



Australian Government

AUSTRAC

FIGHTING
FINANCIAL
CRIME
TOGETHER

Terrorism financing risks in Australia's non-profit organisation sector

May 2026



Contact us

Initial contact point

For enquiries about AUSTRAC, the legislation we administer or other information contact our Contact Centre, Monday to Friday, 8.30 am to 5.00 pm (AEST).

Phone: 1300 021 037 (local call cost within Australia)

Email: contact@austrac.gov.au

Translating and interpreting assistance

AUSTRAC provides free access to a translation and interpreting service to help people from diverse backgrounds to understand and meet their anti-money laundering and counter-terrorism financing (AML/CTF) obligations.

AUSTRAC uses TIS National, an interpreting service provided by the Department of Home Affairs, for people who don't speak English and English speakers who need to communicate with them.

To access the translation service, call during our Contact Centre operating hours on 131 450 and ask for 'AUSTRAC' on 1300 021 037. There is no charge for this service.

Deaf and speech-impaired callers

Callers who are deaf or have a hearing or speech impairment can contact AUSTRAC through the National Relay Service.

TTY (teletypewriter) or computer with modem users phone 133 677 and ask for 1300 021 037.

Speak and listen (speech-to-speech relay) users phone 1300 555 727 and ask for 1300 021 037.

Copyright

The Commonwealth owns the copyright in all material produced by this agency.

All material presented in this publication is provided under Creative Commons Attribution 4.0 International licence, with the exception of:

- the AUSTRAC logo
- content supplied by third parties.

The details of the relevant licence conditions are available on the Creative Commons website, as is the full legal code for the CC BY 4.0 licence.

You may not reproduce or use this material in any way that suggests AUSTRAC or the Commonwealth endorses you or any of your services or products.



Attribution

Material obtained from this publication is to be attributed to:

© AUSTRAC for the Commonwealth of Australia
2026

Contents

About this assessment	1
Methodology	2
Non-profit organisation sector in Australia	3
Higher-risk subset characteristics	5
Terrorism financing environment	6
Threats	8
Vulnerabilities	9
Consequences	10
Conclusion	12
Key terms	13

About this assessment

AUSTRAC is Australia's financial intelligence unit. We also regulate reporting entities under Australia's anti-money laundering and counter-terrorism financing (AML/CTF) and proliferation financing laws.

We work with the Australian Charities and Not-for-profits Commission (ACNC), the Australian Taxation Office (ATO) and other government partners to understand terrorism financing risks in Australia's non-profit sector.

The ACNC is Australia's national charity regulator. It regulates organisations that meet the legal definition of a charity, other registration requirements and choose to register. In most cases, an organisation must be registered with the ACNC to access Commonwealth charity tax exemptions and concessions administered by the ATO.

This assessment updates our understanding of terrorism financing threats, vulnerabilities and consequences linked to Australian non-profit organisations (NPOs). It is meant to help:

- NPOs understand where risks are most likely to occur
- financial institutions identify and manage higher-risk activity
- regulators and policymakers apply proportionate, risk-based responses.



This document is not a national risk assessment. It updates Australia's understanding of terrorism financing risks in the NPO sector. Read it alongside the:

- [*Terrorism financing in Australia national risk assessment 2024*](#) (2024 TF NRA)
- [*National risk assessment on Australia's non-profit organisation sector 2017*](#) (2017 NPO NRA).

This report also highlights changes since 2017, including shifts in visibility, common patterns (typologies) and operating characteristics linked to higher terrorism financing risk.

Methodology

We used a risk-based approach that's consistent with Financial Action Task Force (FATF) guidance. We reviewed a range of Australian and international information to understand terrorism financing risks in Australia's non-profit organisation (NPO) sector.

In this report, we assess risk by looking at terrorism financing threats, who might misuse funds and why. We also assessed vulnerabilities that could make misuse easier. Because controls aim to stop harm before it happens, we focus on situations where misuse could cause serious harm not just how often it may occur.

Data used

We analysed suspicious matter reports (SMRs) and other transaction reports collected by AUSTRAC between 2017 and 2025. We looked for common patterns (typologies), behavioural indicators and structural risk factors linked to NPO-related terrorism financing.

We considered this analysis alongside AUSTRAC's financial intelligence holdings. We also used information from Australian law enforcement and intelligence agencies, the ATO, the ACNC, along with open-source and academic research.

This assessment also uses international typologies, case studies and guidance from FATF member countries. These sources help place Australian findings in a wider context and test how relevant overseas patterns are to Australia. International material is not treated as evidence of risk on its own. Instead, it helps explore whether certain characteristics or behaviour could be relevant in the Australian context.

Advice from the ACNC and the ATO helped review the size, composition and regulatory coverage of the NPO sector. It also covered recent changes to reporting obligations for self-assessed income tax exempt NPOs. The new obligations require ABN-registered, non-charitable self-assessed income tax-exempt entities to submit an annual self-review return to the ATO. This change is expected to improve visibility for a sizeable portion of the NPO cohort.

Non-profit organisation sector in Australia

Australia's non-profit sector poses a limited terrorism financing risk overall. As with earlier national assessments, this report finds the risk is concentrated in a very small subset of non-profit organisations (NPOs). These organisations have higher exposure because of their activities, operating environment or structure.

Focusing on this higher-risk group supports proportionate, risk-based mitigation. This can be done without unduly affecting the vast majority of organisations that are operating legitimately.

Australia's non-profit sector is large and diverse. It includes charitable, religious, humanitarian, social and community-based groups operating here and overseas. Because organisations use different legal structures, operating models and regulatory arrangements, oversight is spread across multiple bodies. As a result, no single body has complete visibility of the whole sector.

This assessment estimates there are about 222,400 NPOs operating in Australia. This estimate is based on ATO and ACNC data and covers the organisations that are administratively visible in national datasets who are registered with an active Australian Business Number (ABN).

About 64,000 Australian NPOs (around 29%) are tax-concession charities. These organisations are registered with the ACNC and endorsed by the ATO for income tax exemption. Most other entities are non-charitable NPOs. These NPOs self-assess their income tax exempt status with the ATO. A smaller group of NPOs are taxable. Together, these groups form the core group over which national level regulatory and financial visibility exists.

Sector changes

A major change since the 2017 NPO NRA is the introduction of mandatory annual self-review reporting. This change applies to ABN-registered NPOs that self-assess as income tax exempt. From the 2023–2024 financial year, these NPOs must lodge a yearly not-for-profit self-review return with the ATO.

An entity that meets the legal definition of a charity under the *Charities Act 2013* but isn't registered as a charity with the ACNC cannot self-assess as income tax exempt. It's treated as taxable instead. Overall, this reform has improved regulatory visibility across a large segment of the sector.

However, official data does not capture informal or unregistered NPOs. This includes community groups and other common-interest groups that do not have an ABN. Groups that have not met registration or reporting requirements are also absent. The size of this part of the sector cannot be reliably calculated using available national datasets. As a result, the figures used here describe

only the administratively visible part of the NPO sector, not the full population. There are about 222,400 ABN-registered non-profit organisations.

Non-profit organisation sector analysis

<p>29%</p> <p>Endorsed tax-concession charities</p> <ul style="list-style-type: none"> – Registered with ACNC – Subject to governance obligations and reporting (with exemptions) 	<p>68%</p> <p>Self-assessed income tax exempt NPOs</p> <ul style="list-style-type: none"> – Non-charitable NPOs – New annual self-review reporting to ATO 	<p>3%</p> <p>Taxable NPOs</p> <ul style="list-style-type: none"> – Required to lodge income tax return
<p>Key changes since previous assessment</p> <ul style="list-style-type: none"> – ABN-registered, self-assessed income tax exempt NPOs must now lodge an annual self-review return with the ATO. – Improves coverage of approximately 68% of the NPO sector that was subject to static self-assessment. <p>Interpretation for terrorism financing risk</p> <ul style="list-style-type: none"> – The NPO sector is large and diverse. – Terrorism financing risk is concentrated to a very small subset. – Improved reporting enhances regulatory view and more accurate understanding of the sector's size and makeup. 		

Financial intelligence analysis shows that nearly all NPOs linked to credible terrorism financing related reporting were, or had previously been, ABN-registered legal entities. Some operate outside the ABN framework, but they were rarely seen in terrorism financing related reporting. This does not mean they have no risk. It indicates most of the risk we have detected sits with organisations that are already visible to regulators.

Recent ATO reforms have improved visibility over self-assessing NPOs for tax integrity. A more accurate picture of the sector's active population supports proportionate, risk-based oversight. With these improvements, regulatory attention – particularly from the ACNC – can be better focused on NPOs with greater exposure to terrorism financing. This can be achieved while supporting the many that are low risk.

Higher-risk subset characteristics

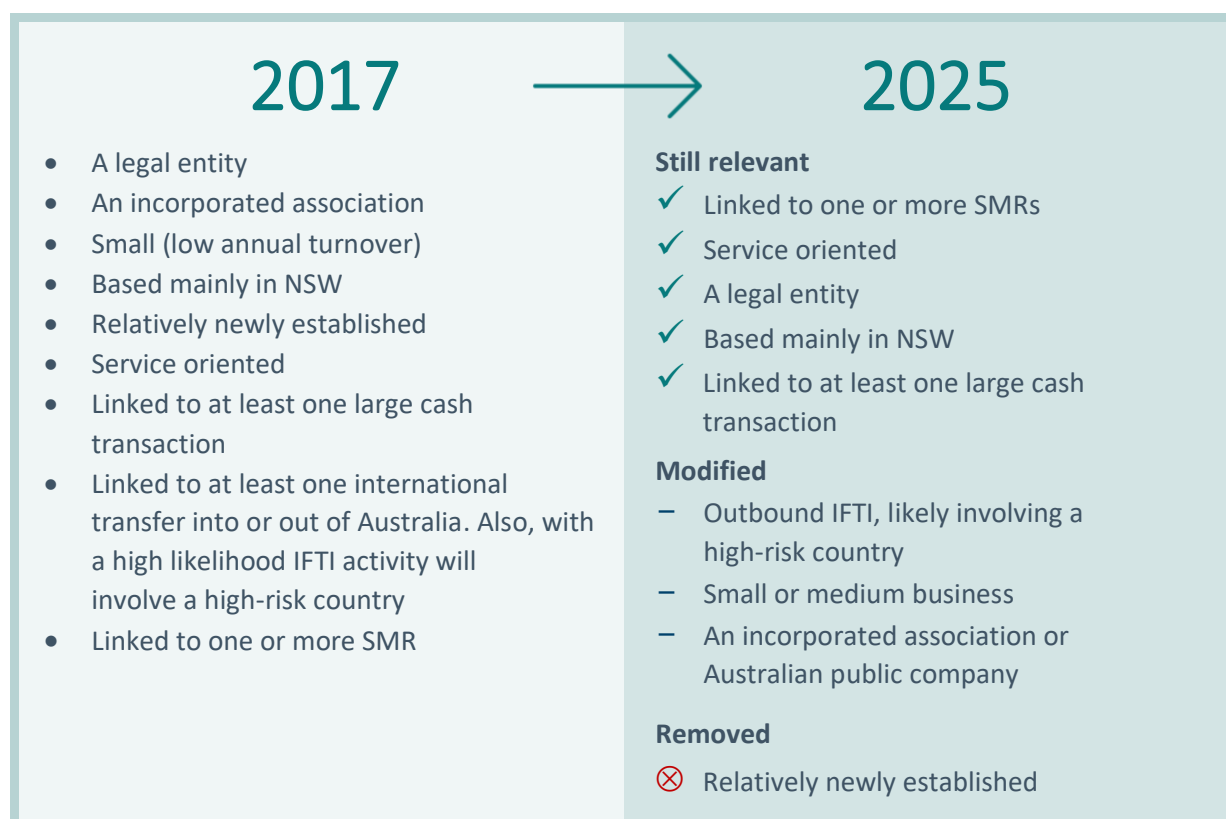
The characteristics in this section are risk signals. They are not proof terrorism financing is occurring. They help guide risk-based monitoring and regulation by highlighting situations where extra safeguards or closer review may be appropriate.

Most Australian NPOs still pose a limited terrorism financing risk.

Some characteristics that signal terrorism financing risk can be difficult to distinguish from normal operations of a legitimate NPO. This is especially the case for organisations working in conflict zones or other complex environments. This assessment aims to support risk management without unfairly affecting organisations that carry out lawful and essential charitable work.

AUSTRAC updated the higher-risk characteristics using analysis of NPOs linked to terrorism financing related financial intelligence. We compared them with the broader visible population to identify repeated structural, operational and transactional features. We then compared the results with the 2017 NPO NRA to confirm what remains relevant. We also used this information to identify characteristics that needed refining.

Most characteristics from the 2017 NPO NRA still apply and some have been refined. These updates reflect what we have observed in practice.



Modified characteristic changes

Small (low annual turnover)

- Since the 2017 NPO NRA, this review shows the combined higher-risk subset profile has shifted. It now reflects a stronger percentage distribution towards both small and medium-sized structures.

An incorporated association

- Since the 2017 NPO NRA, this review shows the combined higher-risk subset profile has shifted. It now reflects a stronger percentage distribution towards an incorporated association and Australian public company.

Linked to at least one international transfer into or out of Australia – with a high likelihood IFTI activity will involve a high-risk terrorism financing country:

- Outbound IFTIs to high-risk jurisdictions remain a relevant risk signal.
- Inbound international transfers are no longer a significant indicator in detected cases. As a result, they have been removed from the updated characteristics.

Removed characteristic

Relatively newly established

- Since the 2017 NPO NRA, most higher-risk NPOs show long-term legitimate activity, so this characteristic indicator no longer applies.

Terrorism financing environment

Since the 2017 NPO NRA, the global terrorism financing landscape has shifted. Large, organised fundraising networks are less common. Decentralised and fragmented financing models are now more typical. Groups such as al-Qa’ida and the Islamic State once relied on structured international fundraising networks, including exploiting NPOs, to move funds at scale. These groups have since weakened and their financial networks have declined.

Today, terrorism financing more often involves individual supporters or small groups. Funding is typically low value, with many relying on self-funding or small donations. This reduces, but does not remove, the appeal of using NPOs for fundraising.

Ongoing fund flows

Even so, NPO-linked fund flows connected to terrorism financing are likely to persist. Financial intelligence indicates observed and suspected cases continue to involve offshore transfers. Most often these are to conflict zones or other high-risk environments where terrorist groups are active. In some cases, transfers to high-risk jurisdictions may support violent extremists or designated terrorist organisations overseas.

SMRs that detect transfers to high-risk jurisdictions often describe humanitarian or religious reasons. They include aid, medical support or donations. This highlights how global conflict and instability continue to shape terrorism financing risk.

Financial intelligence indicates most NPO-related international funds movements use formal banking channels or registered remittance providers. Common patterns include raising funds in Australia, pooling them and then sending money offshore. This often happens through regulated online payment platforms or registered remittance providers. These channels provide the greatest visibility and create opportunities to detect and report suspicious activity. However, our visibility is lower for informal value transfer systems. Consistent with this reduced visibility, informal and cash-based methods rarely appeared in reporting.

Challenges for authorities

Detecting terrorism financing through NPOs remains difficult because suspicious activity can look like legitimate charitable work. This includes donations, religious contributions and emergency relief. Funds may come through small transfers, crowdfunding or salary-funded donations.

Visibility drops when funds go to conflict zones or complex environments. In these cases, reporting entities often note limited ability to verify who received the funds or how they were used.

Detection is harder when NPOs are part of wider charity networks or use intermediaries to send funds offshore. Complex structures, shared office holders and multiple partners can make fund flows harder to trace. The vast majority of NPOs have no obligations under the Act, so detection relies heavily on reporting entities identifying and reporting suspicious activity.

Online risks

Online fundraising platforms and digital payments are increasingly relevant to terrorism financing risks in the sector. Financial intelligence and international assessments show online appeals linked to charitable activity usually seek small donations and often use humanitarian or emergency-relief messaging. Social media, messaging apps and crowdfunding sites can spread these appeals quickly and reach large audiences.

Where online fundraising is linked to terrorism financing, it is most often observed as part of broader fundraising activity rather than a stand-alone method. In the NPO context, funds raised online typically still move through regulated payment channels, which provides some visibility. However, it can be difficult to understand donor intent or confirm end-use. This is especially the case when campaigns start quickly or when funds move through personal or intermediary accounts.

Although online fundraising often raises small amounts, the speed and volume of transactions can make detection harder. Once funds move offshore, they may be diverted or misused. This highlights the need for risk-based monitoring and early detection. This is particularly the case where fundraising relates to conflict zones or other complex environments.

A significant proportion of online fundraising occurs outside the sector. This includes legitimate ad hoc campaigns. It can also involve fake campaigns that use charitable or humanitarian messaging without being linked to a registered organisation. While these activities fall outside the scope of regulated activity, they can damage the reputation of legitimate NPOs and undermine public trust.

Threats

Funds diversion

Diversion of funds is one of the most common ways NPOs are abused in detected terrorism financing cases. Diversion can happen at different points, including during fundraising, while funds are held or when money is spent. It can also occur alongside legitimate charitable activity.

Financial intelligence indicates diversion often involves redirecting money raised for charity to people or groups linked to violent extremism. In some cases, funds are pooled in the organisation or intermediary accounts and then sent offshore or moved through personal or business accounts. People in trusted roles, such as office holders, staff or volunteers, who can influence financial decisions or access funds can enable money being diverted.

Links with terrorist organisations

In some cases, an organisation may have either a known or unknown association with a terrorist organisation, its supporters or an affiliated network. These links may come through personal, family or community ties. They may also occur through shared office holders, intermediaries or overseas partners.

Financial intelligence indicates these associations can also develop through partnerships in conflict zones or other complex environments. Where there is less transparency over a partner's governance or how funds will be used, the risk of indirect support increases.

At times, people who support extremist causes may try to exploit an NPO's legitimacy. They may present themselves as volunteers, donors or fundraisers. In these situations, they use the trust placed in the organisation to hide the ultimate destination or purpose of funds.

Abuse of legitimate work

NPO programs intended to deliver legitimate aid can be misused during delivery, especially in conflict zones or other complex environments. Supplies, equipment or services may be diverted to benefit terrorism groups operating in the area.

Financial intelligence indicates risk often increases after funds move offshore. At that point, NPOs may rely on local partners or intermediaries and visibility over who receives support is lower. In some locations, terrorist organisations may influence partner organisations, control access to communities or dictate who receives aid. These conditions increase the risk aid will be diverted.

Misuse can also occur through the logistical support needed to deliver programs, such as transport, storage or accommodation. Even when funds are raised for valid reasons, they can still support activity in areas under terrorist influence.

In many cases, terrorism financing misuse happens without the NPO's knowledge. This reflects the practical challenges of operating in unstable environments with limited oversight. Targeted, proportionate risk mitigation helps manage these challenges while protecting legitimate charitable activity.

Vulnerabilities

Financial intelligence shows some structural and operational features can increase an NPO's exposure to terrorism financing misuse. These vulnerabilities do not imply wrongdoing. They highlight conditions that terrorist actors may exploit in specific circumstances.

Regulatory framework gaps

Commonwealth, state and territory bodies share Australia's regulatory framework. The level of oversight depends on an organisation's structure, activities and location. As a result, different parts of the sector face varied:

- requirements
- levels of supervision
- reporting obligations.

This distributed framework can reduce consistent visibility across the sector and increases reliance on information sharing and coordination. While individual agencies oversee parts of the sector within their mandates, no single agency has end-to-end visibility of terrorism financing risk across the whole sector.

Self-assessment and oversight

Many organisations assess their own governance and internal controls, including those linked to financial risk. This supports proportionate regulation. However, it can also mean some NPOs do not receive regular, independent review of controls that may help prevent terrorism financing misuse.

Oversight is risk based and often depends on information supplied by NPOs or shared by other agencies. Reporting from AUSTRAC-regulated entities, such as banks and remitters, also helps identify potential terrorism financing concerns.

Regulation exemptions and reduced reporting

Some NPOs operate under exemptions that arise from charity and tax law frameworks. For example, some religious groups are exempt from specific governance and financial reporting requirements under the *Australian Charities and Not-for-profits Commission Act 2012*.

Exemptions from AML/CTF obligations apply only where money laundering and terrorism financing risk is assessed as low. The exemptions described here are not AML/CTF exemptions. However, lower baseline governance or reporting requirements under other regimes can reduce transparency.

Limited AML/CTF coverage

Most NPOs are not covered by the Act. This means they generally do not have obligations such as customer due diligence, transaction monitoring or submitting SMRs to AUSTRAC. As a result, reporting about potential terrorism financing involving NPOs largely depends on reports from entities regulated by AUSTRAC.

Working in higher-risk countries

Organisations that operate in conflict zones or other complex environments face higher exposure to terrorism financing misuse. In these locations, limited oversight, monitoring and verification can make it harder to assess local partners or confirm the end-use of funds.

Exposure can increase where partner jurisdictions have weaker counter-terrorism financing frameworks or limited enforcement capability. In practice, some NPOs may need to rely on intermediaries or local actors to reach people in need. This can increase the chance of diversion or misuse during program delivery.

Consequences

Impact on security

Funds that support terrorism, even indirectly, undermine counter-terrorism efforts in Australia and overseas. International examples show even small amounts can help support planning, travel, recruitment or other operational costs. For this reason, terrorism financing through NPOs is a high-impact risk, even when the total amount involved is low.

Impact on humanitarian outcomes

When funds are diverted or misused, legitimate NPOs may not be able to deliver vital services. Financial intelligence indicates where end-use cannot be confirmed, people in need may receive little or no help. This impact is greatest in conflict zones and complex environments, where communities may rely heavily on support and have few realistic alternatives.

Terrorism financing misuse in the sector can have serious consequences. Even small-scale financial support can strengthen terrorism groups and harm security, humanitarian outcomes and public trust.

Damage to public trust

Any real or suspected terrorism financing incident can damage the reputation of the organisation involved and the wider sector. It can reduce public trust and willingness to donate. International donors and partners may also lose confidence. These effects can continue even when the NPO did not intend or know about the misuse.

Impact on financial access

Concerns about terrorism financing can lead reporting entities, including financial institutions, to restrict or end services to NPOs. This may reduce the immediate risk for the financial institution, but it can create wider problems. Reduced access to banking or payment services can push some organisations towards informal channels. These channels have less visibility and can increase exposure to terrorism financing misuse.

In 2025, approximately 250 charities involved in overseas operations or international funds transfers participated in an ACNC survey on banking experiences. Some reported that account suspensions, closures or the cost and administrative difficulty of sending funds through traditional financial institutions, had prompted them to adopt workarounds, including the use of personal accounts, carrying cash or relying on other informal channels.

Together, these consequences can weaken the sector's resilience and limit the ability to deliver legitimate services. They can also make it harder to apply effective, proportionate, risk based counter-terrorism financing measures. Australia's approach recognises keeping legitimate NPOs within regulated financial channels is integral to counter-terrorism financing objectives. Managing terrorism financing risk is therefore essential for:

- security
- humanitarian goals
- financial inclusion
- public confidence.

Conclusion

Australia's NPO sector plays a vital role in delivering social, community and humanitarian services in Australia and overseas. This assessment confirms terrorism financing risk does not affect the whole sector evenly. Instead, it tends to arise in specific circumstances where certain activities, environments or structures increase exposure to misuse.

This assessment is based on available information. There are known gaps in coverage, including unregistered NPOs, and the limited application of AML/CTF obligations across the sector. This means the full extent of risk cannot be measured with certainty. Understanding where risk concentrates within the visible bounds helps avoid disrupting legitimate work, while focusing supervision and risk mitigation where it is most needed.

Detected cases of terrorism financing involving NPOs remain limited. However, even small or rare instances can have serious consequences. Terrorism financing is a high-impact threat because small amounts of diverted funds can strengthen terrorist groups. This can harm security, humanitarian outcomes and public trust. Risk is highest when:

- funds move offshore
- programs operate in conflict zones or other complex environments
- there's limited visibility over partners or end-use.

In recent years, Australian authorities have improved their understanding of terrorism financing risk involving NPOs. This draws on financial intelligence, regulatory information and international experience to identify where risk is most likely to arise. This improved understanding supports targeted and proportionate risk mitigation. It helps protect security while supporting the sector to continue its essential work.

Key terms

Charity	A non-profit organisation (NPO) that exists for charitable aims, as set out in common law and in the <i>Charities Act 2013</i> .
Consequence	The impact or harm that terrorism financing threats may cause if they eventuated.
Financial Action Task Force (FATF)	A global body that sets international standards for combating money laundering, terrorism financing and proliferation financing. FATF's standards guide countries' anti-money laundering and counter-terrorism financing frameworks.
International funds transfer instruction (IFTI)	An instruction to transfer funds or property into or out of Australia.
Non-profit organisation (NPO)	The term non-profit organisation in this document also applies to the 'not-for-profit' sector or entities. As defined by FATF, this is a legal person, arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other 'good works'.
Reporting entity	An entity that provides a designated service as defined in the <i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i> (the Act). This includes banks and remittance service providers.
Suspicious matter report (SMR)	A report that a reporting entity must submit to us under the Act. This is done when a reporting entity suspects a transaction may be linked to money laundering, terrorism financing, tax evasion, proceeds of crime or any other serious crime under Australian law.
Threat	A person or group of people with the potential to cause harm. This can be by raising, moving, storing or using funds or other assets for terrorism purposes.
Vulnerability	Characteristics or things that can be exploited by the threat or that may support or facilitate terrorism activities.



AUSTRAC.GOV.AU

