



Law Council
OF AUSTRALIA

National Legal Profession Anti-Money Laundering & Counter-Terrorism Financing Guidance

Guidance Note No 5 – What Does Terrorism Financing Look Like?

28 June 2024



National Legal Profession Anti-Money Laundering & Counter-Terrorism Financing Guidance

Guidance Note 5

What Does Terrorism Financing Look Like?

This Guidance Note describes the key features of terrorism financing.¹ It aims to help Australian legal practitioners to detect signs of terrorism financing to avoid unwitting facilitation of it.

What are the Features of Terrorism and Terrorism Financing in Australia?

Terrorism and terrorism financing are distinct but related behaviours. Planning an act of terrorism may involve illegal arms trafficking, training attackers, forging documents and paying bribes. All of these require money. Further, terrorists require housing, mobile phones, food, transport and family support. As such, terrorism financing can involve funds that support entire networks or involve very small sums for specific purchases. Funds that finance terrorism can appear to be used for daily, innocent purposes and can be unwittingly moved across borders by charities, educational institutions and unwitting professional advisers. Funds used for terrorism may originate from otherwise legitimate businesses or from criminal enterprise.

The Australian Transaction Reports and Analysis Centre (**AUSTRAC**) is currently updating its 2014 country-wide assessment of the threat of terrorism financing in Australia. Practitioners should consult this national threat assessment which AUSTRAC is expected to publish in 2024 on its website.

Sections 103.1 and 103.2 of the *Criminal Code Act 1995* (Cth) (**Criminal Code**) make it an offence to:

1. provide or collect funds, whether knowingly, or reckless as to whether the funds will be used to facilitate or engage in a terrorist act; or
2. intentionally make funds available to another person (or collect funds for them), knowing that, or being reckless as to whether, the person will use the funds to facilitate or engage in a terrorist act, and

in each case, the offence is committed even if the funds are not in fact used in a specific terrorist act, or even if a terrorist act does not occur.

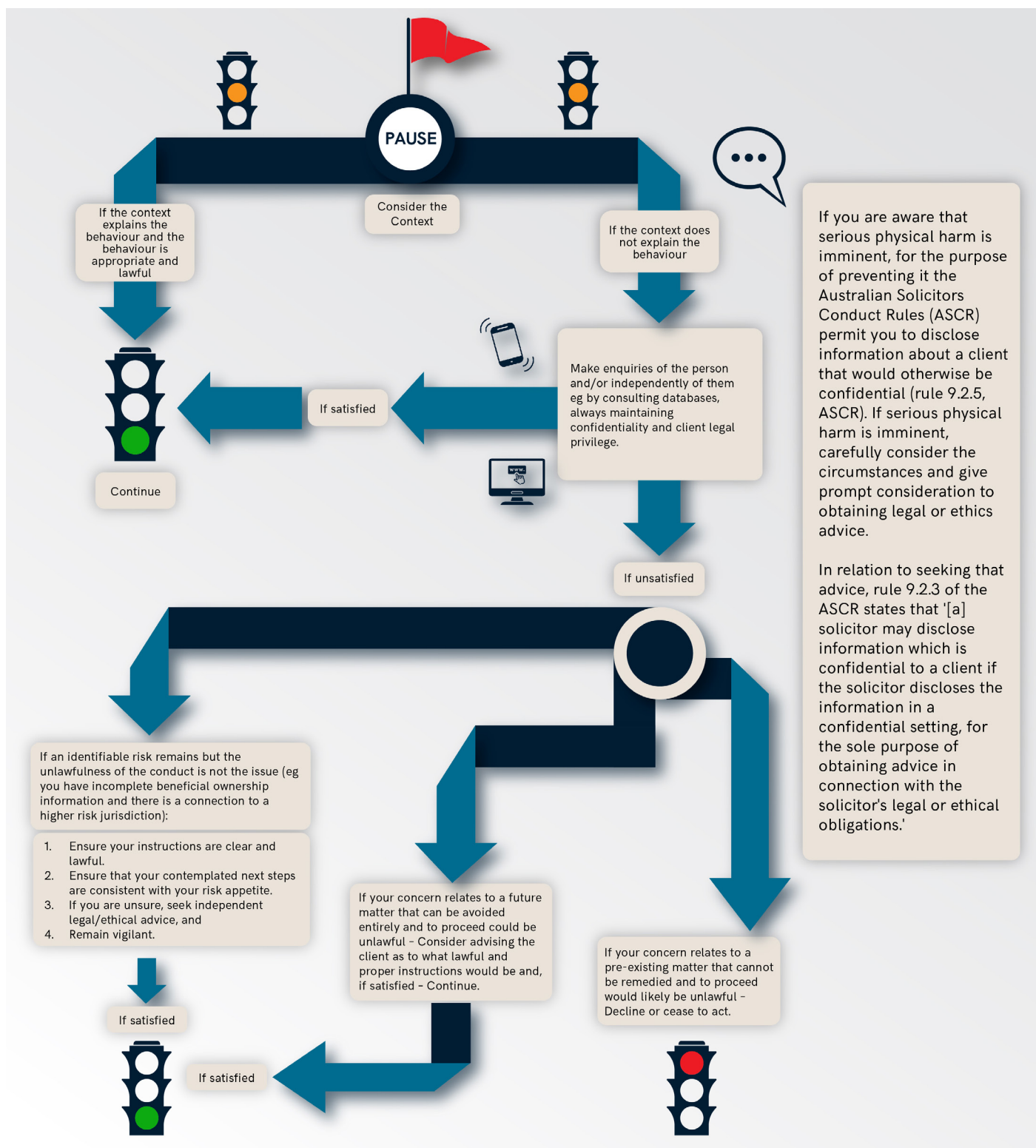
Division 101 of the Criminal Code also provides for a range of 'precursor' terrorism offences, including collecting or making documents likely to facilitate terrorist acts, and doing any 'other acts' in planning or preparation for a terrorist act. As above, recklessness as to the nature of the act is sufficient *mens rea*, and the planned terrorist act need not occur.

Red Flags

Many of the behaviours indicated in this Note will serve as 'red flags'. However, in a given context the behaviours described may not have any association with terrorism financing at all. Once noticed, a 'red flag' behaviour should act to alert a practitioner to the possibility that deception may be at work to disguise criminality. The steps to take are set out in a flow-chart on p 2. For a list of red flags for money laundering and terrorism financing, see *Red Flag List for Legal Practitioners*. For situations where representation is to be declined, see *Guidance Note No 11 - Ceasing or Declining to Act*.



What To Do When You Set a Red Flag – A Overview





Raising Funds

Terrorists are known to raise funds through legitimate sources and criminal activity and sometimes a mix of both. In the aftermath of the territorial defeat of the Islamic State of Iraq and the Levant (ISIL) in 2019, FATF reported that ISIL 'also generates funds from investments in small and medium sized businesses.'² In Australia, terrorist cells disrupted in Melbourne and Sydney in 2005 by a joint Australian Secret Intelligence Organisation-police operation, 'Operation Pendennis', accepted individual donations and also used the proceeds of credit card fraud, and stealing cars and selling their parts, to fund attacks.³

More recently, FATF has reported on the use of crowd-funding to raise money for terrorism, including via established platforms under the guise of appeals for social or humanitarian causes, using messaging apps, social media and virtual assets.⁴ This echoes the more 'traditional' misuse of charities whereby terrorists established sham organisations that were fronts for terrorist groups, or diverted funds through defrauding and infiltrating otherwise legitimate charities⁵ – a global method reported on by FATF and identified in Australia's 2014 national threat assessment as a potential channel for terrorism financing in Australia.

Moving Funds

As mentioned above, terrorists need funds for direct operational support as well as broader organisational needs. How do they move funds to the required destination? The methods include the formal and informal financial systems (alternative remittance services), cash couriers and charities or non-profit organisations.

Formal Financial System

An aim that those engaged in terrorism financing and money laundering have in common is disguising financial activity and hiding assets from law enforcement. The same red flags that pertain to money laundering apply to terrorism financing where the formal financial system is used. The presence of disguise and the active avoidance of cash reporting thresholds are matters to be alert to: see *Guidance Notes 3* and *4*.

Alternative Remittance Services

Alternative remittance services are informal banking systems usually operating across national borders. In Australia, remitters operate legally and are regulated under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth). As with the formal banking system, value is transferred quickly. Service types include account settlement mechanisms where value is released in one jurisdiction upon receipt of value by an agent in another jurisdiction. They also include *hawala*⁶ services which rely on transnational personal and familial associations. While *hawala* was used by terrorist organisation Al-Qaeda, it is also commonly used by migrant workers to remit money to home countries. The risks associated with these services arise from the fact that value is transferred along a chain that can involve many intermediaries and jurisdictions, including jurisdictions that are compromised by corruption and have other features of weak states. It may be that no one authority or organisation will know the true source of funds and there is ample opportunity for intermingling of funds.



Cash Couriers

Despite the availability of digital payment methods globally, the illicit drug trade continues to generate cash. Physical cash affords anonymity to terrorists and their supporters. The features of professional cash networks including the use of couriers are outlined in *Guidance Note No 4 – What Does Money Laundering Look Like?*

Charities or Non-Profit Organisations

Non-profit organisations in Australia's region are considered to be vulnerable to involvement in terrorism financing mainly as victims of misuse, rather than as fronts for terrorist groups. Charities can of course have a range of purposes, including educational purposes, advancing culture and social or public welfare, and they operate in all communities and throughout Australian society. Australian non-profit organisations that transact with high-risk countries may be particularly vulnerable to money being diverted to finance terrorism. The sector is cash-intensive and '[d]ue diligence and screening of personnel may also be a vulnerability NPOs need to address, as cases of terrorist infiltration and manipulation indicate,' according to AUSTRAC's most recent regional risk assessment for non-profit organisations.⁷

Example – Jemaah Islamiyah – sources of funds

The significance of various modes of terrorism financing is illustrated by resilience of Jemaah Islamiyah (JI) in the face of the arrest of its leaders and more than 300 of its members between 2018-2023 by Indonesian authorities. While the arrests have been major set-backs for the terrorist organisation, one of three major factors reportedly sustaining its operations is its access to funds. JI-affiliated charitable organisations are understood to use direct donations and charity boxes to fund the organisation, as well as excess operational budget from its network of educational institutions and 'taxes' from JI-affiliated businesses.⁸

Autonomous Sanctions

Practitioners should ensure that their clients are not the subject of sanctions.

Australia implements United Nations Security Council counter-terrorism sanctions. Under Australian law,⁹ a person or entity who commits, attempts to commit, participates in or facilitates the commission of terrorist acts can be 'designated' by Australia's Foreign Minister. It is an offence to deal with the assets of, or directly or indirectly make an asset available to, a designated person or entity.¹⁰ 'Dealing' with assets includes using, selling or moving assets. In limited circumstances a permit may be obtained from the Minister for Foreign Affairs to engage in an activity that would otherwise be prohibited by a sanction.¹¹

Practitioners with international clients should review the designated entities and persons by consulting this list:

- <https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list>



It is a serious criminal offence to contravene a sanctions measure (or a condition of a sanctions permit) and substantial fines and penalties of up to ten years' imprisonment can apply.

Terrorist Organisations Listed in Australia

Under Pt 5.3 Div 102 of the Criminal Code a regulation may specify an organisation to be a terrorist organisation for the purposes of Pt 5.3 ('Terrorism'). The 'National Security' webpage maintained by the Australian Federal Government names the listed organisations:

- <https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations>

At the time of publication there are 29 listed organisations ranging from ideologically based white supremacist groups to groups currently active in major conflicts abroad.

Terrorism Threat Level and Nature

At the time of publication the Australian Government rates the current terrorism threat level as 'possible' (see 'National Security' webpage) and indicates that the most likely present terrorist threat is an attack carried out by a lone actor or a small group. Despite the degraded capacity of offshore networks of violent extremists at the time of publication, the Government notes that the views of religiously motivated violent extremists continue to hold appeal for small numbers of people. While the underlying beliefs appear, then, to have a degree of persistent appeal, support for such networks has reportedly declined.

This is a partial summary of an ever-evolving area. Practitioners may consult websites such as [nationalsecurity.gov.au](https://www.nationalsecurity.gov.au) and [asio.gov.au](https://www.asio.gov.au) for up-to-date general threat information.

Investigative Measures That Restrict Terrorism Financing

As with money laundering, investigative measures are used to restrict terrorism financing. One of the main methods involves the use of financial transaction reporting and monitoring. This operates, first, by placing impediments in the way of those who seek to raise, accrue and move funds using the regulated financial sector and secondly, by enabling law enforcement and intelligence agencies to better follow financial trails.



References

1. The language of s 103.1 and s 103.2 of the *Criminal Code Act 1995* (Cth) distinguishes between financing terrorism and financing a terrorist. However, the term 'terrorism financing' is used in this Guidance Note for its breadth and for consistency with the *Anti-Money Laundering and Counter-Terrorism Act 2006* (Cth) (**AML/CTF Act**): see, for example, s 3(1)(ac) of the AML/CTF Act.
2. FATF, *Public Statement on the Financing of ISIL, Al Qaeda and Affiliates* (21 October 2021) <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Statement-isil-al-qaeda.html>.
3. *Benbrika v The Queen* (2010) 29 VR 593 at [19], [29].
4. For more information including risk indicators (Annex A) see FATF, *Crowdfunding for Terrorism Financing* (2023) <https://www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html>.
5. FATF, *Terrorist Financing* (2008) at 11-12, <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf.coredownload.inline.pdf>.
6. *Hawala* is an Arabic word for a particular trust or honour-based system for the transfer of funds that operates outside of conventional banking institutions. It uses agents who agree to receive funds and to ensure their remittance, often without money physically being received and sent but instead, with value being transmitted through balancing the ledgers of a *hawala* dealer's books. *Hawala* is believed to have originated in the eighth century in India and spread to other parts of South-East Asia and to the Middle East. It has persisted over time but also grown in modern times, particularly in weaker states. Dealers in Australia are considered to be remittance service providers and must register with AUSTRAC.
7. AUSTRAC, *Regional Risk Assessment: Non-Profit Organisations and Terrorism Financing* (2017) p 5 https://www.austrac.gov.au/sites/default/files/2019-06/regional-NPO-risk-assessment-WEB-READY_ss.pdf.
8. Alif Satria, *Understanding Jemaah Islamiyah's Organisational Resilience (2019-2022)*, 2 November 2023, International Centre for Counter-Terrorism <https://www.icct.nl/publication/understanding-jemaah-islamiyahs-organisational-resilience-2019-2022>.
9. *Autonomous Sanctions Act 2011* (Cth) and *Autonomous Sanctions Regulations 2011* (Cth).
10. <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/counter-terrorism-un-sc-1373-sanctions-regime>.
11. <https://www.dfat.gov.au/international-relations/security/sanctions/what-we-can-do-help/sanctions-permit>.

This Guidance Note was produced on 28 June 2024 and is current at the time of publication.