RISK GUIDE: Terrorist Financing

July 2026

The purpose of this guide is to inform and assists financial institutions in making informed decisions on strategies on detecting and understanding terrorist financing risks in Fiji.

Introduction

Terrorist financing (TF) risks are increasing globally, driven using new technologies, online platforms and diversified funding methods. In Fiji the overall terrorist risk is assessed as low, reflecting the absence of significant domestic terrorist activity and limited exposure to major terrorist network. However, there are existing vulnerabilities that could be exploited for terrorist financing purposes. This guide aims to raise awareness of terrorist financing risks in Fiji and to support financial institutions[1] and stakeholders in identifying, preventing and reporting suspicious activities in line with the findings from Fiji's 2025 National Risk Assessment (NRA) and 2024 Non-Profit Organization (NPO) risk assessment.

Financial institutions include designated non-financial businesses and professions such as legal practitioners, real estate agents and accountants. This term is used as defined in the Financial Transactions Reporting Act.

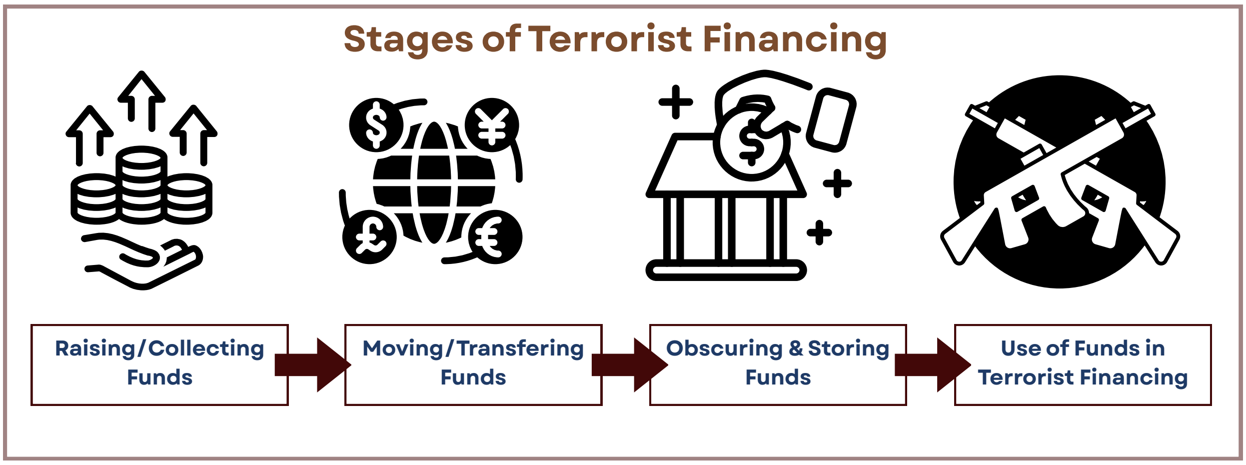
What is terrorist financing?

Terrorist financing is the provision or collection of funds, by any means directly or indirectly with the intention or knowledge that they will be used in full or in part to carry out terrorist acts, or by terrorist organization or an individual terrorist.[2]

Terrorist financing as illustrated by the image below is very linear, this means that money moves through a clear sequence. The money is raised or collected and generally moved through financial channels or intermediaries and then used to support terrorists' individuals, organizations and activities.

Two instrumental elements of terrorist financing are Non-Profit Organizations (NPOs) and crowd funding.

[1] Financial institutions include designated non-financial businesses and professions such as legal practitioners, real estate agents and accountants. This term is used as defined in the Financial Transactions Reporting Act.
[2] https://treaties.un.org/doc/db/terrorism/english-18-11.pdf



How can non-profit organizations be misused for Terrorist Financing?

Non-Profit Organizations (NPO)s can be misused through the following methods:

1. Exploitation of legitimate NPOs – this refers to the exploiting legitimate NPOs where donations are diverted for terrorist financing funding purposes.
2. Using sham NPOs – this refers to the setting up of sham NPOs to use as front organizations, or channel funds to support terrorist activities.

Terrorist organizations operate online platforms such as websites to seek direct financial contributions to support and indirectly through non-profitable organizations crowdfunding.

Crowdfunding is an innovative fundraising solution used by individuals to fund legitimate ideas, projects or business ventures, often under the guise of the operations of NPOs.[3]

Depending on the legal form of the NPO and the country, the NPO may often be subject to little or no governmental oversight (for example, registration, record keeping, reporting and monitoring) or few formalities may require for their creation. Terrorist organizations have taken advantage of these characteristics of NPOs to infiltrate the sector and misuse NPO funds and operations to cover for or support terrorist activity.[4] Weak oversight and high levels of public trust can increase these vulnerabilities.

What is Fiji's Terrorist Financing risk profile?

In Fiji, terrorist financing is addressed through a dual framework in which the Proceeds of Crime Act targets and confiscates assets linked to terrorist, while the Financial Transactions Reporting Act establishes preventive obligations to detect, report, and support the investigation of terrorist financing activities.

[3] *https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf*
[4] *https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R8-public-consultation-jun23.html*

Fiji's 2025 NRA assessed the overall terrorist financing risk for Fiji as low and stable. Internal TF threats for Fiji are considered low, with no active terrorist group or incidents reported in Fiji. Fiji faces medium threat from sympathisers in Fiji who may support terrorist organisations, ideologies, or affiliated individuals.

Fiji's diverse and multicultural population makes it vulnerable to global security threats. The country may also face threats from sympathisers and NPOs that raise funds for various international conflicts. Currently, active terrorist regions worldwide include ethe Middle East (e.g., Gaza), the Sahel region of sub-Saharan Africa, South Asia, and Southeast Asia.

How can the financial sectors be exploited for TF purposes?

As identified in the 2025 NRA, Fiji's financial sector was identified as having medium vulnerabilities to terrorist financing. Sectors that are inherently vulnerable to terrorist financing include banks, money remittances and payment services providers due to the cross-border transactions that they facilitate.[5]

Terrorism financing transactions are normally low-value and high frequency transactions that mix legitimate and illegitimate funds to avoid detection across multiple financial channels. Given that banks, money remitters and payment services providers provide these financial services there is a risk that they may be exploited either independently or collectively. The table below discusses how each of the mentioned sectors may be exploited for TF purposes with examples:

Sector	How can they be misused?	Examples
Banks	• Use of legitimate accounts to disguise activity • Complex transfers to hide original funds • Use of front organizations (e.g. Fake charities)	A group sets up a charity bank account, collects donations for 'humanitarian aid' and then transfers the funds abroad via wire transfers, where a portion is diverted to finance terrorist activities.
Remittance Service Providers	• Small frequent transfers to avoid detection • Use of intermediaries or fake receipts • Cross-border movement of funds to high-risk areas	An individual sends $200 multiple times through money transfer service to different people in another country. Those recipients then combine the funds and move it to a terrorist group avoiding suspicion by keeping each transfer small.

[5] *https://www.fijifiu.gov.fj/getattachment/Pages/Publications/National-Risk-Assessment-Reviews/Fiji%E2%80%99s-2025-NRA-Summary.pdf.aspx?lang=en-US*

Sector	How can they be misused?	Examples
Payment Service Providers	• Fasts digital transfers across sectors • Use of prepaid card and mobile wallets • Online fundraising through apps or platforms	A person creates several mobile wallet accounts and receives funds from supporters online. The funds are then quickly transferred between accounts and withdrawn in cash, making it difficult to trace the final recipient.
Combination of all 3 Sectors	• Same as mentioned in the 3 sections above.	A network collects small online donations through payment apps, transfers them via bank accounts to appear legitimate and then sends the funds through remittance services to individuals in another country who pass them on to a terrorist group.

Legal practitioners and real estate agents are not identified as highly vulnerable sectors to terrorist financing in Fiji, as noted in the 2025 NRA, however, they may still be exposed to potential misuse if appropriate safeguards are not in place.

Sector	How can they be misused?	Examples
Legal Practitioners	• Use of lawyer's trust account, to conduct transactions seem legitimate or hide their true source. • May set up companies, trusts, or foundations to hide ownership, or create shell entities without genuine business activity. • May structure deals in ways that reduce transparency, such as using nominees or intermediaries. • Lawyer-client privilege can limit what information authorities can access, which may be exploited to shield illicit activities.	• An individual places funds into a legal practitioner's client trust account under the pretext of a legitimate transaction, such as a property purchase. The lawyer subsequently transfers the funds to another account as part of the arrangement, thereby concealing their origin and facilitating their use for terrorist financing. • An individual engages a legal practitioner to establish a company or trust structure, presenting it as a legitimate business venture. The lawyer forms the entity without identifying the true beneficial owner. The company is then used to receive and transfer funds, hiding their origin and ultimately facilitating their use for terrorist financing.

Sector	How can they be misused?	Examples
Real Estate Agents	• This sector may be used for obscuring funds intended for use in TF through purchasing property with illicit funds. • Properties can be owned by companies or nominees instead of the real person, hiding involvement. • Frequent buying and selling to hide origin of funds.	An individual uses illegal money to buy a property through a real estate agent, making it look like a normal purchase. Because the transaction follows legal steps, such as contracts and registration, the money appears clean. This makes it harder to trace where the money originated from.

What are some other common indicators and red flags for terrorist financing?

Further to the above-mentioned points the following indicators may be linked to terrorist financing activities:

Indicators linked to the financial transactions

1. The use of funds by the non-profit organization is not consistent with the purpose for which it was established.
2. The transaction is not economically justified considering the account holder's business or profession.
3. Transactions which are inconsistent with the account's normal activity.
4. Deposits were structured below the reporting requirements to avoid detection.
5. Multiple cash deposits and withdrawals with suspicious references.
6. Frequent domestic and international ATM activity.
7. No businessrationale or economicjustification for the transaction.
8. Unusual cash activity related to bank accounts held abroad.
9. Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
10. Use of multiple, accounts held abroad.

Behavoral Indicators

1. The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
2. Use of false corporations, including shell-companies.
3. Listed in the ISIL (Da'esh) and Al Qaida (1267/1989/2253) list and the Taliban (1988) list.
4. Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.
5. Beneficial owner of the account not properly identified.
6. Use of nominees, trusts, family member or third-party accounts.
7. Use of false identification.
8. Abuse of non-profit organization.

Source: FIU Enforceable Guideline 1

Funds Transfers

1. A large number of incoming or outgoing funds transfers takes place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
2. Funds transfers are ordered in small amountsin an apparent effort to avoid triggering identification or reporting requirements.
3. Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
4. Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
5. Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.

Source: FIU Enforceable Guideline 1

What are Targeted Financial Sanctions?

The United Nations Security Council (UNSC) has imposed financial sanctions on persons and entities who have been identified by the UNSC (or relevant UN Committees) as contributing to a particular threat to, or breach of, international peace and security. These measures are referred to as "targeted financial sanctions" as they are financial sanctions aimed at designated persons or entities as opposed to a country.

Obligations of the Financial Institutions

Under the Public Order Act, financial institutions in Fiji (including legal practitioners, accountants and real estate agents) are required to, without delay:

1. immediately freeze and restrict access to any property, funds and accounts owned or controlled, directly or indirectly, by a sanctioned person or entity;
2. prohibit the provision of any transaction related to property or funds owned or controlled, directly or indirectly, by a sanctioned person or entity;
3. prohibit the provision of any property or any financial service, directly or indirectly, for the benefit of a sanctioned person or entity.

Financial institutions and DNFBPs must screen customers, beneficial owners, transactions and relevant parties against applicable UN and local designations and must freeze without delay where there is a confirmed match. Financial institutions and DNFBPs must report confirmed matches, frozen property, and attempted transactions involving a sanctioned person or entity to the Fiji Police Force through the FIU.

You may refer to the FIU website Targeted Financial Sanctions

UN Sanctions List
The UNSC Consolidated Sanctions List contains persons and entities designated by the UNSC under a range of sanctions regimes. For the purposes of Fiji's targeted financial sanctions obligations under Part 3B of the Public Order Act 1969, the relevant UN specified entities are those listed pursuant to UNSCRs 1267, 1988, 1540, 1718, 1737, 1989, 2253 and successor resolutions. For terrorism and terrorist financing, these include the ISIL (Da'esh) and Al-Qaida, Taliban sanctions list.

The relevant lists can be accessed through the Fiji Financial Intelligence Unit - UNSC - List of Designated Individuals and Entities webpage.

Local List
Under the Public Order Act, Fiji may also through the Courts, designate persons or entities who are linked to terrorist and terrorist financing for targeted financial sanctions. This is referred to as the Local List. There are currently no local designation of persons or entities for targeted financial sanctions.

More information can be accessed through the Fiji Financial Intelligence Unit - Fiji Sanctions - Local List webpage.

Conclusion
Although Fiji's overall TF risk is low, the vulnerabilities are medium. Fiji's financial system, instruments and process can be exploited by terrorist financiers under the guise of legitimate crowdfunding by NPOs.

Financial institutions and government agencies must remain highly vigilant to the terrorist financing risks posed by certain individuals, including those holding citizenship acquired through investment programs. Proactive risk identification, comprehensive verification procedures, and strong coordination between relevant agencies are critical to detecting and disrupting potential terrorist financing avenues and safeguarding Fiji's national security.

How to use this information?
- Share this information to improve awareness of these TF indicators.
- Use your internal reporting systems and procedures to identify and report on any TF related transaction or activity.

How to contact us?
Email: info@fijifiu.gov.fj; fijifiu-intel@rbf.gov.fj or fijifiu-compliance@rbf.gov.fj
Phone: (679) 322 3333
Website: www.fijifiu.gov.fj

Link for other financial crime guides and resources:
- Guides and Resources