USDT transfers.
- **USD Coin (USDC)**, **Solana (SOL)** and **Arbitrum (ARB)** – identified in a limited number of transactions.

Across these assets, transactions often exhibited rapid deposit and withdrawal activity with minimal trading, consistent with layering or flow-through typologies.

USE OF FIAT CURRENCIES

The VA SARs also reflected the use of traditional fiat currencies as entry and exit points as follows:

- **US Dollar (USD)** – most frequently referenced, used in deposits, withdrawals, and transaction equivalents.
- **Euro (EUR)** – commonly observed in deposits and subsequent conversion into virtual assets such as USDT.
- **British Pound Sterling (GBP)** – identified in a smaller number of cases.

In several instances, fiat deposits were followed by rapid conversion into virtual assets, with limited economic rationale or trading activity, consistent with typologies involving movement rather than investment.

These observations support the identified typologies and provide additional context for recognising similar patterns in transaction monitoring and reporting.

COMMON RED FLAGS

The following indicators were frequently observed across the VA SARs reviewed:

- Use of VPNs or other anonymised access methods, which may obscure user location and complicate attribution.
- Transfers to or from wallets identified in seizure actions or listed under international sanctions regimes, including repeated interaction with such wallet addresses.
- Rapid movement of funds with minimal holding periods, including same-day deposit, conversion, and withdrawal activity without a clear economic rationale.
- Limited or no trading behaviour, where accounts function primarily as transit points rather than being used for investment or market activity.
- Use of privacy-enhancing tools, including privacy coins or interaction with non-KYC exchanges.
- Inconsistent, incomplete, or unverifiable KYC information, including discrepancies between declared customer profiles and observed transaction activity.
- Dormant accounts reactivated to process high transaction volumes within a short period.

These indicators should be considered in combination, as isolated occurrences may not independently indicate suspicious activity.

IMPLICATIONS AND CONSIDERATIONS

The typologies identified in the report highlight several areas where enhanced controls and analytical focus may assist in mitigating potential terrorist financing risks and reducing jurisdictional exposure.

ENHANCED RISK-BASED SUPERVISION OF VASPs

Enhanced risk-based supervision of VASPs by regulators may assist in identifying platforms exhibiting high volumes of rapid flow-through activity, stablecoin passthroughs, and limited trading behaviour. Review of business models against observed transaction patterns may support the identification of potential misalignment between stated activities and actual use.

TRANSACTION MONITORING FOR HIGH-RISK BEHAVIOUR

Strengthening transaction monitoring frameworks by VASPs, to identify behavioural patterns, rather than relying solely on transaction value thresholds, may improve detection. Relevant patterns include same-day deposit, conversion, and withdrawal activity, repeated small-value transfers, and the use of intermediary wallets that rapidly forward funds to higher-risk clusters.

USE OF PRIVACY-ENHANCING TOOLS

The presence of privacy coins, non-KYC exchanges, VPN usage, and anonymised access patterns may reduce transparency. Where such features appear alongside rapid flow-through activity or exposure to high-risk entities, further review by VASPs may assist in determining the underlying risk.

QUALITY OF VA SAR REPORTING

Clear and detailed SAR narratives from VASPs, including transaction flows, timing, value relationships, and any links to designated or seized wallets, may enhance the ability of competent authorities to identify systemic risks and emerging trends.

INFORMATION SHARING AND INTELLIGENCE USE

Leveraging blockchain analytics, open-source intelligence, and international cooperation mechanisms by the FIA may support the identification of cross-border activity and enable a more comprehensive understanding of emerging typologies.

SECTOR GUIDANCE AND OUTREACH

Ongoing engagement with the VASP sector by regulators, including the dissemination of typologies and red flag indicators, may assist in strengthening sector-wide awareness and reducing potential vulnerabilities.

BROADER IMPLICATIONS

The typologies highlighted herein may have broader implications for the BVI, particularly given the cross-border nature of virtual asset activity and the involvement of platforms operating within or from the BVI. Continued identification and monitoring of such patterns may assist competent authorities and reporting entities in mitigating potential exposure to higher-risk financial flows.

CONCLUSION

The typologies identified in this report demonstrate the evolving tactics used in terrorist financing, particularly through the use of virtual assets, privacy-enhancing tools, and cross-border platforms. These developments present increasing challenges for financial institutions, VASPs and competent authorities, particularly in terms of transparency, detection and attribution. The findings highlight the importance of enhanced monitoring, continued inter-agency collaboration, and the effective use of blockchain analytics in supporting the identification and disruption of illicit financial networks.

Date: 24th June, 2026


FINANCIAL INVESTIGATION AGENCY
VIRGIN ISLANDS
COMBATING FINANCIAL CRIME GLOBALLY