Australian Government
AUSTRAC

FIGHTING FINANCIAL CRIME TOGETHER

TERRORISM FINANCING IN AUSTRALIA

NATIONAL RISK ASSESSMENT

COPYRIGHT

This risk assessment is intended to provide a summary and general overview. It does not set out the comprehensive obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act), the Anti Money Laundering and Counter Terrorism Financing (Prescribed Foreign Countries) Regulations 2018 (AML/CTF Regulations) or the Anti Money Laundering and Counter Terrorism Financing Rules Instrument 2007 (No. 1) (AML/CTF Rules). It does not constitute nor should it be treated as legal advice or opinion.
The Commonwealth accepts no liability for any loss suffered as a result of reliance on this publication. AUSTRAC recommends that independent professional advice be sought.

CONTACT US

If you have questions about your AUSTRAC compliance obligations, or enquiries regarding the licence and any use of this report please email contact@austrac.gov.au or phone 1300 021 037 (within Australia).

AUSTRAC is committed to continual improvement and values your feedback on its products. We would appreciate notification of any outcomes associated with this report by contacting AUSTRAC at austrac.gov.au/contact-us/form.

CONTENTS

EXECUTIVE SUMMARY

Australia is committed to ensuring the country and its financial system are resilient in preventing the financing and support of terrorism nationally and overseas. Australia combats terrorism financing through a well-established, robust counter-terrorism financing (CTF) regime, which forms an important part of the country's national approach to countering terrorism and violent extremism in all forms.

The *Terrorism Financing in Australia National Risk Assessment* (the assessment) is an important contribution to Australia's CTF regime. It brings together insights from across Australia's national intelligence community, law enforcement and regulatory agencies, private sector stakeholders and international financial intelligence units (FIUs) to assess risk associated with the methods and channels used to finance and support terrorism activity. It also examines the international and domestic drivers that influence the Australian environment, and considers how Australia mitigates and combats terrorism financing activity and where improvements could be made.

AUSTRALIA'S TERRORISM FINANCING ENVIRONMENT

DOMESTIC TERRORISM THREAT

The number of violent extremists who have both the intention and capability to undertake terrorist attacks in Australia has decreased in recent years. However, violent extremists across the ideological and religious spectrums continue to connect and radicalise. Any terrorist attack is most likely to be conducted by a lone actor or a small group. These types of attacks are difficult to detect, and can occur with little to no warning.

SMALL SCALE AND LOW VALUE

Australia's terrorism financing environment is small scale and low value. Domestic terrorist attacks are infrequent and are usually committed by individuals, known as lone actors, who self-fund their activities and often lack a detectable financial element. When financing is evident, it usually involves the direct provision of a weapon or small amounts of cash by known associates to the offender.

OUTGOING FUNDS FLOWS

Australia is primarily an exporter of small-scale terrorism financing funds flows to offshore terrorist organisations and affiliated groups. Organisations assessed as most likely to receive funds or support from Australians include Islamic State, al-Qa'ida and both their respective affiliates; and Hamas and Hizballah to a lesser extent, although the Hamas-Israel conflict may change this trajectory. The scale of funds to support foreign fighter travel has decreased in line with fewer individuals participating in offshore conflicts. However, this could also change if increasing tensions in the Middle East draw Australian fighters to participate.

There is no evidence or intelligence base to suggest terrorism financing funds are flowing into or returning to Australia. One instance was identified in the review for this assessment that likely involved the movement of suspicious funds 'through' Australia. However, these types of funds flows are rarely detected and are likely uncommon. The scale of funds to support foreign fighter travel has decreased, in line with fewer individuals participating in offshore conflicts.

CONTINUED USE OF ESTABLISHED METHODS

Terrorists and their financiers largely continue to use the same established methods for raising funds. The use of personal funds and contributions from individual supporters, often under the guise of charitable giving, provide a viable revenue stream for both domestic and offshore funding. For violent extremists across the ideological and religious spectrums, the use of social media, communication, and crowdfunding platforms (the 'online funding ecosystem') have become integral to recruitment and fundraising activities. Terrorist financiers also continue to prefer readily available and proven methods to move funds, such as banking, remittance and exchange of cash, over complex schemes. An uptick in the use of digital currencies has been observed, but there is no evidence to suggest it will overtake more simple methods over the next three years.

DIFFICULT TO DETECT

Terrorism financing can be difficult to detect. Transactions conducted through regulated financial channels often mirror legitimate financial activity and do not raise suspicion. The increased speed of financial products in recent years has also made it harder for reporting entities to identify and freeze suspicious transfers before funds leave an account. Funds can also be raised or moved via less visible channels such as cash or unregistered remittance dealers.

IMPROVED CTF OPERATIONAL CAPABILITIES

Australia's CTF regime, operational capabilities and investigative outcomes nationally and in the Southeast Asia region have evolved substantially in recent years. Operational CTF working groups collaborate across government agencies and national boundaries to share intelligence and coordinate activities, and provide a significant toolkit for disrupting terrorism and terrorism financing actors.

Financial intelligence efforts continue to evolve from a largely reactive role in monitoring suspected violent extremists and supporting investigations, towards a proactive role in countering violent

extremism. The creation of the Fintel Alliance National Security Working Group[1] has enabled national security agencies and members of Australia's largest financial reporting institutions to share classified information in near-real time. This is a critical element in preventing and countering violent extremism given the sometimes rapid and unexpected escalation to acts of violence.

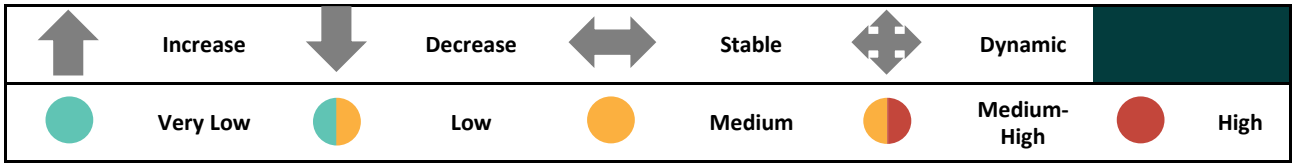
[1] The Fintel Alliance National Security Working Group builds on the success of the Fintel Alliance public-private partnership. Further details of the Working Group are provided on page 22.

SNAPSHOT OF INHERENT RISK RATINGS

Key risks identified in this assessment have been calibrated to Australia's terrorism financing environment, which is assessed as small scale and low value.

A **high** risk rating **does not** indicate the nature and extent of suspected misuse of the channel or method is significant. Instead, it indicates the channel or method is more likely to be used for terrorism financing, and it is generally exposed to a high level of inherent vulnerability to misuse.

LEGEND



RAISING FUNDS

CHANNEL/METHOD	SINCE 2016	RATING		OUTLOOK
		RMVE	IMVE	
Self-funding	↔	●	●	↔
Fundraising via social media, communication applications and crowdfunding platforms (includes purported charitable fundraising)	↑	●	●	↔
Registered charities and legitimate NPOs	✥	●	◑	✥
Membership fees for groups	*	-	●	↔
Fraud	↔	●	◑	↔
Legitimate and front businesses	↔	◑	◑	↔
Wealthy private donor in Australia	↔	◑	◑	↔
Wealthy private donor outside Australia	↔	◑	◑	↔
Superannuation funds	↓	◑	●	✥
Funding from offshore terrorist group	↔	●	●	↔
Kidnap-for-ransom payments	↔	●	●	↔
Crypto-jacking (theft of digital currency)	↔	●	●	↔
Cyber-extortion (e.g. ransomware)	↔	●	●	↔

*This was not assessed in the 2016 regional risk assessment.

MOVING FUNDS

CHANNEL/METHOD	SINCE 2016	RATING		OUTLOOK
		RMVE	IMVE	
Banking system*				
Remittance service providers				
Non-bank online payment service providers				
Digital currencies*				
Cash exchange (domestic)*				
Cash smuggling (offshore)				
Foreign exchange providers				
Luxury goods (e.g. jewellery, watches etc.)*				
Precious metal traders (e.g. gold bullion)				
Stored value cards				
Non-bank lenders and financiers				
Pubs and clubs				
Casinos, betting agencies and other gambling activities				
Stockbroker and securities dealers				

* These channels are also used to store terrorism financing funds. The intelligence picture on estimated amounts and duration of time that funds are stored before or after moving is unclear.

CONSEQUENCES

The overall consequences of terrorism financing in Australia are assessed as **low** to **moderate**.

RISK FACTORS			
	LOW	**MODERATE**	**HIGH**
IMPACT: USE OF FUNDS	Terrorism financing is more often used to support organisational costs such as propaganda, meetings and recruitment, salary payments to members, or payments to widows, orphans and families of dead fighters and terrorist actors.	Terrorism financing is evenly used for both organisational costs and operational expenses.	Terrorism financing is more often linked to a terrorist act or weapons, vehicle, explosives, equipment, training or other activity to prepare to undertake a terrorist act; foreign fighter travel to conflict zones; or sent directly (or indirectly) to recognised foreign terrorist groups.
POLITICAL AND SOCIAL HARM	Instances of terrorism financing are unlikely to erode trust and confidence in the Australian government; and are unlikely to cause high levels of social discord.	Instances of terrorism financing are likely to erode a moderate level of trust and confidence in the Australian government; and are likely to cause a moderate level of social discord.	Instances of terrorism financing are likely to erode a significant level of trust and confidence in the Australian government; and are likely to cause a significant level of social discord.
ECONOMIC HARM	Instances of terrorism financing do not erode Australia's financial performance or reputation, and do not affect the broader Australian financial system.	Instances of terrorism financing moderately erode Australia's financial performance or reputation, and somewhat affect the broader Australian financial system.	Instances of terrorism financing significantly erode Australia's financial performance or reputation, and significantly affect the broader Australian financial system.

INTRODUCTION

This assessment is an important tool in Australia's fight to detect and disrupt terrorism financing in all forms. It provides an intelligence base to better assist policy and operational responses to identified terrorism financing risks. The assessment also provides contextual guidance to reporting entities on the scale and impact of terrorism financing risks and aims to help businesses to continue improving their anti-money laundering and counter-terrorism financing (AML/CTF) programs and the reporting of terrorism financing activity to relevant authorities. A comprehensive assessment of terrorism financing risks and channels is also critical to implement the international standards for combatting terrorism financing set by the Financial Action Task Force (FATF).[2]

AUSTRAC has completed this assessment as Australia's Financial Intelligence Unit. AUSTRAC wishes to acknowledge and thank the following agencies and bodies for their important contributions to this project.

Attorney-General's Department
Australian Border Force
Australian Charities and Not-for-profits Commission
Australian Criminal Intelligence Commission
Australian Federal Police
Australian Security Intelligence Organisation
Australian Taxation Office
Commonwealth Director of Public Prosecutions
Department of Foreign Affairs and Trade
Department of Home Affairs
Fintel Alliance
Office of National Intelligence

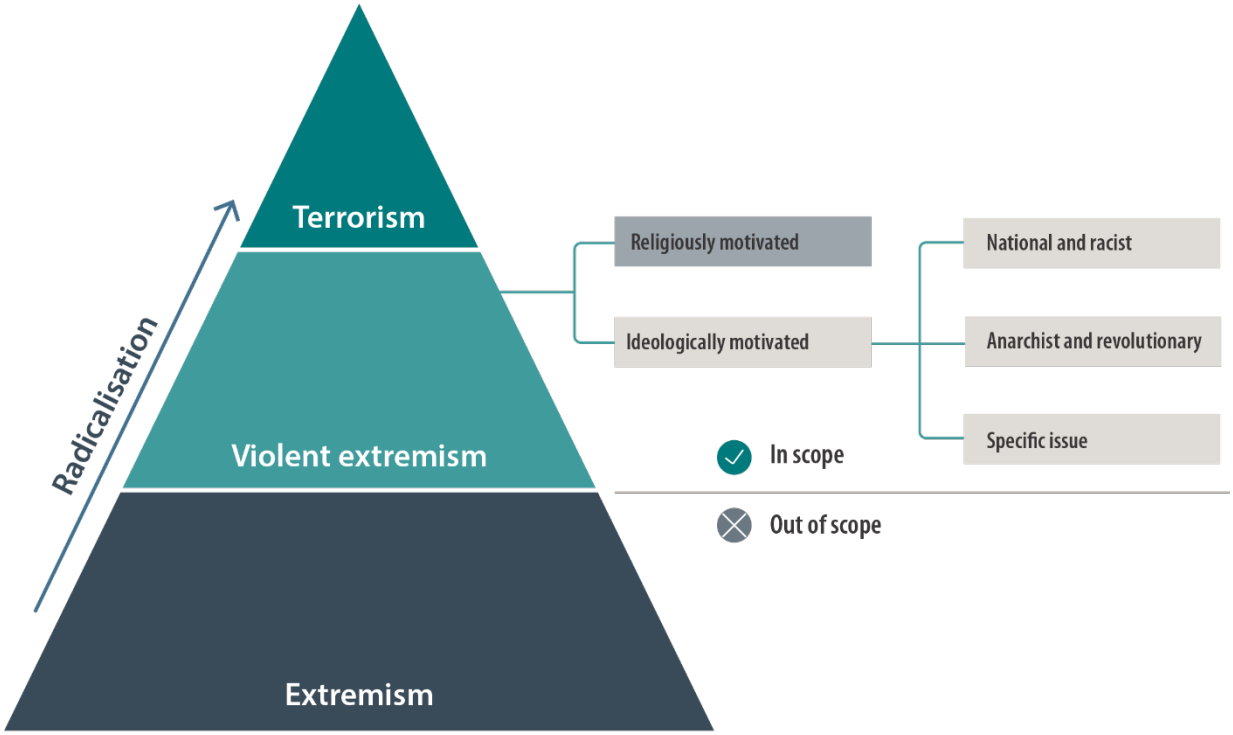
[2] The FATF Recommendations require countries to identify, assess and understand terrorism financing risks at a national level. These risks should be assessed on an ongoing basis and be kept up to date.

SCOPE

This assessment considers financing risks associated with all forms of violent extremism and acts of terrorism, regardless of whether the activity meets Australia's legal threshold for terrorism financing. The financing of non-violent forms of extremism are outside the scope of this assessment.

Escalation from violent extremism to an act of terrorism can be swift and difficult to predict or identify. It is therefore critical for authorities and reporting entities to understand financing risks and indicators associated with all forms of violent extremism.

DIAGRAM 1: FINANCING ACTIVITIES EXAMINED FOR THIS RISK ASSESSMENT



DEFINITIONS AND EXPLANATIONS

Extremism comes in different forms and scales of violence, which can range from holding or promoting extreme views to engaging in acts of terrorism.

EXTREMISM

Extremism refers to religious, social or political ideologies that exist substantially outside more broadly accepted belief systems in large parts of society, and are often seen as objectionable to large parts of society. Extremists may seek to radically change the nature of government, religion or society; or to create a community based on their ideology.

VIOLENT EXTREMISM

Violent extremism refers to support for violence to achieve social, political or legal outcomes or in response to specific political or social grievances. Australia uses two umbrella terms to describe violent extremism.

Religiously motivated violent extremism (RMVE) denotes support for violence to oppose or achieve a specific social, political or legal system based on religious interpretation. It is a faith-neutral term,

and may be applied to any violent extremist or terrorist act that is assessed by security and law enforcement agencies to have been inspired by a religion.

Ideologically motivated violent extremism (IMVE) denotes support for violence to achieve political outcomes or in response to specific political or social grievances. Motivations include nationalist and racist, anarchist and revolutionary, or a specific issue.

TERRORISM

Under Australian law, a terrorist act is defined in the *Criminal Code Act 1995* (the Criminal Code) and includes:

- Acts or threats of violence that are done to advance a political, ideological or religious cause, either in Australia or overseas.
- Acts or threats of violence intended to coerce or influence through intimidation a part of government, either in Australia or overseas.
- Acts or threats of violence that are done to intimidate the public or a section of the public.

TERRORISM FINANCING

Terrorism financing is defined in section 5 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act). In practical terms, it is a terrorism financing offence under the Criminal Code and the *Charter of the United Nations Act 1945* to provide funds to a terrorist organisation or individual, or to make an asset available to a person or entity who is subject to relevant sanctions.

The terrorism financing process generally involves three distinct stages:

1. Raising funds through donations, self-funding, legitimate business or criminal activity.
2. Moving funds to a terrorist network, organisation, cell or individual, or between such entities.
3. Using funds for direct (operational) and indirect (organisational) costs associated with terrorist activity.

Direct costs are required to fund terrorist attacks. Examples include expenses for travel, training, explosive materials, weapons and vehicles.

Indirect costs are required to maintain a terrorist network, organisation or cell, for example funds used to promote a group's ideology, fundraising events, living or legal expenses for members, or support for deceased members' family.

Funds also need to be stored during the terrorism financing process. Storage methods might include hiding cash, depositing funds in a bank account or maintaining some other financial product.

TERRORISM FINANCING OFFENCES AND RELATED LEGISLATION

The Criminal Code contains offences aimed at individuals who engage in, train or travel for, prepare, plan, finance or provide support for terrorist acts. In general terms:

- Division 102 includes offences relating to the finance, support or receipt of funds from a terrorist organisation. The maximum penalty is 25 years imprisonment.

- Division 103 includes offences relating to financing or supporting a terrorist or a terrorist act. The maximum penalty is imprisonment for life.

- Division 119 makes it is an offence for Australians to enter a foreign country with the intention to engage in hostile activity. It includes offences relating to the recruitment of, and provision of funds and support to, persons intending to enter a foreign country to engage in hostile activities in that country. Penalties range from 10 years imprisonment to imprisonment for life.[3]

In addition, individuals who are members or supporters of terrorist organisations proscribed by the Criminal Code or listed in the Criminal Code Regulations 2002 can be charged with a criminal offence.[4]

Australia implements United Nations Security Council (UNSC) sanctions relating to terrorism and terrorism financing into Australian law under the *Charter of the United Nations Act 1945,* and related subsequent legislation. Under sections 20 and 21 of the Charter of the United Nations Act 1945, it is an offence for a holder of freezable assets to use or deal with, allow dealings with, or facilitate the use of or dealing with that frozen asset; or make a frozen asset available to a designated person or entity. Further details of these sanctions frameworks are provided in the next section of this report.

The *Suppression of the Financing of Terrorism Act 2002* amended a number of existing acts to implement Australia's obligations under the United Nations Suppression of the Financing of Terrorism Convention and relevant UNSC Resolutions.

Regulation 4A of the *Customs (Prohibited Import) Regulations 1956* prohibits the importation of objectionable goods including films, publications and other goods that are objectionable material. This includes materials that promote, incite or instruct in matters of crime or violence, and advocate the doing of a terrorist act.

[3] On 1 December 2014 the *Crimes (Foreign Incursions and Recruitment) Act 1978* was repealed and foreign incursions and recruitment offences were relocated to Division 119 of the Criminal Code. While it is no longer in force, the *Crimes (Foreign Incursions and Recruitment) Act 1978* applies to and is used for relevant historical offences.

[4] As of October 2023, Australia has listed 29 organisations as terrorist organisations under the Criminal Code. These organisations and their date of listing can be found on the Australian National Security website nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations/islamic-state-khorasan-province.

METHODOLOGY

This assessment employs the standard risk framework (likelihood x consequence = risk) and international best practice and guidance on terrorism financing risk assessments as a general guide. For this assessment, *inherent* risk ratings are assigned to channels and methods based on an assessment of likelihood (threat x vulnerability) only. This includes an assessment of the likely current to near-term trajectory (next three years) of each risk factor. This approach will help AUSTRAC monitor and track changes in the risk environment.

Consequences of terrorism financing are assessed, but estimates are made at the national level only. Accurately estimating the level of consequence for each channel/method is problematic. There is insufficient contextual data, given Australia's very small-scale and low-value terrorism financing environment and limited visibility of how funds are used once they are moved offshore.

RISK MODEL

	RISK FACTORS
LIKELIHOOD A combined assessment of the threat of terrorists and terrorist financiers using a particular channel or method, and the vulnerability of the channel/method to misuse.	**Threat** refers to the estimated extent of misuse of a channel or method for terrorism financing, based on known and suspected cases investigated by Australian authorities. Threat is estimated based on the following factors or indicators. • Use of the methodology by terrorists or their financiers. • The capability (the size of the network and specialist capability) and intent of the individual or groups to carry out the methodology. • General security environment – are groups who typically use this method currently active? **Vulnerability** refers to factors that may facilitate, enable or be exploited for the purpose of terrorism financing. It includes regulated and unregulated financial channels, as well as national vulnerabilities such as Australia's AML/CTF framework. Vulnerability is estimated based on the following factors: • *Profitability* - the volume of funds that can be raised, moved and/or stored through the channel • *Accessibility* - the cost of a channel or other barriers to access, for example getting funds to a higher-risk region • *Ease of use* - the level of expertise or technical skills required to use a particular channel • *Detection* - reporting entities' visibility of terrorism financing through the channel and measures to report misuse to authorities • *Disruption* - the ability of AUSTRAC and law enforcement authorities to triage and investigate instances of terrorism financing through the channel.
CONSEQUENCE An assessment of the level of impact or harm caused by terrorism financing events.	**Consequence** is estimated based on the following factors: • How funds are used – operational expenses, which generally pose greater immediate harm – organisational costs, which generally pose lower immediate harm, but can ultimately help fund greater capability and resilience of a terrorist organisation. • Observed levels of perceived or real harm to the Australian government, national economy or society caused by the presence of terrorism financing.
OUTLOOK An assessment of the risk for the next three years.	A risk may be assessed as likely to 'increase' or 'decrease', usually based on known and evident drivers. A risk may be assessed as 'dynamic' if it is likely to change, but the trajectory is undetermined and largely dependent on external drivers. Risks that are likely to remain unchanged are considered 'stable'.

ASSESSING AND RATING RISK

A likelihood matrix was developed to assess and rate terrorism financing risk associated with 79 individual channels, methods and mechanisms across two dimensions: one for RMVE actors and one for IMVE actors. This approach recognises the different threat environments posed by each cohort. A matrix was also developed to assess and rate the level of consequence associated with instances of terrorism financing. Please refer to **Appendix A** for details of both matrices and an explanation of how risk scores were achieved.

Final risk assessments were weighted as follows: very low, low, medium, medium-high and high. Conditional risk statements are provided in the below table.

CONDITIONAL RISK STATEMENTS

CONDITIONAL RISK STATEMENT		
	High	Risk requires ongoing attention. The channel/method is often used in cases of terrorism financing, and there are many barriers to detecting and disrupting criminal actors.
	Medium-high	Risk requires further assessment. The channel/method is sometimes used in cases of terrorism financing, and there are barriers to detecting and disrupting criminal actors.
	Medium	Risk requires monitoring and may require further assessment. The channel/method might be used for terrorism financing, and there are some barriers to detecting and disrupting criminal actors.
	Low	Risk is acceptable but may require monitoring. There is limited evidence the channel/method is used for terrorism financing, but inherent vulnerabilities could be exploited by criminal actors.
	Very low	Risk is acceptable and does not require monitoring. There is very limited or no evidence the channel/method is used for terrorism financing.

INFORMATION SOURCES

This assessment draws on a range of intelligence and data inputs including:

- A formal request for information and/or survey to partner agency stakeholders, as well as state and territory non-profit organisations (NPO) regulators.
- Survey responses provided by 111 reporting entities and industry representatives.
- Survey responses provided by 35 international FIU partners.
- A comprehensive review of terrorism-related prosecutions.
- Financial transaction reporting to AUSTRAC.
- Financial, criminal and national security intelligence holdings.
- International reporting on terrorism financing trends.
- Feedback and professional insights offered during interviews and consultation with key stakeholders.

VALIDATION OF RESULTS

To ensure accuracy of the risk ratings and key findings, AUSTRAC developed this assessment in close consultation with the key contributors noted on page 8. This included engagement across three main stages of the project:

1. Collection: stakeholders completed a terrorism financing risk perception survey, questionnaire and/or a formal request for information.
2. Analysis: AUSTRAC collated all collection responses and held a first validation workshop to develop draft risk ratings. Draft risk ratings were provided to relevant contributors for review and feedback. AUSTRAC reviewed the feedback and held a second validation workshop, and final risk ratings were developed.
3. Review: a consultative draft of the final assessment was provided to all contributors for review, feedback and (where appropriate) final endorsement.

AUSTRALIA'S COUNTER-TERRORISM FINANCING REGIME

Australia has a well-established, robust CTF regime which forms an important part of the country's national approach to countering terrorism and violent extremism in all forms. The CTF regime is a multifaceted and cooperative effort across law enforcement, national security, regulatory, intelligence and policy agencies; as well as industry, international partners and the broader community. It enables the timely and effective investigation, disruption, prosecution and sanctioning of terrorist and terrorist financing offenders. The regime also enables Australia to identify and designate terrorists, terrorist organisations, and terrorist support networks.

INTERNATIONAL CONTEXT

Australia's AML/CTF regime is based on international standards developed by the Financial Action Task Force (FATF). Australia is a founding member of the FATF, which was established in 1989. In 2001, its mandate was extended to countering terrorism financing following the terrorist attacks in the United States of America (USA). FATF is the major inter-jurisdictional body for setting AML/CTF standards known as the FATF Recommendations, and has established a peer review process, known as 'mutual evaluations'. These are undertaken by member countries to assess the effectiveness and compliance of the assessed country's measures to combat money laundering, terrorism financing and proliferation financing.

The FATF Recommendations and its mutual evaluations of Australia have been major catalysts for enhancements to Australia's AML/CTF regime since 2003. Most recently this involved a comprehensive statutory review of the AML/CTF Act and associated Rules and Regulations in 2016. The review report takes into account the outcomes of the 2015 FATF mutual evaluation of Australia and made a range of recommendations to modernise and strengthen the AML/CTF regime. These recommendations are being implemented in phases.

Australia is a signatory to various international treaties that seek to address terrorism and disrupt its sources of funding, including the United Nations Suppression of the Financing of Terrorism Convention.

As a member of the United Nations, Australia implements UNSC *Resolution 1373* through the Charter of the United Nations Act 1945. UNSC Resolution 1373 is a global commitment to suppress terrorism by implementing targeted financial sanctions in relation to persons or entities involved in terrorist activities.[5] Australia has also implemented the UNSC *ISIL (Da'esh) and al-Qa'ida sanctions framework* (UNSC Resolution 1989 and successor resolutions).

The Australian Government is committed to working with foreign partners to share intelligence and strengthen domestic, regional and global resistance against terrorism financing threats. This engagement is facilitated by various multilateral and bilateral agreements that the Australian Government has in place through its agencies.

Regional and international co-operation and engagement is channelled through:

- Intelligence exchange and requests for information including for mutual legal assistance and extradition with foreign counterpart agencies.
- Regional capacity building in Southeast Asia, South Asia, the Pacific, the Middle East and Africa.
- Active involvement in key international forums including the United Nations, the Association of Southeast Asian Nations (ASEAN), the ASEAN Regional Forum, the East Asia Summit, FATF, the Egmont Group of FIUs, the Asia/Pacific Group on Money Laundering, and the Global Coalition to Fight Financial Crime.

COUNTERING TERRORISM FINANCING IN THE REGION

Australia is a leading member of a regional network of FIUs in Southeast Asia with a strong CTF focus. In 2015, AUSTRAC and PPATK (Indonesia's FIU) established the CTF Summit with four other Southeast Asian FIUs to foster closer operational cooperation and in response to the revival in regional terror groups coinciding with the rise of Islamic State. The CTF Summit assessed regional terrorism financing risks, including assessments on NPOs and cross-border cash couriering, and conducted joint analyst projects on regional terrorism financing networks. It has evolved to include the FIUs of all ASEAN members, New Zealand, and observer countries being Japan and the Cook Islands. It now operates as the Financial Intelligence Consultative Group (FICG).

The FICG facilitates the Southeast Asia Counter-Terrorism Financing Working Group (SEA CTFWG). The SEA CTFWG provides practical mechanisms for FIUs to progress strategic priorities and coordinate operational work in the region. A recent notable outcome was the designation of high-risk NPOs for terrorism financing-related targeted financial sanctions. The FICG has also built a secure technology platform to enable closer virtual collaboration and intelligence sharing among members.

[5] As of September 2023, 35 persons and 48 entities are designated by Australia under UNSC Resolution 1373. A 'designated' person or entity is placed on Australia's Consolidated List and referred to as 'listed'. Listed persons and entities are subject to targeted financial sanctions, and listed persons may also be subject to travel bans. These listings are a key tool in combatting terrorism financing. The interagency and international co-operation that go into supporting these listings is a strength of Australia's CTF regime. The Consolidated List is available at dfat.gov.au/international-relations/security/sanctions/consolidated-list.

DOMESTIC CONTEXT

AML/CTF LEGISLATIVE FRAMEWORK

Australia's AML/CTF legislative framework comprises:

- the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act)
- the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (AML/CTF Rules)
- the *Anti-Money Laundering and Counter-Terrorism Financing (Prescribed Foreign Countries) Regulations 2018*
- the *Financial Transaction Reports Act 1988* (FTR Act).

The AML/CTF Act focuses on regulating businesses that provide a range of services known as designated services.[6] Businesses that provide designated services are known as reporting entities. Reporting entities must comply with obligations under the AML/CTF legislative regime. There are currently approximately 17,000 reporting entities enrolled with AUSTRAC.

The FTR Act imposes several obligations on cash dealers. These include the requirement to verify the identities of account holders and report cash transactions of $10,000 or more and suspicious transactions to AUSTRAC. Solicitors must report cash transactions of $10,000 or more.

A statutory review of the AML/CTF regime was completed in 2016. The review made a number of recommendations to strengthen and simplify Australia's AML/CTF legislative framework. These recommendations are being implemented in phases.

The Australian Government is currently developing legislation for the most substantial phase of proposed reforms. These reforms will aim to simplify and modernise the regime in line with international standards and best practice. The proposed reforms would also extend AML/CTF regulation to additional services that are recognised globally as posing high ML/TF risks. These include certain services provided by businesses such as lawyers, accountants, trust and company service providers, real estate agents, property developers and dealers in precious metals and precious stones. If enacted, these reforms will significantly increase the number of entities reporting to AUSTRAC and bring Australia in line with other FATF member countries.

[6] Designated services are defined in section 6 of the AML/CTF Act and include financial services, including remittance and digital currency exchange, gambling, and bullion dealing.

NATIONAL CTF COORDINATION MECHANISMS

Australia's CTF regime forms an important part of the national counter-terrorism strategy. It is coordinated through broader counter-terrorism coordinating bodies and led by the Australia-New Zealand Counter-Terrorism Committee (ANZCTC).

The ANZCTC is the primary and most senior forum for developing and managing national counter-terrorism coordination strategies, plans and capability. It comprises senior official representatives from Commonwealth agencies, state and territory law enforcement, first minister departments and New Zealand counterparts.

The Department of Home Affairs (Home Affairs), leads domestic coordination and policy development in relation to a wide range of activities relevant to combatting terrorism and terrorism financing. This includes: national security, counter terrorism, cyber security, countering foreign interference, critical infrastructure protection, countering violent extremism programs, transport security, emergency management, multicultural affairs, and immigration and border-related functions.

The Commonwealth Counter-Terrorism Coordinator, through the Counter-Terrorism Coordination Centre (CTCC), provides national coordination and policy leadership to counter terrorism, and prevents and counters violent extremism in Australia. The CTCC advises on the full spectrum of counter-terrorism issues from challenging extremist ideologies through to effective response and recovery in the event of a terrorist attack.

The Ambassador for Counter-Terrorism, within the Department of Foreign Affairs and Trade (DFAT), has a leading role in Australia's international counter-terrorism engagement. This includes the negotiation of Australia's counter-terrorism partnerships, arrangements and agreements with partner countries. Further, the Ambassador ensures harmonisation of Australia's capacity building activities; provides foreign policy advice related to the management of Australia's counter-terrorism interests offshore; and advises the Foreign Minister regarding the listing of persons and entities for counter-terrorism financial sanctions in accordance with Australia's international obligations.

The Ambassador works with international partners to shape the global counter-terrorism environment, leverage Australia's counter-terrorism engagement in support of its national interests more broadly, and advises domestic stakeholders on the international counter-terrorism landscape and international best practice.

OPERATIONAL CTF FRAMEWORK

The following are the main Commonwealth agencies, authorities and bodies responsible for formulating and implementing Australia's CTF regime:

- The **Attorney-General's Department** has administrative responsibility for most of Australia's counter-terrorism and CTF laws.
- **AUSTRAC** is Australia's AML/CTF regulator and FIU. AUSTRAC provides specialist financial analysis capabilities to help protect Australia from terrorism and terrorism financing activities.
- The **Australian Border Force** monitors and detects the illegal movement of people, goods, and illicit cash across the border. It also administers border controls on a range of goods, including UN-sanctioned goods, to prevent activities that may contribute to terrorism.
- The **Australian Charities and Not-for-profits Commission (ACNC)** provides guidance to charities to help identify and mitigate exposure to terrorism financing risks for activities both in Australia and overseas. It monitors and manages non-compliance with a range of obligations, including governance arrangements, financial reporting and record keeping.
- The **Australian Criminal Intelligence Commission (ACIC)** is Australia's national criminal intelligence agency. The ACIC works with state and territory, national and international

partners on investigations and collects intelligence to improve the national ability to respond to crime impacting Australia.

- The **Australian Federal Police (AFP)** is a multi-faceted law enforcement organisation. In addition to providing a traditional law enforcement role, the AFP also has Commonwealth responsibilities focused on counter-terrorism and national security. The AFP investigates terrorism and terrorism financing offences in partnership with state and territory law enforcement and other intelligence partners. The AFP also investigates instances of sanctions breaches.
- The **Australian Security Intelligence Organisation (ASIO)** is the nation's security service. ASIO protects Australia and Australians from threats to their security. ASIO collects, assesses and investigates intelligence on threats targeting Australian interests, including terrorism, espionage and foreign interference. It also provides protective security advice to government and industry, and works with partners to strengthen public safety and disrupt attacks.
- The **Australian Secret Intelligence Service** is Australia's overseas secret intelligence collection agency. It informs the government on potential terrorist threats overseas.
- The **Commonwealth Director of Public Prosecutions** prosecutes offences against federal law, which includes terrorism, terrorism financing and sanctions offences.
- The Defence Export Controls (DEC) branch within the **Department of Defence** is Australia's military and dual-use goods and technology export regulator. The DEC issues permits to export, supply, publish or broker military and dual-use goods and technology listed on the Defence and Strategic Goods List;[7] and works to ensure exported items are not used in, or assist, a weapons of mass destruction program.
- **DFAT** hosts Australia's Ambassador for Counter-Terrorism who is responsible for leading Australia's international engagement on counter-terrorism and represents Australia at bilateral, regional and multilateral forums. The Australian Sanctions Office in DFAT is responsible for the administration of Australian sanction laws, including counter-terrorism financing sanctions.
- In addition to its role in national coordination and policy development, **Home Affairs** provides operational and intelligence support to investigations of suspected terrorist activities (including terrorism financing).
- Australia's **Joint Counter Terrorism Teams** are a partnership between members from the AFP, state and territory law enforcement and ASIO. The Teams work closely with other domestic agencies in the broader intelligence community and with international partners to identify and investigate terrorist activities in Australia (including terrorism financing), with an emphasis on preventative operations.

[7] The Defence and Strategic Goods List was updated and came into effect in August 2021. It can be accessed here: defence.gov.au/business-industry/export/controls/export-controls/defence-strategic-goods-list.

- The **Joint Threat Financing Group (JTFG)** was established to formalise the relationship between the AFP and AUSTRAC and includes its predecessor, the AFP's Terrorism Financing Investigations Unit. The JTFG identifies and disrupts threat financing activities. Through expert financial intelligence analysis the JTFG: supports the operational work of Australia's Joint Counter-Terrorism Teams, generates new intelligence leads, and provides advice to government and international partners regarding counter-terrorism strategies.
- The **National Intelligence Community (NIC)** is comprised of ten Commonwealth agencies that have intelligence and operational roles for aspects of counter-terrorism and CTF response efforts. The NIC and other agencies have formed operational CTF working groups to share intelligence and coordinate their activities. This provides wide-ranging intelligence collection capabilities as well as a significant toolkit for disrupting terrorism and terrorism financing actors.
- The **Office of National Intelligence (ONI)** produces all-source intelligence assessments on international political, strategic and economic developments for the Prime Minister, other senior government members and department officials.

A number of law enforcement and Commonwealth agencies, including AUSTRAC, also work closely to support a collaborative, cross-agency effort to protect the safety, security and national interests of Australia. A number of these efforts are directly relevant to combatting terrorism and terrorism financing threats, which include:

- maintaining secure borders (includes preventing smuggling and other criminal cross-border activities)
- disrupting organised crime, including cybercrime, money laundering, and the importation of illicit drugs, illicit tobacco, firearms and weapons
- enhancing the integrity of trade and travel systems. This includes the migration system and the movement of goods and people across Australia's borders through air and sea ports.

FINTEL ALLIANCE NATIONAL SECURITY WORKING GROUP

Fintel Alliance's National Security Working Group (the working group) is a trusted partnership between government, law enforcement and private industry that leverages financial intelligence, forensic accounting, criminal investigative skills and national security knowledge. The working group identifies terrorism financing risks and provides operational support to the JTFG.

In addition, the working group:

- Develops and maintains a dynamic set of financial indicators and data analysis tools to identify national security and terrorism financing risks across all motivational spectrums.
- Provides a forum for information sharing between members to update threat awareness and examine the operational dimensions of the AML/CTF framework.
- Is streamlining response protocols for participants following a terrorism event.

EVOLUTION OF AUSTRALIA'S CTF REGIME

Since the release of FATF's mutual evaluation report of Australia's AML/CTF framework in 2015, the CTF regime, capabilities and outcomes have evolved substantially. Improvements to the regime include significant investments in resources, joint agency and government-industry mechanisms and international engagement. Table 1 provides a snapshot of these improvements over time.

TABLE 1: EVOLUTION OF AUSTRALIA'S CTF REGIME SINCE 2015

CTF ACTIVITY	AS AT 2015	AS AT 2023
Terrorism financing convictions (since 2001)	3	22
AUSTRAC resources	2 x analysts out-posted to partner agencies with CTF remit	• AUSTRAC is a member of the NIC • National security team with dedicated CTF analysts • 5 x analysts out-posted to partner agencies with CTF remit • 4 x international out-posted liaison officers with general remit including CTF.
Southeast Asia regional engagement	Regional engagement is limited, and broader than CTF.	Regional engagement has expanded to include: • five CTF summits • Financial Intelligence Consultative Group • SEA Counter-Terrorism Financing Working Group • analyst exchange programs with regional FIUs • 3 x regional risk assessments of terrorism financing • joint research and intelligence reports and projects on critical regional TF risks.
Fintel Alliance	Not yet established.	• Established by AUSTRAC in 2017, as a public-private partnership with 29 member agencies • Hosts the Fintel Alliance National Security Working Group.
Regulation and tracing of digital currency	Nil.	• In 2018, AUSTRAC started regulating digital currency exchange providers, also known as virtual asset providers. They must register with AUSTRAC and satisfy required reporting obligations to operate in Australia • Tracing capability including dedicated team of analysts and specialist blockchain tracing tools.
Understanding of risks posed by NPOs	Reasonable understanding.	• Comprehensive national sector risk assessment released in 2017 • Co-lead for corresponding regional risk assessment released in 2017

		• Co-lead for red flag indicators of regional terrorism financing abuse of NPOs released in 2018 • Introduction of the External Conduct Standards into the ACNC Regulations in 2019.

THE ROLE OF FINANCIAL INTELLIGENCE IN PREVENTING AND COUNTERING VIOLENT EXTREMISM

Financial intelligence continues to evolve from a largely reactive role in monitoring suspected violent extremists and supporting investigations, towards a proactive role in countering violent extremism. Financial transactions assist in identifying new persons or networks of interest. Financial patterns offer insights for detecting ideological alignment with extreme beliefs. Transactions and customer information frequently contain observable indicators that can help detect when an individual or group may be mobilising towards violence.

Using transactional signatures, AUSTRAC and key partners have developed a dynamic set of financial indicators and data analysis tools to identify and monitor extremist actors across ideological and religious spectrums. Subsequent referrals to partner agencies have led to operational preventive responses.

AUSTRAC publishes a wide range of practical guidance to help businesses understand, identify and report suspicious activity, and meet their AML/CTF obligations. Reporting entities are encouraged to review the full list of available guidance on our website and identify products and tools that may be relevant to their business. In particular, financial crime guides provide information about the financial aspects of different crime types. They include case studies and indicators that can be used to identify if offending could be occurring. A number of indicators will be relevant to detecting terrorism financing. This is because criminals and terrorist financiers often exploit the same channels and methods to move their illicit funds.

CASE STUDY 1: DETECTION OF RADICALISATION BY MAJOR BANKS LEADS TO ARREST AND CONVICTION OF OFFENDER

In 2018, two major banks identified suspicious transaction activity by a male Australian national (Suspect X) and submitted an SMR to AUSTRAC. Initial SMRs identified Suspect X as collecting funds on behalf of a small registered NPO. Subsequent SMR submissions by the banks identified further religiously motivated radicalisation indicators, and AUSTRAC referred the matter to partner agencies.

In 2019, Australian authorities commenced an investigation into Suspect X's suspected links to terrorism activity. Initially Suspect X attempted to steer the NPO towards funding more radical causes, but he abandoned this organisation and co-established a new NPO (registration is now cancelled). Suspect X then made arrangements to travel and fight abroad with Islamic State Khorasan in Kashmir.

In 2021, Suspect X pleaded guilty to one charge of foreign incursions contrary to s119.4 of the Criminal Code and was sentenced to 4 years and 9 months' imprisonment. At the time of initial detection and reporting of his suspicious financial activity in 2018, Suspect X was not known to Australian authorities and his financial transaction and social media activity appeared ordinary.

This case demonstrates the invaluable role that reporting entities and financial intelligence play in the early detection of radicalisation and in assisting Australia's efforts to counter violent extremism.

CASE STUDY 2: AUSTRAC DISCOVERY TOOL IDENTIFIES PERSONS OF INTEREST

In 2020, an Australian national (Suspect X) was arrested and charged for advocating terrorism. His radicalisation was identified in online forums, where he reportedly described the Christchurch offender as a 'hero'. At the time of his arrest AUSTRAC held no transaction reporting to indicate Suspect X held a nationalist and racist extremist ideology. The majority of his financial transactions appeared benign.

Following Suspect X's arrest AUSTRAC used a discovery tool to identify other nationalist and racist extremists residing in the same geographic area. Two individuals with a similar financial profile to Suspect X were identified and reported to partner agencies.

AUSTRAC's discovery tools are designed to uncover financial and transacting profiles similar to known persons of interest. These tools can potentially identify other individuals who may be radicalising or are already members of an extremist network, or who may be planning an attack.

INVESTIGATIONS AND PROSECUTIONS

Most Australian counter-terrorism investigations incorporate financial analysis to determine whether terrorism financing elements are present. Matters can be resolved or progressed for further investigation. Authorities then determine whether to pursue criminal charges or other measures (e.g. passport cancellation) where a terrorism financing prosecution is not practicable.

Since 2001, 22 individuals have been convicted of terrorism financing offences in Australia. As at September 2023, one terrorism financing matter was before the courts. These offences primarily relate to funds supporting a terrorist organisation abroad or a foreign fighter. This is broadly consistent with the dominant characteristic of Australian terrorism financing, which mostly involves funds flows going overseas as opposed to use onshore.

AUSTRALIA'S TERRORISM THREAT ENVIRONMENT

DIAGRAM 2: NUMBER OF TERRORIST ATTACKS AND DISRUPTIONS IN AUSTRALIA

		2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
ATTACKS	RMVE	2	1	1	1	2	-	2	2	1	-
	IMVE	-	-	-	-	-	-	-	-	-	-
DISRUPTIONS	RMVE	3	3	5	2	1	2	1	2	-	-
	IMVE	-	-	1	-	-	-	1	-	-	-

In November 2022, Australia's national terrorism threat level was lowered to POSSIBLE**.** The Director-General of ASIO stated in his Annual Threat Assessment that in 2024, threats to our way of life have surpassed terrorism as Australia's principal security concern. However, he also notes that terrorism remains a real and pervasive threat, even with a lower national threat level. ASIO remains concerned about the potential for lone actors or small groups to commit an act of terrorism with readily available weapons. This is a concern across the motivational spectrums.

Violent extremists have a significant online presence and will continue to use the internet and other technology to facilitate their activities. Radicalisation to a violent extremist ideology often occurs online. Australia's terrorism environment is also influenced to an extent by overseas conflicts and geopolitical tensions. Ethnic, religious and political tensions and events overseas can provoke strong reactions among individuals and communities in Australia. This can include driving propaganda and recruitment by violent extremist groups, inciting violence or accelerating attack planning.

The adoption and adaptation of emerging technologies poses a current and future challenge to countering violent extremism. New technologies, such as artificial intelligence, unmanned aerial

systems, 3D printing and encryption are becoming increasingly accessible. Violent extremists of all motivations will likely seek access to these new technologies to further their objectives.

The Hamas-Israel conflict has drawn protests and accelerated online hate rhetoric by a range of individuals and groups in Australia. This includes supporters of proscribed terrorist organisations in the region, as well as pro-Palestine, pro-Israel and other specific issue supporters. The Hamas-Israel conflict is likely to be protracted, which will continue to feed onshore reactions and disparate grievances among these individuals. No terrorist attacks have occurred in Australia since the commencement of the Hamas-Israel conflict in October 2023. Australian authorities are closely monitoring the security environment and reporting on threats.

RELIGIOUSLY MOTIVATED VIOLENT EXTREMISM (RMVE)

The threat from RMVE actors has reduced. In particular, the offshore networks, capabilities and allure of Sunni violent extremist groups, such as Islamic State and al-Qa'ida, have been substantially degraded. While support for these groups in Australia has declined, their violent extremist agenda will continue to appeal to a small number of Australians. Driven by local agendas but with global ambitions, these groups thrive by promulgating their ideology, raising funds, undertaking attacks and encouraging their adherents to engage in violence. They are able to influence, either physically or virtually, in unstable regions of Africa, the Middle East, South Asia and Southeast Asia.

Christian violent extremism has also occurred in Australia. The most notable terrorist attack of this kind occurred on 12 December 2022 in Wieambilla in Queensland, which resulted in the death of two police officers and one civilian.

THREAT PICTURE IN THE REGION

Despite strong counter-terrorism pressure in the Philippines and Indonesia, Islamic State-aligned violent extremists continue to plan and conduct simple, often opportunistic attacks, primarily directed against local security forces and sectarian targets. In Indonesia, the al-Qa'ida aligned Jemaah Islamiyah continues to recruit, train and prepare for possible future violence. Cross-border links across the region and in international conflict zones increase the risk of extremists absorbing new attack methods, ideology, skills and know-how.

IDEOLOGICALLY MOTIVATED VIOLENT EXTREMISM (IMVE)

IMVE actors, particularly nationalist and racist extremist groups, remain a threat to Australian security. A key belief system of this cohort is an inevitable race war and subsequent creation of a white ethno-state. Some extremists are becoming more overt and provocative, and in some cases this has led to incidents of opportunistic, low-level violence between extremists, counter-protestors and police. Nationalist and racist violent extremist groups are more likely to focus on recruitment and radicalisation, rather than attack planning. However, there is still potential for these groups to radicalise individuals who then go on to undertake attacks, potentially without any warning.

FOREIGN TERRORIST FIGHTERS

There has been a sharp decrease in the number of foreign terrorist fighters departing Australia to participate in offshore conflicts since the decline of Islamic State in Syria and Iraq, and given the impact of travel restrictions as a result of COVID-19. Despite this, international violent extremist groups have drawn people to travel overseas to train and fight, and some groups have motivated others to use

violence in their home countries. Australians who have joined violent extremist groups overseas and continue to hold a violent extremist ideology, could present a security threat if they return to Australia. Australian authorities will continue to assess and manage the enduring terrorism risk posed by these individuals.

HIGH-RISK TERRORIST OFFENDERS

High-risk terrorist offenders who are approaching the end of their custodial sentence can pose a threat to the community once released from prison, and Australia has made extensive investment to understand and manage this enduring risk. The *Counter-Terrorism Legislation Amendment (High Risk Terrorist Offenders) Bill 2021* has implemented a risk management approach that addresses this risk through the consideration of Post Sentence Orders (PSO).

PSOs consist of Continued Detention Orders and Extended Supervision Orders. Both of which are designed to manage risk, and provide released offenders with therapeutic support to ensure effective rehabilitation and reintegration into the community. The PSO scheme allows for conditions to be imposed on an individual that may include, but are not limited to: restrictions on movement, access to devices, requirements to not associate with particular individuals, and to participate in specified rehabilitation and treatment programs. Breaches of conditions are an offence punishable by up to five years imprisonment.

OUTLOOK

Australia's domestic terrorism threat environment will continue to change as drivers of threat emerge and dissipate. These can include both foreseen and unforeseen circumstances and authorities will need to continue to monitor the domestic terrorism environment for emerging threats.

KEY FEATURES OF THE TERRORISM FINANCING ENVIRONMENT

This chapter highlights key features of the terrorism financing environment that have been identified in this assessment. It provides important context for understanding the extent of Australia's terrorism financing risk, how it primarily manifests and challenges in detecting and quantifying illicit transactions.

SMALL SCALE AND LOW VALUE

Australia's terrorism financing landscape is small scale and low value. Domestic attacks are very infrequent and are mainly committed by lone actors who self-fund their activities and often lack a financial element. When financing is evident, it usually involves the direct provision of a weapon or small amounts of cash. Domestic fundraising in support of individual terrorists or violent extremists does occur, but this often involves raising funds to assist with legal fees or other legitimate costs. These financing activities are not illegal.

> In a perception survey issued to international FIUs for this assessment, many noted that Australia poses a 'low' or 'very low' terrorism financing risk to their country/jurisdiction. Of 35 respondents, only four countries noted a suspected terrorism financing link to Australia. More results from this survey are at **Appendix B**.

OUTGOING FUNDS FLOWS

Australia's terrorism financing environment is predominantly characterised by small-scale outgoing international funds flows, and is influenced by offshore events, conflicts and geopolitical tensions. These events can evoke strong reactions among Australians, including provision of funds for legitimate humanitarian or charitable causes (which are later diverted to support terrorism), as well as direct and witting transfer of funds to support violent extremist groups or actors.

Terrorist organisations assessed as most likely to receive Australian funds include Islamic State, al-Qa'ida and their respective affiliates; and Hamas and Hizballah to a lesser extent.[8] The Hamas-Israel conflict has drawn increased funds flowing from Australia to the region, ostensibly for humanitarian purposes. Some of these funds may be exposed to diversion or coercion by Hamas.

Funds are also sent offshore to support IMVE groups and actors—in particular nationalist and racist extremists—but these funds flows are assessed to be mainly for legal purposes (at present) and very low in volume and value.

In known and suspected cases of outgoing terrorism financing, total associated value generally ranges from several hundred to several thousand dollars per case. In cases involving registered charities or legitimate businesses, suspected values have been higher at times given the larger volumes of funds at their discretion. However, developing accurate estimates of the value of terrorism financing diversions is difficult. Illicit transactions can go undetected and therefore unreported. It can also be challenging to explicitly determine the funds were used for illicit purposes, or follow the money trail overseas where Australian authorities may have less visibility.

There is no evidence or intelligence base to suggest terrorism financing funds are flowing into or returning to Australia. One instance was identified in the review for this assessment that likely involved the movement of suspicious funds 'through' Australia. However, these types of funds flows are rarely detected and are likely uncommon. The scale of funds to support foreign fighter travel has decreased, in line with fewer individuals participating in offshore conflicts.

The Hamas-Israel conflict has seen increased funds flowing from Australia to the region, ostensibly for humanitarian purposes. The use of social media, communication, and crowdfunding platforms (the 'online funding ecosystem') has played a critical role for not only raising and moving legitimate funds in response to the humanitarian crisis, but also any funds that go to terrorist actors in the region. Charities and legitimate NPOs operating in or near Gaza may be exposed to illicit diversion or coercion of funding by Hamas.

The conflict could also trigger limited Australian foreign fighter travel to the region. Linked financing risks would be the same as those observed with prior foreign fighter travel from Australia. Travel would likely be self-funded through legitimate means, but individuals may also receive low-value transfers from supporters. Currency exchange providers may also be used pre-travel or en-route to the region.

Australia's close allies and like-minded foreign partners are observing largely similar terrorism financing risk indicators in response to the conflict. While risk profiles differ across countries, Australia is working closely with foreign partners and multinational initiatives to share intelligence on emerging patterns related to the crisis, and monitoring Australia's environment for any change and signs of new terrorism financing threats.

CONTINUED USE OF ESTABLISHED METHODS

Since the publication of the Terrorism financing regional risk assessment in 2016, terrorism financing activity in Australia has evolved but largely continues to employ the same established methods for raising and moving funds. The use of personal funds is most often seen in domestic terrorist plots, and contributions from individual supporters, often under the guise of charitable giving, provide a viable revenue stream for both domestic and offshore funding. For violent extremists across the ideological

[8] As of February 2024, Australia has listed 29 organisations as terrorist organisations under the Criminal Code. Information about each organisation, including the reason for their listing, details of terrorist activity and their impact on Australia, is available on the Australian National Security website nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations.

and religious spectrums, the online funding ecosystem has become integral to recruitment activities and soliciting small-scale contributions from individual supporters.

Terrorist financiers prefer readily available and proven methods to move funds, such as banking, remittance and exchange of cash, over complex schemes. Non-bank online payment service providers play an increasingly important role in the terrorism financing payment chain as they facilitate many payments for platforms in the online funding ecosystem. Consistent with international experience, an uptick in the use of digital currencies has been observed, but there is no evidence to suggest it will overtake simpler methods over the next three years.

DIFFICULT TO DETECT

Terrorism financing can be difficult to detect. The amounts involved are generally small, and transactions often mirror legitimate financial activity and do not raise suspicion. Illicit funds can also be sent through less visible channels such as exchange of cash or unregistered remittance providers. While transaction detection models can identify terrorism financing indicators, reporting entities remain heavily reliant on open source information or law enforcement intelligence to identify individuals that pose a potential terrorism financing risk. It can be very difficult to identify terrorism financing without a link to a known criminal or sanctioned entity.

Technological advancements over the past decade have further complicated the ability to detect and track illicit transactions. The speed of some payment systems enable value to be transferred almost instantaneously, across national and international borders, and in some cases outside regulatory capture. Artificial Intelligence (AI) and the widespread access to it will almost certainly create further and more complex challenges for reporting entities and authorities, for example by challenging identity verification processes.

Reporting entities and investigators are often unable to see the ultimate end-use of funds or confirm their use for terrorism activity. Especially when funds are sent to conduit countries or jurisdictions with weaker AML/CTF controls, and/or recipients are not flagged on sanctions or screening lists. While many reporting entities refuse to service higher-risk jurisdictions, funds can be sent to neighbouring jurisdictions and then physically smuggled across land or maritime borders into a nearby conflict zone. These transfers can be difficult to identify as they are often combined with legitimate transactions intended to support displaced persons. Tactics such as diverting genuine charitable donations, or terrorist-affiliated organisations using funds for seemingly benign reasons such as construction projects, further complicate the picture.

TERRORISM FINANCING CHANNELS AND METHODS

INTERPRETING THE RATINGS

Key risks identified in this assessment have been calibrated to Australia's terrorism financing environment, which is assessed as small scale and low value. A high risk rating **does not** indicate the nature and extent of suspected misuse of the channel or method is significant. Instead, it indicates the channel or method is more likely to be used for terrorism financing in Australia's small-scale environment, and it is generally exposed to a high level of inherent vulnerability to misuse.

This chapter is divided into two sections:

1. raising funds
2. moving funds (which includes storing funds).

The use of funds is covered in the *Consequences* chapter.

Each section presents risk ratings for a range of terrorism financing channels and methods. The small scale of terrorism financing in Australia and the use of less sophisticated methodologies means that few channels and methods appear to be exploited. The existence of a vulnerability does not automatically mean that it will be used to finance terrorism. For this reason, discussion is provided only for those channels and methods that have been rated medium-high and high. An exception is made for registered charities and legitimate NPOs, which have been assessed as posing a medium risk, given these businesses have historically been considered a key terrorism financing channel in Australia.

Each risk rating provides:

- how the level of risk has changed since the release of the *Terrorism financing regional risk assessment* in 2016
- the current overall assessment for RMVE and IMVE actors
- and an assessment of how the risk is likely to change over the next three years.

RAISING FUNDS

CHANNEL/METHOD	SINCE 2016	RATING		OUTLOOK
		RMVE	IMVE	
Self-funding	↔	High	High	↔
Fundraising via social media, communication applications and crowdfunding platforms (includes purported charitable fundraising)	↑	High	High	↔
Registered charities and legitimate NPOs	✥	Medium	Low	✥
Membership fees for groups	*	n/a	Medium	↔
Fraud	↔	Medium	Low	↔
Legitimate and front businesses	↔	Low	Low	↔
Wealthy private donor in Australia	↔	Low	Low	↔
Wealthy private donor outside Australia	↔	Low	Low	↔
Superannuation funds	↓	Low	Very Low	✥
Funding from offshore terrorist group	↔	Very Low	Very Low	↔
Kidnap-for-ransom payments	↔	Very Low	Very Low	↔
Crypto-jacking (theft of digital currency)	↔	Very Low	Very Low	↔
Cyber-extortion (e.g. ransomware)	↔	Very Low	Very Low	↔

*This was not assessed in the 2016 regional risk assessment.

LEGEND

↑	Increase	↓	Decrease	↔	Stable	✥	Dynamic		
Very Low		Low		Medium		Med-High		High	

SELF-FUNDING

RISK RATING

Self-funding is assessed as a **high** terrorism financing risk. The level of risk has remained stable since 2016.

INTELLIGENCE PICTURE

Self-funding remains the main form of terrorism financing in Australia. Violent extremists across the ideological and religious spectrum rely upon it to support both domestic and offshore terrorism activity. It generally involves very low to low value transactions, for example between A$5 and a few thousand dollars per individual in observed cases. Transactions are most often conducted in cash or through legitimate financial channels. Funds are mainly derived from personal savings, income, disposal of assets, sale of personal items, credit cards, loans, welfare payments and pension funds, or superannuation. Specific to nationalist and racist violent extremist groups, funds are also derived from group membership fees.

VULNERABILITIES

- Funds are almost always sourced through legitimate activity, so they are very difficult to detect at their origin.
- The low value of transactions makes it difficult to distinguish from ordinary financial behaviour.
- The time-lag between an individual accessing funds and either committing an attack or travelling to a conflict zone can be very short, therefore failing to trigger suspicion in time for authorities to respond.

OUTLOOK

Self-funding from legitimate sources will remain an enduring risk over the next three years, particularly as Australia's terrorism threat environment continues to be dominated by terrorist activity that requires little to no funding.

Authorities and reporting entities should continue to exchange timely, secure and trusted information on persons of interest and related financial activity through Fintel Alliance. The Fintel Alliance National Security Working Group should continue developing sophisticated financial indicators and data analysis tools for the detection of radicalisation and violent extremist activity.

CASE STUDY 3: AUSTRALIAN NATIONAL SELF-FUNDS HIS ATTACK ON TWO MOSQUES IN CHRISTCHURCH

In March 2019, an Australian national killed 51 worshippers, and injured another 49, at two mosques in Christchurch, New Zealand. This represented the first mass-casualty attack by an Australian ideologically motivated terrorist. The Christchurch offender had been living in New Zealand since August 2017, and was not known to either Australian or New Zealand authorities prior to the attack.

The attack cost an estimated NZD$60,000 (approximately A$57,000). This included travel to and living expenses in New Zealand, and the purchase of weapons and items used to facilitate the attack. The offender used personal savings that he acquired from a family inheritance in 2010 to fund these expenses. The offender transferred funds for the attack from his bank account held with one major bank in Australia to his bank account held with a major bank subsidiary in New Zealand. Given the offender was an Australian national residing in New Zealand, and because he was not previously known to authorities, his offshore transfers appeared legitimate and did not raise suspicion.

FUNDRAISING VIA SOCIAL MEDIA, COMMUNICATION APPLICATIONS AND CROWDFUNDING PLATFORMS

RISK RATING

The overall risk that social media, communication applications and crowdfunding platforms are used by Australian violent extremists to connect, inspire and raise funds is assessed as **high**. The level of risk has increased since 2016, driven by product availability and greater uptake by threat actors.

This category of risk refers to the misuse of social networking and content hosting platforms, internet communication applications, and crowdfunding platforms by violent extremists. This assessment considers these platforms collectively because fundraising campaigns often integrate multiple channels across this ‘online funding ecosystem’.

This category of risk includes fundraising that is fraudulently conducted under the guise of charitable giving and for the purpose of this report is referred to as ‘purported charitable fundraising’. Registered charities and legitimate NPOs also use the online funding ecosystem to solicit and receive donations. Terrorism financing risk associated with these activities is considered in the next section *Registered charities and legitimate NPOs*.

Social media, internet communication applications, and crowdfunding platforms are abused for terrorism financing in a variety of ways.

Social networking and content hosting services are used to solicit donations, distribute propaganda and broadcast calls for radicalisation. Some services contain integrated payment mechanisms, allowing users to contribute/send funds directly through the application, or enable users to generate income through selling merchandise or monetisation features.[9] In such cases, these providers engage in activities comparable to crowdfunding platforms and a third-party online payment service provider facilitates payment transfers.

Internet communication applications facilitate private communication between donors, promoters of fundraising campaigns and/or violent extremists groups. Encrypted communication applications are popular for facilitating fundraising linked to violent extremism, as they allow unguarded discussions regarding payment methods and actual intended use of funds. In particular, the chat application Telegram plays an important role in the online ecosystem of violent extremists in Australia.

Crowdfunding platforms enable fundraising project promoters to reach potential donors quickly and at relatively low cost.[10] Donation-based digital crowdfunding is most commonly observed in suspected terrorism financing cases both globally and in Australia.[11] Payments to crowdfunding platforms are facilitated by third-party online payment service providers. Efforts by larger crowdfunding platforms in recent years to restrict or remove violent extremist content has displaced some illicit fundraising to sites that cater to extremist causes such as Hatreon and Wesearchr.

INTELLIGENCE PICTURE

The online funding ecosystem has become integral to recruitment and fundraising activities by violent extremists across ideological and religious spectrums globally.[12] It allows Australian violent extremists a potential means to grow their resources, as well as connect, inspire and build their networks both within Australia and with overseas groups. Funds are raised through direct calls for contributions. The value of suspicious campaigns identified in Australia is generally low (e.g. hundreds to several thousand dollars per individual campaign).

Payments can be made in the online funding ecosystem in a number of ways (see Diagram 3). This includes provision of cash; transfer or deposit into a nominated bank or remittance account; contributions made directly through platforms in the ecosystem, which are facilitated by online payment service providers; or transfer of digital currency. These channels are also discussed in the next chapter *Moving funds*. A small but increasing number of fundraising campaigns accept or request donations be made in digital currency, particularly privacy coins.

[9] For example live-streaming, video hosting or subscription platforms that allow various forms of monetisation, including tips paid to content makers or donations facilitated by the content makers video page or channel.

[10] Total cost varies, but generally crowdfunding platforms charge between five and 12 per cent of the total value of funds raised. Some platforms charge additional fees, for example if a campaign fails to meet its fundraising target.

[11] The main types of crowdfunding include donation-based, reward-based, investment-based or loan-based. Donation-based crowdfunding can be either physical, for example in-person solicitation of funds, or digital.

[12] Numerous countries and international bodies have noted an increasing use of the online funding ecosystem by violent extremists, particularly IMVE actors. In response, the UN introduced the Security Council Resolution 2462 (2019), calling on its members to assess and address potential risks associated with crowdfunding platforms. The United Nation's Delhi Declaration (2022) further reinforced this message.

Given the public facing nature of most platforms in the ecosystem, fundraising campaigns are often in support of legal activities, for example members' legal fees or travel to attend group rallies. In instances involving purported charitable fundraising, donors may be aware or unaware of the intended illicit purpose of funds. Activities that are directly and overtly linked to terrorist organisations are much more likely to occur via encrypted communication applications (e.g. Telegram). In the context of fundraising, this can involve instructions to donate cash or digital currency which are perceived as less detectable channels.

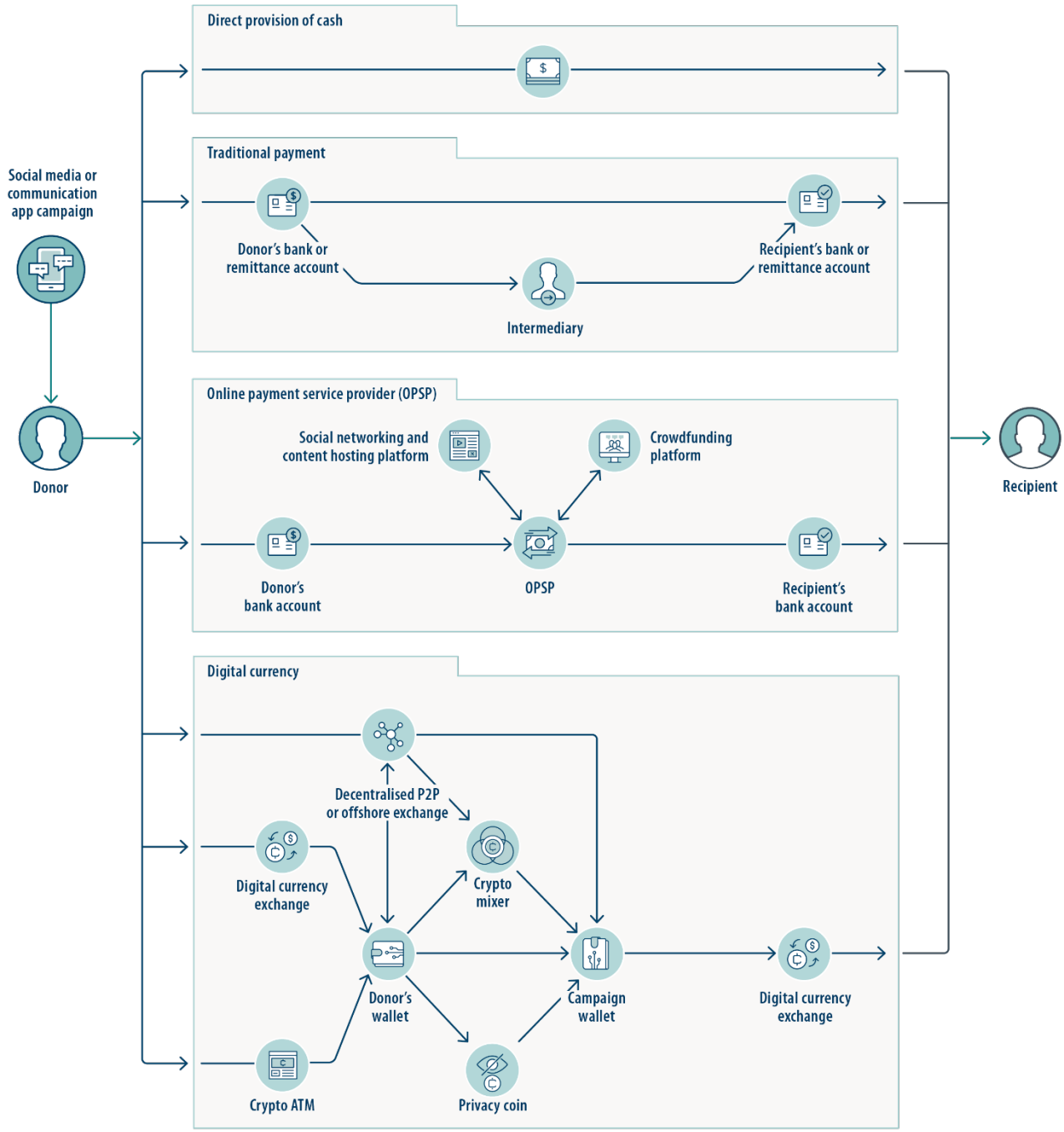
Purported charitable fundraisers often involve both onshore and offshore promoters who target Australian donors and divert funds in support of offshore terrorist groups. Fraudulent campaigns are generally established by sympathisers, supporters, relatives or associates of members of these terrorist organisations. Some campaigns falsely claim to be an operational arm of an overseas charity or NPO but do not have a legal presence in Australia (i.e. they are not a registered charity or legitimate NPO).

In August 2021, the Australian Strategic Policy Institute (ASPI) published a policy brief titled Buying and selling extremism: New funding opportunities in the right-wing extremist online funding ecosystem.[13]

The study examined nine Telegram channels that shared extremist content in Australia between 1 January and 15 July 2021. It identified the use of 22 platforms, payment services, online tools and digital currencies in the online funding ecosystem to solicit, process and earn funds. The range of platforms identified mirrored findings from similar studies conducted in the USA and the United Kingdom in 2020 and 2021 respectively. While the ASPI study was specific to ideologically motivated extremists, the same channels and platforms are misused by RMVE actors as well.

[13] ASPI, 'Buying and selling extremism: New funding opportunities in the right-wing extremist online funding ecosystem'.

DIAGRAM 3: COMMON PAYMENT CHANNELS IN THE ONLINE FUNDING ECOSYSTEM



VULNERABILITIES

- Social media, communication applications, and crowdfunding platforms are all widely accessible, low-cost and can reach a global audience. They can be established quickly with varying degrees of identity verification requirements, and be dissolved equally as fast to avoid disruption.
- Most platforms enforce anti-hate or anti-violence, and in some cases anti-extremism policies. In general, however, policies are not consistent or uniformly implemented across the ecosystem, and there is limited independent oversight of enforcement. Most platforms will rapidly remove extremist content, and some have formalised processes for engaging with Australian law enforcement. Other platforms have less effective processes that limit or delay law enforcement access to information, and some deliberately market services that help avoid police detection.
- Many payments made by Australians in the online funding ecosystem traverse financial entities regulated by AUSTRAC. For example banks, digital currency exchanges, remitters or online payment service providers, which are addressed in the next chapter of this assessment. While this presents opportunity for detection of suspicious or illicit transactions, it can be difficult for reporting entities to distinguish legitimate campaigns from fraudulent fundraising or links to extremists. Furthermore, the third-party nature of some online payment service providers can conceal certain customer details.
- Prosecuting individuals who donate to purported charitable fundraisers, either wittingly or unwittingly, can be difficult because donors can claim to have responded to a front-facing humanitarian fundraiser. While public lists of registered charities and fundraising licences are available, donors must do their own due diligence.

OUTLOOK

Fundraising through the online ecosystem will remain an enduring risk over the next three years. Especially given their availability, ease of use, and capacity to connect Australians with onshore and offshore donors and illicit actors. The pace of emerging technologies in the online payments space will likely complicate this further. Authorities will need to consider whether AML/CTF regulation of certain platforms is practicable and possible.

Purported charitable fundraising will also remain an enduring risk. It can provide a seemingly legitimate avenue to attract funds from both witting and unwitting donors, and successfully prosecuting donors will remain very difficult. Opportunities for detection do exist, as some campaigns are highly visible and intersect with regulated financial entities.

It is highly likely the Hamas-Israel conflict will continue to draw support from Australian donors in the online ecosystem, both witting and unwitting.

CASE STUDY 4: RAISING FUNDS THROUGH SOCIAL MEDIA AND CROWDFUNDING PLATFORMS

An Australian national (Suspect X) is suspected of terrorism financing in Syria. In 2015, Suspect X travelled to Syria and later gained notoriety in videos posted by a northern Syria-based aid group. He became influential in his own right, and ran a social media page appealing for funds. In 2016, the Australian government cancelled Suspect X's passport on suspicion he joined al-Qa'ida affiliate, Al-Nusra Front.

Suspect X denies being a terrorist or supporting a terrorist group, and publicly claims to be a humanitarian aid worker. Suspect X has not attempted to return to Australia and continues to rely on public donations made via several crowdfunding campaigns. Donors have included Australians.

CASE STUDY 5: USE OF ONLINE FUNDING ECOSYSTEM BY CONVICTED EXTREMIST

In 2021, the leader of Australian neo-Nazi group National Socialist Network used social media, digital currency and a crowdfunding platform to fund his legal defence in relation to assault and affray charges. A communication platform was used to make an appeal for digital currency donations and supporters were provided instructions on how to create a personal cryptocurrency wallet and donate funds. Funds were also raised in both cash and micro-donations via a crowdfunding platform.

CASE STUDY 6: USING SOCIAL MEDIA TO INCITE VIOLENCE AND SUPPORT FOR ISLAMIC STATE

In 2021, a male (Suspect X), was arrested when he returned to Australia from Saudi Arabia and charged with various terrorism-related offences including conspiracy to provide support for another person to engage in hostile activity in a foreign state. Suspect X allegedly played a senior role in a Brisbane-based group that supported jihadist ideology and advocated for travelling to Syria to fight. This included video posts on a social media page between March 2019 and February 2020, in which he allegedly solicited support for Islamic State and called for followers to retaliate against those who were fighting against Islamic State. Suspect X also allegedly co-founded a purported charity that solicited donations for Australian foreign fighters, and he is accused of transferring A$1,010 to a fighter in Syria.

CASE STUDY 7: USE OF THE ONLINE FUNDING ECOSYSTEM BY THE CHRISTCHURCH ATTACKER

The Christchurch attacker used various social media platforms to spread propaganda and garner support for his national and racist violent extremist ideology. Prior to his March 2019 attack, he released a manifesto outlining his anti-immigration and anti-Islamic and accelerationist ideas. The offender announced the attack on 8chan, an online message board dedicated to extreme free speech and anonymity, and he live-streamed the attack on social media. Around 1.5 million uploads of the video were detected and removed from a social media platform in the first 24 hours alone.

REGISTERED CHARITIES AND LEGITIMATE NPOS

RISK RATING

The overall risk that Australian registered charities and legitimate NPOs are used to raise or divert funds for terrorism financing is assessed as **medium**. The level of risk has remained largely stable since the release of Australia's non-profit organisation sector national risk assessment in 2017.

This category of risk refers to charities that are registered with the ACNC and NPOs that have an active Australian Business Number (ABN) or 'legitimate NPOs'. It does not include unregistered organisations or fundraising that is conducted without an appropriate licence. This activity is covered in the previous section titled *Fundraising via social media, communication applications and crowdfunding platforms.*

AUSTRALIA'S NPO SECTOR

Australia's NPO sector is large, diverse, and provides critical services to millions of Australians and overseas beneficiaries. The sector contributes significantly to Australia's economy and civil society. In 2021, registered charities alone reported an annual revenue of A$190 billion, including A$13.4 billion in donations and bequests.[14]

Approximately 225,300 ABN[15]-registered NPOs operate in Australia. This includes 157,100 entities who self-assess to the Australian Taxation Office (ATO) as income tax exempt; 57,800 charities registered with the ACNC,[16] and approximately 9,000 taxable not-for-profits. This combined population is generally considered to be the 'NPO sector'.

NPOs operate under a range of legal structures including companies limited by guarantee, incorporated associations, and non-distributing co-operatives. Regulatory oversight is dependent on the legal structure in place. Each regulator has different requirements, functions and powers. Please refer to the 2017 Australia's non-profit organisation sector national risk assessment of NPOs for a detailed breakdown of the national NPO regulatory landscape.

Unregistered NPOs

NPOs are not required to register with Commonwealth and state or territory regulators unless they use certain legal structures, for example if they are incorporated, want to access benefits such as deductible gift recipient status or tax charity concessions, or conduct certain activities such as fundraising. There are no reliable estimates of the number of unregistered NPOs operating in Australia. The last research estimates were made in 2010, placing the figure at approximately 400,000.

Unregistered NPOs tend to be very small, and are not subject to regulation on the basis that they do not have an ABN, they do not employ staff, they do not need to register for goods and services tax and are not charities.

INTELLIGENCE PICTURE

Registered charities and legitimate NPOs provide an attractive channel for terrorism financing as donations can be solicited from a large number of individuals, witting and unwitting, and diverted for illicit purposes. Most observed cases relate to outgoing funds flows to support RMVE actors or designated terrorist organisations overseas. The intelligence picture regarding the misuse of registered charities and legitimate NPOs by IMVE actors is developing. While some Australian IMVE actors maintain ties to legitimate NPOs that support ethno-nationalist ideals, these organisations do not appear to be funding violent activity.

[14] Please refer to the Australian Charities Report - 9th Edition for the most recent comprehensive analysis of Australia's charities.

[15] ABNs are a unique 11-digit identifier that are generally required for a business to operate in the tax system.

[16] Charities register with the ACNC based on 'charitable purpose' and may choose to also register for tax exemptions. Self-assessing income tax exempt status is available to entities who operate as not-for-profit but don't have a charitable purpose (e.g. sporting clubs).

Registered charities and legitimate NPOs are exploited for terrorism financing in several ways. They can be established with the genuine intent to undertake charitable activity, with unintended illicit diversion occurring downstream. This usually involves an NPO that is acting in good faith, but has limited control and ability to ensure funds are used for their intended purpose. In general, large, international NPOs better understand and mitigate their terrorism financing risks. They can do this because of their access to resources and governance expertise, and in some cases, requirements by funding bodies to have effective financial control and acquittal.[17] In contrast, small and medium NPOs generally rely on trust-based relationships with in-country individuals or partner organisations to deliver projects overseas. These organisations may not understand their terrorism financing risks, and may not implement adequate mitigation strategies.

Legitimate NPOs can also be established with the intent to support individuals or organisations linked to terrorism activity. These NPOs are usually linked to offshore terrorist organisations or networks and provide an onshore humanitarian front to obscure the intended diversion of donations. Where detected in Australia, these organisations have often been established and controlled by family members or associates of offshore violent extremists. They often combine terrorist financing with other charitable activities, which can complicate disruption efforts.

Suspected terrorism financing plots involving legitimate NPOs have largely involved simple methods for raising and moving funds overseas. Donations are accepted by direct bank transfer, online payment service providers, cash and increasingly, digital currency. Traditional banking and remittance service providers are commonly used to move funds overseas. Informal remittance channels such as Hawala and cash couriering are also used to a lesser extent, particularly by NPOs that have been de-risked by major financial institutions.

Accurate estimates of the value of terrorism financing through legitimate NPOs remain elusive in the absence of investigation outcomes. However, case studies suggest some legitimate NPOs provide a more lucrative revenue stream than other channels, given their access to multiple donors. This increases their terrorism financing risk profile.

Since the 2017 national risk assessment, Australian authorities have invested heavily to better understand, monitor and disrupt terrorism financing abuse of registered charities and legitimate NPOs both within Australia and across the Southeast Asia region. These activities have led to operational outcomes including multiple charity registration revocations and the listing by Indonesian authorities of one Australian NPO and its main Australian facilitator for targeted financial sanctions.

[17] This is reinforced by governance standards required of these NPOs to meet Australian Council for International Development and Australian Department of Foreign Affairs and Trade accreditation to deliver projects overseas.

HIGH-RISK SUBSET OF AUSTRALIA'S NPOS

International AML/CTF standards require countries to identify the subset of NPOs which, due to their activities or characteristics, are likely to be at risk of terrorism financing abuse. Focusing on the subset most at risk instead of the whole sector, is intended to enable a targeted and proportionate response to outreach and monitoring. It also recognises that not all NPOs are inherently high risk and some may represent little or no risk.

The 2017 national risk assessment of NPOs identified a number of characteristics of the high-risk subset of Australian NPOs. AUSTRAC and the ACNC are currently validating and updating this subset and intend to produce a report in 2024. This report will expand the scope to cover registered charities and legitimate NPOs, as well as unregistered NPOs, to understand the extent of risk that sits outside Australia's regulatory framework.

VULNERABILITIES[18]

- Nationally, Australia has multiple agencies at the Commonwealth level that provide regulatory oversight of registered charities and legitimate NPOs. Additionally, each state and territory may impose different regulations on legitimate NPOs operating within their jurisdiction. This results in inconsistent levels of visibility, capability and resources among NPO regulators to monitor and support vulnerable organisations. It also means, in some instances, problematic charities and NPOs can move to another jurisdiction should their registration or licence be revoked.
- Most legitimate NPOs are required to fulfil some form of financial reporting obligation. However, many self-assess governance arrangements, risk mitigation and control strategies, and are not subject to independent oversight.
- There are regulatory and visibility gaps regarding religious NPOs. These entities do not require a fundraising licence in most jurisdictions, and 'basic religious charities'[19] do not need to comply with the ACNC governance standards or provide financial reporting to the ACNC. However, basic religious charities are required to comply with the External Conduct Standards where they conduct activities or send money overseas.[20] This includes directly or indirectly through third parties.
- Generally, NPOs are not captured under the AML/CTF Act, and do not have reporting obligations to AUSTRAC. An NPO would only be regulated by AUSTRAC if it provides a designated service as defined in section 6 of the AML/CTF Act. Detection of suspicious financial activity is therefore reliant on financial institutions who provide services to NPOs. These visibility gaps are somewhat mitigated by AUSTRAC analysts and members of the Fintel Alliance National Security Working Group targeting high-risk NPOs.
- There is wide variation in the level and sophistication of risk mitigation strategies employed by individual NPOs. NPOs that are more vulnerable to terrorism financing generally demonstrate one or more of the following factors:
    - poor understanding of terrorism financing risks and limited implementation of related mitigation strategies
    - poor due diligence on key personnel, volunteers, partners and beneficiaries

[18] Please refer to the 2017 national risk assessment of NPOs for a comprehensive overview of inherent vulnerabilities that increase the sector's exposure to terrorism financing and its capacity to combat it.

[19] A basic religious charity is defined in section 205 of the *ACNC Act 2012*. It is a registered charity with the sole purpose of advancing religion. It cannot be an incorporated association and cannot receive $100,000 or more in government grants.

[20] Charities are also required to take steps to protect assets and funds from misuse; and obtain and keep records necessary to prepare summaries of its activities and expenditure on a country-by-country basis for each financial year.

- inexperienced staff and lack of formalised training and ongoing professional development
- poor record keeping
- poor transparency and accountability of the end-to-end funding cycle
- NPOs' use of cash or informal money transfer businesses to move funds outside regulated channels
- operations in countries with poor AML/CTF regimes, or in conflict or post-conflict regions.[21]

OUTLOOK

Registered charities and legitimate NPOs will likely continue to be used by Australian RMVE actors and supporters to raise funds for overseas terrorist activities over the next three years. It is highly likely the Hamas-Israel conflict will continue to draw support from Australian donors to registered charities and legitimate NPOs with operations in or financing links to the region. While most donations will be made in good faith to address the humanitarian crisis in Gaza, funds/aid will remain exposed to potential diversion by Hamas.

Registered charities and legitimate NPOs are unlikely to become a key terrorism financing avenue for IMVE actors in the next three years given their successful use of other channels. However, links between ideologically motivated extremists and legitimate NPOs warrant monitoring by authorities to understand potential misuse to spread propaganda and engage in recruitment activities.

The ACNC should continue to educate registered charities about terrorism financing risks and compliance with the External Conduct Standards. Commonwealth and state or territory regulators should continue to collaborate with relevant stakeholders to improve governance and oversight across the sector, and improve outreach to vulnerable NPOs.

AUSTRAC should provide relevant guidance and indicator reporting to NPO peak bodies and reporting entities to ensure proportionate customer due diligence and transaction monitoring is applied to high-risk NPOs.

CASE STUDY 8: AUSTRALIAN CHARITY LINKED TO SUSPICIOUS TURKISH NPO

In 2020, suspicious and structured transfers between a registered Australian charity, an Indonesian charity and a Turkish charity were identified. The Turkish NPO had previously been implicated in terrorism financing, as well as people and weapons smuggling for terrorist organisations. Incoming and outgoing transfers made between the Australian charity and Turkish charity totalled approximately A$1.6 million, and did not make commercial sense. Financial investigation suggested the transfers were likely a coordinated approach to raise funds in Australia, pool funds in Southeast Asia, then move funds to high-risk jurisdictions in support of offshore terrorist and extremist groups in the Middle East and North Africa.

[21] Australian registered charities must comply with the External Conduct Standards and Governance Standards in the ACNC Regulations to maintain their registration. Those standards put obligations upon charities to maintain good financial controls in Australia and overseas. However, under-investment in good governance means that, in practice, many charities operating in high-risk regions are vulnerable to terrorism financing.

CASE STUDY 9: AUSTRALIAN CHARITY AND ITS INTERNATIONAL PARENT ENTITY WITH MULTIPLE LINKS TO TERRORISM

A registered Australian charity ('Charity X') raised funds in Australia and transferred or physically carried the funds to high-risk regions in Niger, Bangladesh and Türkiye to provide to their parent organisation. The parent organisation is an international NPO and has longstanding associative and financial links to Australian foreign fighters. It has been identified in several counter-terrorism investigations as likely diverting a portion for legitimate donations to fund violent jihadists in Syria. Charity X also has historical links to known and suspected terrorists and terrorist financiers. For example, one Australian director was previously detained by Kurdish security services for suspected association to al-Qa'ida. Charity X failed to disclose their high-risk financial and operational links with the parent organisation to the ACNC. There is a high risk that a portion of donations raised in Australia are being diverted to finance offshore violent extremists.

MOVING FUNDS

CHANNEL/METHOD	SINCE 2016	RATING		OUTLOOK
		RMVE	IMVE	
Banking system*				
Remittance service providers				
Non-bank online payment service providers				
Digital currencies*				
Cash exchange (domestic)*				
Cash smuggling (offshore)				
Foreign exchange providers				
Luxury goods (e.g. jewellery, watches etc.)*				
Precious metal traders (e.g. gold bullion)				
Stored value cards				
Non-bank lenders and financiers				
Pubs and clubs				
Casinos, betting agencies and other gambling activities				
Stockbroker and securities dealers				

* These channels are also used to store terrorism financing funds. The intelligence picture on estimated amounts and duration of time that funds are stored before or after moving is unclear.

LEGEND

BANKING SYSTEM

RISK RATING

The risk of the banking system being used to move and store funds for terrorism financing is assessed as **high**. The level of risk has remained stable since 2016. Banks continue to be a reliable and efficient way to move funds nationally and globally by threat actors.

AUSTRALIA'S BANKING SECTOR

Australia's banking sector sits at the centre of the financial services industry. The sector is led by four major banks, who service approximately 45.6 million customers[22] and hold 73 per cent of all Australian household deposits. These major banks offer thousands of products and services to a diverse range of customers, and process the majority of international transactions.

In 2021, AUSTRAC published four national ML/TF risk assessments of Australia's banking sector. These included Australia's major banks, other domestic banks, foreign subsidiary banks and foreign bank branches. Please refer to these assessments for a comprehensive overview of each sub-sector including the distinct terrorism financing risks they face. An overview of key findings and snapshot of ratings from each assessment is also available.

In 2019, AUSTRAC published a national ML/TF risk assessment of Australia's mutual banks. The size and composition of this sub-sector has changed since publication of the assessment. However, the terrorism financing risks noted in the assessment remain relevant.

INTELLIGENCE PICTURE

Given their central role in the Australian economy and the global payments ecosystem, most terrorism financing activity will intersect with reporting entities in the banking sector at some point in the transaction chain. The nature and extent of the risk is largely proportional to a reporting entities' size, the types and location of customers it services, its products and services and its global reach. Risk profiles are also impacted by the maturity of a bank's AML/CTF risk culture and compliance program.

Major banks are almost certainly exposed to the majority of terrorism financing risk facing the sector given the size of their customer base, scale of operations, cash transaction infrastructure,[23] and global reach. They are also the key conduit for international transactions in and out of Australia, and serve as correspondent banks for other financial institutions. These links to offshore institutions and customers expose major banks to a high level of foreign jurisdiction risk. However, major banks invest heavily in their AML/CTF capabilities, have a strong understanding of their terrorism financing risk exposure, and implement sophisticated monitoring systems. They also detect and report more suspicious transactions than any other banking subsector, providing significant amounts of financial intelligence to law enforcement and intelligence bodies. In instances of customer de-banking by a major bank, terrorism financing risk can be displaced to a smaller bank which may employ less regulatory and compliance oversight.

Terrorism financing risk is concentrated in retail banking, which is exposed to high volumes of low-value transactions. Transaction accounts and electronic funds transfers are particularly attractive for terrorism financing as they allow rapid, reliable and easy collection, storage and movement of funds nationally and globally. Transaction accounts are key transit points in and out of the banking

[22] This figure has been compiled from the number of retail and corporate customers noted on each major banks' website. It is current as at July 2023.

[23] Major banks have the most extensive and accessible cash transaction infrastructure in Australia, and facilitate more cash transactions than all other regulated sectors combined. This results in extreme exposure to cash-based terrorism financing methodologies.

system, making them the most commonly and persistently misused product. They are easy to open, can often be established online, and are highly exposed to cash transactions, including the withdrawal of cash in high-risk jurisdictions. Misuse of stored value cards and credit cards has declined in recent years as fewer Australians travel overseas to participate in foreign conflicts. However, terrorism financing risks associated with these products is dynamic and will likely shift in line with the threat landscape.

Most terrorism financing cases involve simple unsophisticated methods such as low value customer-to-customer transfers. Some have involved structured deposits of cash or multiple domestic funds transfers into bank accounts, including pooling or storing funds, followed by international funds transfers out of Australia. More complex cases are rare, for example those involving efforts to obscure beneficial ownership through the use of legitimate or shell companies or third-country transfers. In these instances it is often difficult to definitively link the transaction to terrorism financing.

VULNERABILITIES

- Despite significant investments into sophisticated monitoring and detection systems and specialised AML/CTF staff, many banks remain exposed to a high level of inherent vulnerability to terrorism financing. Illicit transactions are usually low value and difficult to distinguish from legitimate financial activity. This can make detection of suspicious transactions challenging.
- Technological innovations have increased transaction speed and convenience in recent years. The rollout of the New Payments Platform (NPP) has enabled near real-time transfers, making it harder for banks to identify and freeze suspicious transfers before funds leave an account. The exploitation of multiple NPP-enabled accounts across different banks makes it difficult for law enforcement to trace transactions to investigate and prosecute terrorism financing offences.

OUTLOOK

Retail banking products and services will remain attractive to terrorist financiers for the same reasons they appeal to regular customers: they provide a fast, reliable channel to move funds domestically and overseas. More complex terrorist financing schemes involving the banking system (e.g. misuse of products and accounts linked to international trade or business structures of varying complexity) will likely remain less common in the current terrorism environment.

The Fintel Alliance National Security Working Group should continue developing sophisticated financial indicators and data analysis tools for the detection of radicalisation and violent extremist activity.

AUSTRAC should continue to profile emerging risks and provide guidance and outreach across the banking sector. This is particularly to vulnerable reporting entities and especially if shifts in the terrorism environment lead to new or emerging financing behaviours.

CASE STUDY 10: CHALLENGES IN DISCERNING TERRORISM FINANCING FROM LEGITIMATE FINANCIAL ACTIVITY IN THE BANKING SECTOR

Suspect X, an Australian national, was allegedly providing support for al-Qa'ida. Suspect X used a range of methods to avoid detection. This included registering and operating a global network of companies in Australia, Qatar, Brazil, Colombia, Sri Lanka, Tanzania, Türkiye and the Persian Gulf. Each company had limited visibility of his entire operation. Suspect X maintained multiple business and personal accounts with international banks, major Australian banks and remittance service providers, also known as remitters. Suspect X conducted frequent cash transactions within the limits of their customer and business profiles, usually via ATMs, and transferred funds offshore via remitters. This made it very difficult for a single reporting entity to identify suspicious financial activity.

REMITTANCE SERVICES

RISK RATING

The overall risk that remittance services are being used to move funds for terrorism financing offshore is assessed as **high**. The level of risk has remained stable since 2016, and remitters continue to provide a proven channel for financing terrorism. Remitters are particularly popular for funds flows to places where formal banking networks may not operate, including high-risk jurisdictions.

This category of risk includes registered remittance service providers and unregistered remittance dealers operating in Australia. Terrorism financing risk varies between these service providers, and is reflected in Table 2.

TABLE 2: TERRORISM FINANCING RISKS ASSOCIATED WITH DIFFERENT REMITTANCE SERVICES

TYPE OF REMITTANCE SERVICE	THREAT		VULNERABILITY
	RMVE	IMVE	
Registered remittance service providers	●	●	●
Unregistered remittance dealer	●	●	●
Hawala/offsetting	●	●	●

AUSTRALIA'S REMITTANCE SECTOR

Remittance service providers operating in Australia offer fast and relatively low-cost methods of transferring funds domestically and overseas. These services are a crucial component of global financial inclusion and are particularly important for migrant communities and expatriate workers supporting families in their countries of origin.

Remittance service providers must register with AUSTRAC as one or more of the following:

- A Remittance Network Provider (RNP), operates a network of affiliates that use the RNP's brand, products, platforms or systems to provide remittance services to customers. An RNP is responsible for an affiliate's registration and reporting obligations to AUSTRAC, and must ensure the affiliate has an appropriate AML/CTF program.
- An affiliate has an agreement with an RNP to provide remittance services. Under the agreement the affiliate accepts instructions directly from customers to send funds to a recipient in another location. Affiliates are independently-owned, and the RNP does not exercise control over other activities or services provided by the business.
- Independent remittance dealers can be registered as a single entity operating independently, or own and operate multiple branches. They use their own products, platforms or systems to provide remittance services directly to customers.

In 2022, AUSTRAC published two national ML/TF risk assessments of Australia's remittance sector. Independent remittance dealers in Australia and Remittance network providers and their affiliates in Australia. Please refer to these assessments for a comprehensive overview of each sub-sector including their size, scale of operations and the distinct terrorism financing risks they face.

INTELLIGENCE PICTURE

Registered remittance service providers

Registered remittance service providers are used to transfer funds overseas by both RMVE and IMVE actors. Law enforcement investigations have demonstrated that RMVE actors are sometimes linked to the remittance service providers they exploit. Transactions are usually low-value, approximately several hundred to a few thousand dollars each. Methods to remit funds are largely unsophisticated, in most cases little effort is made to hide the source or destination of funds. However, third-party intermediaries are sometimes used to complete remittances in order to hide the end beneficiary of illicit transfers.

Unregistered remittance dealers[24]

Despite concerted law enforcement attention, unregistered remitters continue to operate in Australia. In terms of terrorism financing, unregistered remittance dealers have been used by RMVE actors. Its use by IMVE actors is assessed as much less likely. As with registered remittance service providers, RMVE actors are sometimes linked to the unregistered remittance dealer they exploit.

AUSTRAC'S UNREGISTERED REMITTER CAMPAIGN

Between August and November 2019, AUSTRAC ran a community campaign targeting unregistered remittance dealers. During this time, more than 130 AUSTRAC staff visited over 400 registered remittance service providers across the country. These visits gave businesses the opportunity to provide feedback and ask AUSTRAC staff questions about their obligations. Over 240 people attended town hall meetings including local community leaders and multicultural organisations, registered remittance service providers, partner agencies, and journalists.

At each event, AUSTRAC staff shared information and provided materials in 11 languages that explained the threat of using unregistered remittance dealers. Participants shared this information with their communities to help them identify unregistered remitters, and make informed decisions about who they choose to transfer money overseas with.

Hawala/offsetting

Offsetting is a legitimate method of exchanging value that is used by both registered remittance service providers and unregistered remittance dealers. For some reporting entities offsetting is a viable alternative to using formal banking channels, particularly if an entity has been de-risked by a financial institution. The use of offsetting by RMVE actors is well documented globally, and has been observed in Australia as well. Its use by IMVE actors has not yet been observed.

VULNERABILITIES

- Illicit transactions are usually low value and difficult to distinguish from legitimate financial activity. This can make detection of suspicious transactions challenging.
- Remitters have a high exposure to high-risk foreign jurisdictions. Particularly those servicing customers with strong ties with high-risk countries or jurisdictions that border a conflict zone.
- The effectiveness of AML/CTF programs and associated detection capabilities are uneven across the remittance sector. Some businesses are unwilling or unable to detect and report suspicious matters and mitigate the terrorism financing risks they face.[25]
- Certain outsourcing arrangements[26] and operational structures, for example the RNP-affiliate structure used by some reporting entities, lengthen the product-delivery chain and reduce the level of oversight a reporting entity might have over customers and transactions.
- The trend towards remote product delivery channels such as websites or mobile applications, accelerated by COVID-19, provides a layer of anonymity for customers, increasing vulnerability

[24] For the purpose of this assessment, the terms 'unregistered remitter' or 'unregistered remittance dealer' refer to an individual, business or organisation that carries on a business of providing a designated remittance arrangement in Australia and is not registered on AUSTRAC's Remittance Sector Register. Individuals and entities that provide remittance services in Australia do not always comply with registration and regulatory requirements. A variety of businesses operate as unregistered remitters. They often pose as cash-intensive businesses or international trading businesses to provide a veneer of legitimacy for international transactions. Some unregistered remitters specialise in moving funds to or from foreign jurisdictions that have underdeveloped or quarantined financial systems.

[25] This can be influenced by a range of factors such as language barriers, poor understanding of AML/CTF obligations, mistrust of the government, a belief that submitting SMRs makes their business look bad, or apprehension to report suspicious matters regarding customers that are well known to them.

[26] For example, the use of super agents, correspondent institutions or third party service providers. Please refer to the two national ML/TF risk assessments of the remittance sector for details of vulnerabilities posed by outsourcing arrangements.

to criminal actors. The adoption of mobile technology has also increased global accessibility to services and provides an additional element of anonymity that may be attractive to terrorist financiers. Illicit actors can exploit online remittance account applications to establish mule accounts, in some cases using stolen identities, which can then be used to send illicit transfers offshore.

- Offsetting affords customers greater anonymity, and transactions are often subject to less scrutiny. Particularly if the reporting entity has poor or limited record-keeping practices. Offsetting also increases the ability of a criminally complicit business to avoid reporting requirements.[27]
- Unregistered remittance dealers do not comply with applicable AML/CTF requirements and may be used by customers who wish to avoid regulated channels.

OUTLOOK

Similar to banking channels, remittance services will remain attractive to terrorist financiers for the same reasons they appeal to regular customers: they provide a fast and reliable channel to move funds overseas. Unregistered remitters will continue to provide additional appeal as they enable customers to transact outside the formal financial sector.

Authorities should identify the types of remitters at high risk of being misused for terrorism financing. A better understanding of high-risk factors, activity and remittance corridors linked to high-risk countries would help strengthen targeted oversight, outreach and intelligence monitoring of financial behaviour.

AUSTRAC will continue to provide tailored guidance regarding terrorism financing risks across the sector and offer outreach to vulnerable reporting entities. AUSTRAC will also continue to assess reports of suspected unregistered remittance dealers and take any action required.

CASE STUDY 11: CONVICTED ASPIRING ISLAMIC STATE FIGHTER

In 2017, an Australian national (Suspect X) was arrested and charged with terrorism offences for preparing an incursion into a foreign country with the intention to carry out violent acts. During a controlled police operation Suspect X consulted with a person he believed could assist his travel offshore; participated in training exercises; purchased camping and military equipment; and attempted to remit A$300 to a person in Syria to help facilitate his travel there. Suspect X also sold personal belongings and attempted to obtain money from a relative to fund his travel prior to attempting to depart Australia. In 2019, Suspect X was found guilty of engaging in conduct preparatory to committing a foreign incursion offence. He was released from custody for time served and placed on a five-year good behaviour bond.

[27] Reporting entities must still submit relevant reports to AUSTRAC when using offsetting arrangements. AUSTRAC expects remitters to know and understand their AML/CTF reporting obligations when using these arrangements.

CASE STUDY 12: REMITTING FUNDS TO SUPPORT ISLAMIC STATE

In 2014, an Australian national (Suspect X) was arrested and charged for terrorist and terrorism financing offences after he planned a terrorist attack in Australia and sent funds to Islamic State. With respect to the terrorism financing activity, Suspect X attempted to transfer A$9,000 to a member of Islamic State with whom he had been in regular contact. He converted Australian currency to US currency at a foreign exchange service provider and then recruited an individual intermediary to remit the funds offshore through a registered remittance service provider. Suspect X provided instructions to the intermediary as to how and to whom the US currency was to be transferred in Türkiye. However, the intermediary was concerned about the fees and abandoned the transfer. The cash was then found and confiscated by the intermediary's mother. Suspect X also organised an individual intermediary to remit A$3,000 on two separate days (A$6,000 total), to Pakistan to assist Islamic State foreign fighters. In 2019, Suspect X was sentenced to over 18 years imprisonment for all offences, of which ten years and eight months related to his financing offences.

NON-BANK ONLINE PAYMENT SERVICE PROVIDERS

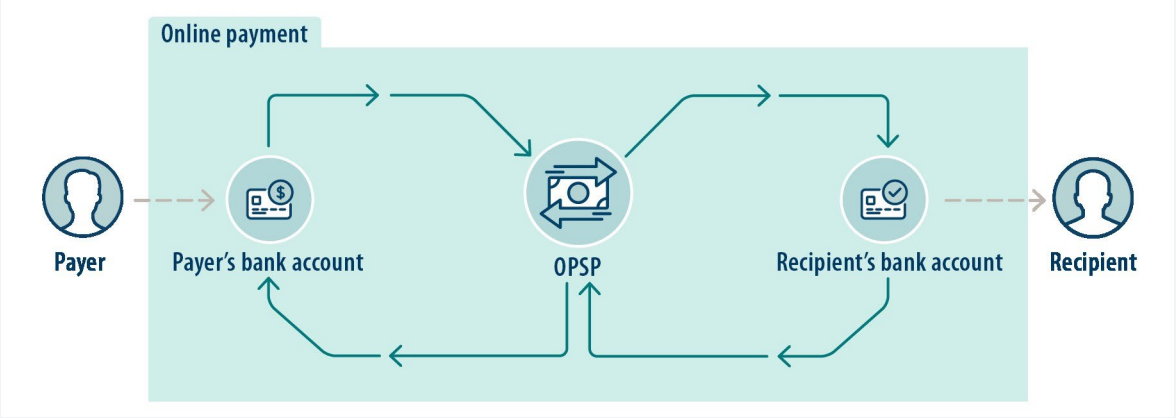
RISK RATING

The risk of non-bank online payment service providers (OPSPs), being used to move funds for terrorism financing is assessed as **high**. The level of risk has increased since 2016, in line with its increased uptake by the general community.

INTELLIGENCE PICTURE

OPSPs are a critical mechanism in the violent extremist online funding ecosystem (see *Fundraising via social media, communication applications and crowdfunding platforms).* They facilitate a range of low-value payments, onshore and offshore, for illicit actors across the ideological and religious spectrums. Few examples of sophisticated activity have been observed, however, some individuals without a criminal record have allowed their accounts to be used for fundraising campaigns linked to nationalist and racist violent extremists to help avoid detection.

WHAT IS AN ONLINE PAYMENT SERVICE PROVIDER?



An OPSP is a third party that provides services for merchants to accept online payments by linking customer payment information to the merchant's account, and facilitating the transaction between the customer's and merchant's respective financial service providers. OPSPs ensure transactions make it from the customer to the merchant securely.

OPSPs facilitate a constantly evolving range of transaction types, including purchased payments, peer-to-peer payments, micropayments and donations, crowdfunding, digital wallets, buy-now-pay-later, e-commerce, and subscriptions.

Over the past two decades, the payments landscape has undergone a significant transformation with electronic payment instruments displacing both cheques and cash. In the financial year 2020-21 alone, Australians made around 625 electronic transactions per person on average, compared to 275 ten years ago. Online payment services in Australia were initially controlled by major banks, which operated an end-to-end service. This has evolved and now there are numerous and varied OPSPs who have one or more roles in the payments ecosystem.

VULNERABILITIES

- OPSPs enable funds to be moved around the financial system in seconds. This can create challenges for financial institutions and authorities in detecting, tracing and freezing illicit funds. This is further complicated given terrorism financing is usually low value and difficult to distinguish from legitimate transactions.
- The introduction of additional parties to the payment process can reduce end-to-end visibility of the transaction chain. Additionally, some OPSPs require minimal credentials on a receiver.
- The design of some OPSP products and services may not fit within existing regulatory frameworks. It may be difficult for reporting entities to determine whether the OPSPs product or service meets the definition of a designated service under the AML/CTF Act, whether a provider is required to enrol with AUSTRAC, and what reporting obligations they may have.
- From cost and technology perspectives, OPSPs have low access barriers for merchants and customers. OPSPs can offer merchants more choices and better pricing compared to traditional banks. These commercial benefits are likely to see the continued disruption of traditional payment gateways and the growth of OPSPs.

OUTLOOK

OPSPs will remain an enduring terrorism financing risk over the next three years. Particularly given the likely growth of this sector including offshore entities providing settlement services to domestic individuals.

CASE STUDY 13: SENDING FUNDS TO AN ISLAMIC STATE FIGHTER

In 2017, an Australian national (Suspect X) was arrested and charged with terrorism financing offences for providing funds to an Islamic State fighter in Syria. The first offence involved three deposits totalling A$2,610 into Suspect X's bank account. He then transferred these funds to an OPSP account held by an intermediary who was to then transfer the funds to the Islamic State fighter. The second offence involved the payment of US$103.07 to the same individual to maintain his website forum that promoted Islamic State. In 2019, Suspect X pleaded guilty to the offences and was sentenced to imprisonment.

DIGITAL CURRENCIES

RISK RATING

The risk of digital currencies being used to move and store funds for terrorism financing is assessed as **high**. The level of risk has increased since 2016, driven by technological and product advancements and greater consumer uptake. Digital currencies also remain exposed to a range of inherent vulnerabilities that create exposure to terrorism financing threats, and can complicate efforts to combat misuse.

A digital currency[28] is a type of currency that exists in digital rather than physical form. There are three main types of digital currency: cryptocurrency, stablecoin and central bank digital currency (CBDC). Terrorism financing risk in Australia relates to cryptocurrency and stablecoins only. Where the term 'digital currency' is used below, it refers specifically to these products. There is no intelligence base indicating CBDCs are used for terrorism financing.

INTELLIGENCE PICTURE

The use of digital currency by violent extremists across the ideological and religious spectrums is increasingly identified in Australia. This uptake coincides with international experience and reporting that threat actors are demonstrating an increased comfort in digital currency use, despite recent large-scale disruptions. For some IMVE actors in Australia, notably nationalist and racist violent extremists, digital currency is a key channel for moving and storing funds. The Hamas-Israel conflict has also seen an increased number of fundraising campaigns soliciting donations in digital currency.

In Australia, recent detections include direct low-value cryptocurrency flows from Australian entities to wallet addresses reportedly controlled by offshore terrorist organisations. However, the use of privacy coins and stablecoins have also been observed and will likely remain popular, particularly during periods of market volatility.[29]

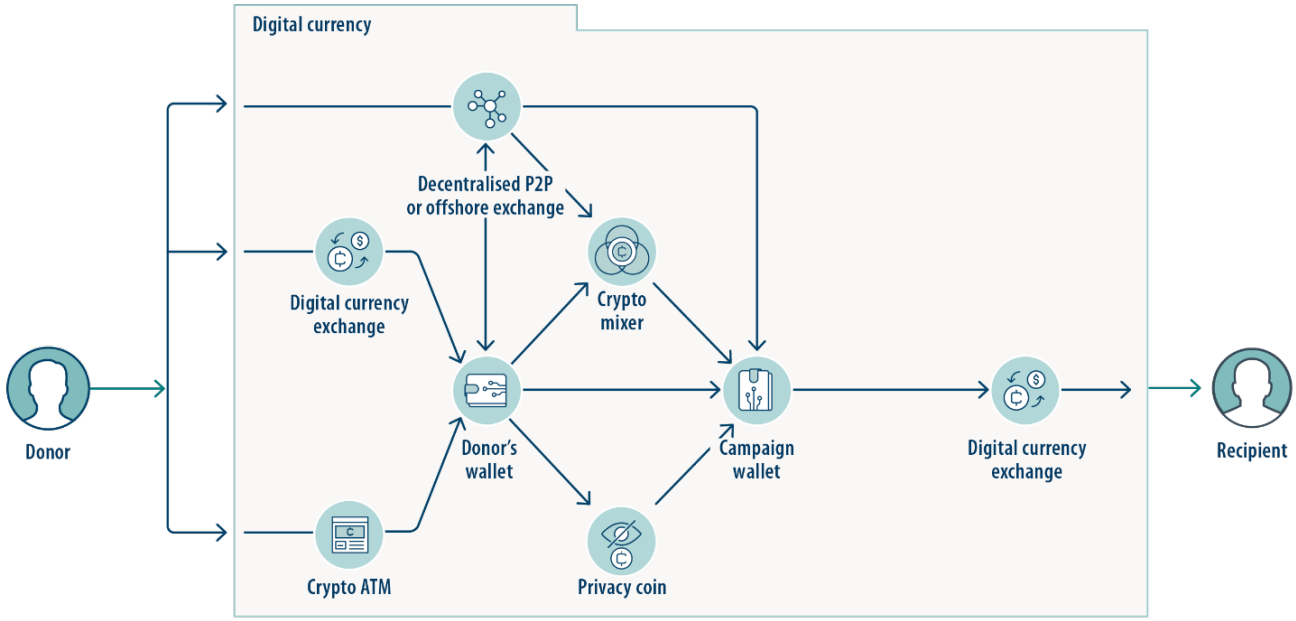
Other digital currency services that are likely misused for terrorism financing include:

[28] AUSTRAC's legislation references digital currencies whereas FATF and others use the broader term 'virtual assets'.

[29] Stablecoins are typically hedged against market volatility as they are said to be pegged against real assets, like the United States Dollar (USD). This provides stablecoin users with the ability to move USD values but with all the key advantages of a blockchain technology (i.e. de-centralised administration and near instantaneous transaction times).

- The transfer of coins through peer-to-peer (P2P) traders, within international or decentralised digital currency exchanges, to obscure the source and destination of funds.
- The use of crypto ATMs to on-ramp funds.
- The use of mixer services[30] to further the distance from the original source and wallet holder.

DIAGRAM 4: COMMON DIGITAL CURRENCY PRODUCTS/SERVICES IDENTIFIED IN TERRORISM FINANCING INVESTIGATIONS



VULNERABILITIES

- Digital currency offers speed, global reach, pseudonymity[31] and anonymity of financial transactions to criminal actors. The near-instant and irreversibility of transactions present a persistent challenge for digital currency exchanges in detecting and disrupting illicit transactions before funds leave wallets. This is further complicated given terrorism financing is usually low value and difficult to distinguish from legitimate transactions.
- The level of sophistication and knowledge required to buy, sell, and store digital currencies is relatively low. The infrastructure behind e-commerce and transactional applications on the blockchain allows market participants to trade and store cryptocurrencies quickly and easily, similar to sending and receiving money through internet banking applications.
- In Australia, digital currency exchange providers must register with AUSTRAC and comply with AML/CTF obligations, including identifying their customers, maintaining records and reporting transactions including suspicious matters to AUSTRAC. However, the regulatory framework only applies to the exchange of digital currency to fiat currency and the reverse. Australia is currently consulting on broad AML/CTF reforms, including the range of digital currency services that are captured in legislation. In addition, Australia is consulting on requirements that would

[30] A crypto mixer is a service that blends the cryptocurrencies of many users together to obfuscate the origins and owners of the funds.

[31] Pseudonymity can be defined as 'traceable anonymity' whereby under ordinary evaluation, identity cannot be determined. However, with technical procedures, association to an individual can be made.

extend FATF's 'Travel Rule' to digital currency transactions. The Travel Rule would require regulated businesses to identify all parties involved in transactions. Implementation of FATF's requirements would provide greater visibility of the ultimate beneficial ownership of digital currency assets, as well as parties to transactions.

- The use of offshore P2P platforms can reduce regulatory oversight of digital currency transactions. Transactions to un-hosted or self-hosted wallets also offer increased anonymity and privacy.
- The effectiveness of AML/CTF controls in digital currency exchange providers are generally of a moderate standard, with good compliance across the growing sector. However, given the infancy of the sector, many reporting entities assess their products, delivery channels and customers as low risk by default. Understanding of terrorism financing risk exposure may therefore be poor among some reporting entities.

OUTLOOK

The digital currency ecosystem will remain attractive to terrorist financiers so long as it maintains its core features of privacy, pseudonymity and accessibility. Innovation and adaptation from law enforcement agencies is required to sufficiently address the evolving threat. It remains an ongoing priority for AUSTRAC and partner agencies.

AUSTRAC should continue to provide guidance to registered digital currency exchange providers. Guidance should cover the assessment of risk exposure, compliance with AML/CTF obligations and should include the screening of transactions against sanctioned wallet addresses, entities and individuals. Additionally, AUSTRAC continue to work with national and international partners to increase and enhance its digital currency tracing capabilities.

CASE STUDY 14: AUSTRALIAN LINKS TO GLOBAL FINANCING CAMPAIGNS BY PROSCRIBED GROUPS

In August 2020, the U.S. Department of Justice announced its largest ever seizure of cryptocurrency linked to terrorism financing. The seizure involved Al-Qassam Brigades, the military wing of Hamas, al-Qa'ida and Islamic State. The operation seized over 300 cryptocurrency accounts reportedly holding a total of US$2 million (A$3 million), in cryptocurrency. The funds were raised through crowdfunding via social media platforms, websites and Telegram. The Department of Justice reported that in some instances, al-Qa'ida and affiliated groups purported to be charities.

AUSTRAC identified two instances of direct cryptocurrency flows from an Australian entity to these campaigns. The matters were referred to the AFP and led to investigations. In both cases, there was insufficient evidence to prove beyond a reasonable doubt that each individual was motivated to finance a terrorist group as opposed to an offshore front-facing humanitarian charity. Despite the increasing capabilities of authorities to detect illicit cryptocurrency transactions, securing sufficient evidence for a successful prosecution can be very difficult.

CASH EXCHANGE (DOMESTIC)

RISK RATING

The domestic exchange of cash poses a **high** terrorism financing risk. This risk has remained stable since 2016. Much of the risk comes from the high vulnerability cash use poses, rather than the volume and intensity of observed activity.

This category of risk refers to the exchange of cash between parties in Australia only. It does not include the movement or smuggling of cash offshore.

INTELLIGENCE PICTURE

Cash is used by violent extremists across ideological and religious spectrums and has been a common feature in attempted and completed lone-actor terrorist attacks. Observed uses of domestic cash exchange include: donating to purported charitable fundraisers or social media campaigns, the payment of membership fees (specific to IMVE actors), and the purchase of tactical equipment or weapons. Cash can also be pooled and provided to banks or remitters for transfer offshore.

VULNERABILITIES

- Cash is easy to access, transport and often will not trigger suspicion or reporting to AUSTRAC, even when it intersects with the formal economy. Particularly given the low values associated with terrorism financing in Australia.
- Cash affords high anonymity as ownership cannot be attributed, and transactions can occur outside the formal economy.
- Many reporting entities allow third party cash deposits. While many banks are enhancing mitigation strategies involving these deposits, third party transactions increase anonymity and can make it difficult to determine the source of funds.

OUTLOOK

The domestic exchange of cash for terrorism financing will remain an enduring risk over the next three years because of its accessibility and anonymity.

CASE STUDY 15: CASH TO FUND TRAVEL TO SYRIA AND IN SUPPORT OF ISLAMIC STATE

In 2018, an Australian national pleaded guilty to two terrorism financing offences contrary to s102.6 of the Criminal Code. The principal terrorism offence was his involvement in the terrorist attack at New South Wales Police Force headquarters by Farhad Mohammad. The offender was sentenced to 38 years imprisonment for all offences.

The first funding offence involved the offender providing $1,000 cash to Mohammad for provision to his radicalised sister. The cash was intended to fund her travel to Syria. The second offence involved the planning of facilitating the transfer of A$5,000 from Australia to Islamic State. The offender arranged to deliver the cash to a woman who was prepared to send the funds offshore. Ultimately the funds did not reach Islamic State.

CONSEQUENCES

The overall consequences of terrorism financing in Australia are assessed as **low** to **moderate**. Please refer to **Appendix A** for details of the data inputs and methodology used to measure consequences.

When financing leads directly to a terrorist attack, the levels of impact and harm are visible and almost always severe. However, the impacts and harm of terrorism financing that are not directly linked to an attack can be far less obvious, immediate and significant.

This assessment recognises that the nature of terrorism financing in Australia is small scale, low value, diffuse, and fragmentary. This means the link between terrorism financing and a terrorist attack is often weak, and makes assessing consequences associated with terrorism financing largely approximate. For example:

- A significant portion of suspected terrorism financing goes offshore to support overseas terrorist groups, violent extremists or Australian foreign fighters (and at times their families). This makes following the money trail difficult and determining the end-use challenging, if not impossible.
- Domestic terrorism financing is likewise often opaque. The purpose and likely consequence of financing can sometimes be ascertained through surveillance of groups and individuals, but the ultimate use of funds remains hazy.
- Terrorism financing for foreign fighter travel is more clear-cut, but the number of departing foreign fighters has declined following operational losses incurred by IS and other terrorist groups.
- As Australia has been able to detect and disrupt the vast majority of terrorist plots onshore, potential consequences associated with any financial element have been largely mitigated.

To address these challenges this assessment uses a mix of quantitative and qualitative inputs, and where possible, case studies and inductive methods are used. Broader political, social and economic

harms are considered and calibrated to fit Australia's experience with terrorism and terrorism financing.

This assessment considers the consequences of terrorism financing at a national level *only*. It does not assign a consequence score to each individual channel and method assessed in this report.

Estimates are made across two areas.

1. **Use of funds** (impact) examines the impact of terrorism financing cases in Australia based on how funds are ultimately used. It is assumed that funding used for operational purposes will have more severe consequences as it often culminates in attacks and physical harm.[32]
2. Estimates of **political, social and economic harms** are more theoretical in nature, and are based on observed and potential terrorism financing activity. A discussion of likely harms arising from terrorist attacks in Australia is also provided.

USE OF FUNDS

The overall impact of terrorism financing events is assessed to be **moderate**. In known and suspected cases of terrorism financing where the use of funds could be reasonably ascertained, funds were evenly used for both organisational costs and operational expenses.

RMVE actors send funds offshore to help support foreign fighters and overseas terrorist groups. Funds that remain onshore are most often used to purchase weapons in preparation for a terrorist act, or to develop and share materials that incite violence.

IMVE actors send funds offshore to help support overseas extremist organisations, and individuals supporting violent extremist views. Funds that remain onshore are used to purchase tactical gear and invest in recruitment and radicalisation activities. Funds do not appear to be used to support onshore attack-planning. There has also been an increase in purported charitable campaigns to support individuals charged with terrorism offences. It is not a criminal offence to fundraise in support of extremist organisations or to pay for an individuals' legal fees.

POLITICAL AND SOCIAL HARM

The overall level of political and social harm arising from instances of terrorism financing are assessed as **low**. Political and social harms of terrorism financing in the form of community discord; erosion of trust in government and liberal democratic norms; and polarisation have not been observed. The political side-effects of terrorism financing present some costs, but not of a lasting nature. Diplomatic friction might arise where Australia's CTF efforts are perceived as not meeting international standards or foreign partner expectations, but these are very infrequent and are often resolved.

Terrorism financing sourced from high-harm criminal activity (such as trafficking in drugs, humans and firearms, sexual servitude and cybercrime), contributes to related downstream social and economic harms.[33] However, this is only relevant for the purpose of this assessment when individuals engage in crime for the sole purpose of raising terrorism funds. These cases are not common and have primarily involved individuals committing fraud against federal government programs. As noted below, related

[32] Terrorism financing is used for a range of purposes. Generally, funding that is used for operational purposes will have more severe consequences culminating in attacks and physical harm. The consequences of funding for organisational purposes can be less immediate but help support terrorist actors and networks to conceal themselves, build operational capability, and prepare for and stage attacks. Organisational funding helps terrorist groups to recruit, expand networks and entrench their presence in communities.

[33] Social harm linked to criminal activity is well-documented and can manifest at personal, community and societal levels and range from minor to severe.

harm from these crimes is largely economic and any resulting political or social harm (e.g. in the form of public disapproval), is almost certainly minimal.

Social harm does arise when legitimate funds raised through NPOs are siphoned or diverted away from intended beneficiaries, both onshore and offshore, and vital services are not delivered. It is difficult to estimate the overall value of potential diversions, particularly those that occur offshore, and associated social harm. However, overall values in cases observed onshore and related social harms have been low.

ECONOMIC HARM

The overall level of economic harm arising from instances of terrorism financing are assessed as **low**. The small-scale, low-value nature of most Australian terrorism financing activity results in negligible harm on the overall economy. Where government revenue is lost from fraudulent activity, known and suspected cases indicate that any losses likely represent an extremely small fraction of overall government spending.

Financial institutions that have been linked to terrorism financing have likely suffered some reputational and economic damage. Particularly when regulatory action has been taken or an institution incurs costs necessary to repair brand image or increase capability to mitigate threats. However, damage is more due to exposure of general non-compliance than any serious terrorism financing concerns.

Terrorism financing through an NPO can likewise impact its reputation and result in a number of increased costs, as well as loss of public trust and charitable donations. For smaller organisations, this could result in job losses or the NPO ceasing operations. This then carries flow-on harms for intended beneficiaries who do not receive needed assistance. Nonetheless, sector representatives report economic harms linked to terrorism financing and adverse media more generally, are usually short-term in nature.

APPENDIX A: LIKELIHOOD AND CONSEQUENCE MATRICES

LIKELIHOOD MATRIX

RISK FACTORS			
	LOW	**MEDIUM**	**HIGH**
THREAT **e.g. level of misuse**	**LOW** The channel/method is rarely used for terrorism financing.	**MODERATE** The channel/method is sometimes/intermittently used for terrorism financing.	**HIGH** The channel/method is more commonly used for terrorism financing.
VULNERABILITY			
PROFITABILITY **e.g. opportunity to raise/move/store large volumes of funds**	**LOW** The channel/method likely limits only small amounts[34] to be raised/moved/stored.	**MODERATE** The channel/method likely enables modest amounts to be raised/moved/stored.	**HIGH** The channel/method likely enables larger amounts to be raised/moved/stored.
ACCESSIBILITY **e.g. relative cost and barriers to access, including to/from foreign jurisdictions**	**DIFFICULT** Many barriers to access and/or costs more than other financing options.	**MODERATE** Some barriers to access and/or may cost more than other financing options.	**EASY** Few or no barriers to access and/or costs less than other financing options.
EASE OF USE **e.g. knowledge and/or technical expertise and support required**	**DIFFICULT** Requires more planning, knowledge and/or technical expertise than other options.	**MODERATE** Requires some planning, knowledge and/or technical expertise.	**EASY** Requires little planning, knowledge and/or technical expertise compared to other options.
DETECTION **e.g. ability for terrorism financing to be identified and reported to authorities**	**LIKELY** Illicit transactions are relatively easy to detect and are routinely reported or visible to authorities.	**LIMITED** Illicit transactions are sometimes detected and reported or visible to authorities.	**DIFFICULT** Illicit transactions are difficult to detect and/or are rarely reported or visible to authorities.
DISRUPTION **e.g. ability for authorities to investigate and prosecute or disrupt terrorism financing offences**	**LIKELY** Authorities face few challenges in successfully investigating and prosecuting or disrupting offences.	**LIMITED** Authorities face some challenges in successfully investigating and prosecuting or disrupting offences.	**DIFFICULT** Authorities face a number of challenges in successfully investigating and prosecuting or disrupting offences.

[34] Given the much lower amounts of funds needed for terrorism financing generally and that particularly characterise Australia's terrorism financing context, assigning figures in dollars to this measure is problematic. Refer to the case studies in this assessment for examples of the amount of funds in known or suspected Australian cases.

CONSEQUENCE MATRIX

RISK FACTORS	LOW	MODERATE	HIGH
IMPACT: USE OF FUNDS	**LOW** Terrorism financing is more often used to support organisational costs such as propaganda, meetings and recruitment, salary payments to members, or payments to widows, orphans and families of dead fighters and terrorist actors.	**MODERATE** Terrorism financing is evenly used for both organisational costs and operational expenses.	**HIGH** Terrorism financing is more often linked to a terrorist act or weapons, vehicle, explosives, equipment, training or other activity to prepare to undertake a terrorist act; foreign fighter travel to conflict zones; or sent directly (or indirectly) to recognised foreign terrorist groups.
POLITICAL AND SOCIAL HARM	**LOW** Instances of terrorism financing are unlikely to erode trust and confidence in the Australian government; and are unlikely to cause high levels of social discord.	**MODERATE** Instances of terrorism financing are likely to erode a moderate level of trust and confidence in the Australian government; and are likely to cause a moderate level of social discord.	**HIGH** Instances of terrorism financing are likely to erode a significant level of trust and confidence in the Australian government; and are likely to cause a significant level of social discord.
ECONOMIC HARM	**LOW** Instances of terrorism financing do not erode Australia's financial performance or reputation, and do not affect the broader Australian financial system.	**MODERATE** Instances of terrorism financing moderately erode Australia's financial performance or reputation, and somewhat affect the broader Australian financial system.	**HIGH** Instances of terrorism financing significantly erode Australia's financial performance or reputation, and significantly affect the broader Australian financial system.

APPENDIX B: SURVEY RESULTS

INTERNATIONAL FIU SURVEY

The international FIU survey was issued to 67 FIU partners. In total, 35 FIUs responded. An overview of key responses is below.

18 FIUs

- Say Australia poses a **very low** or **low** TF risk to their jurisdiction.

2 FIUs

- Say Australia poses a **moderate** or **high** TF risk to their jurisdiction.
- Risk stems from Australians sending funds to local suspected terrorists.

15 FIUs

- Say they cannot make an assessment of TF risk posed by Australia because they do not have sufficient data holdings.
- However, all 15 FIUs note they have **no recorded TF interactions** involving Australia, and they do not believe there are TF links between their jurisdiction and Australia.

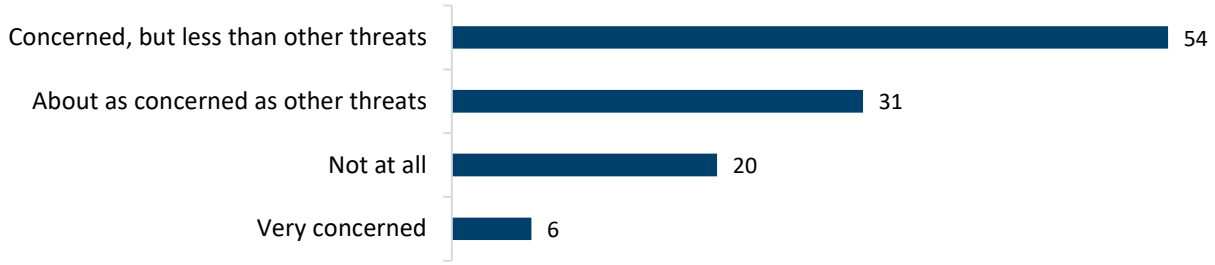
4 FIUs

- Have identified possible TF involving Australia. Of these:
  - all cases involved used of remittance or banking channels
  - three cases involved outgoing transfers from Australia
  - one case involved an incoming transfer to an Australian espousing IMVE views.

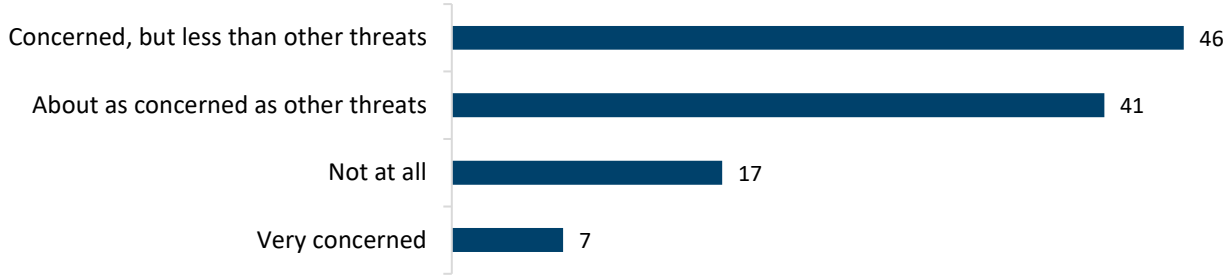
INDUSTRY SURVEY

The industry survey was issued to approximately 60 reporting entities and 21 industry associations across the banking, gambling, remittance, bullion and digital currency sectors. In total, 111 individuals responded. Responses to four key questions are below.

HOW CONCERNED ARE YOU OF YOUR BUSINESS'S EXPOSURE TO TERRORISM FINANCING?



HOW CONCERNED ARE YOU OF YOUR BUSINESS'S ABILITY TO COUNTER TERRORISM FINANCING?



DOES YOUR BUSINESS OR YOUR CUSTOMERS CONDUCT BUSINESS WITH NATIONALS OF COUNTRIES YOU CONSIDER TO BE A TERRORISM FINANCING RISK?

IN YOUR OPINION, WHAT ARE THE GREATEST CHALLENGES YOUR BUSINESS FACES WHEN IT COMES TO COUNTERING TERRORISM FINANCING?

The majority of responses can be summarised by the following five statements:

- Detection of suspicious transactions and threat actors.
- Keeping abreast of emerging terrorism financing risk indicators, including limited information sharing within industry and guidance from government agencies.
- Lack of public and government registers to help verify customer identification.
- Digitisation of the financial ecosystem and the speed of transactions—making it much harder to prevent and detect high-risk activity due to the speed of transactions.
- Limited personnel and resources to perform robust CTF activities, including monitoring sanctions lists and investigating hits.

AUSTRAC.GOV.AU