Australian Government

Australian Transaction Reports and Analysis Centre

Terrorism financing in Australia 2014

AUSTRAC contact details

If you have enquiries about the Australian Transaction Reports and Analysis Centre (AUSTRAC), obligations under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* or other related information, please contact the AUSTRAC Help Desk:

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

Email: help_desk@austrac.gov.au

Post: PO Box 5516 West Chatswood NSW 1515

The Help Desk operates from 8.30am to 5.00pm, Monday to Friday.

Information is also available on AUSTRAC's website at **www.austrac.gov.au**

© Commonwealth of Australia 2014

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Where material has been sourced from other third-party sources, copyright continues.

Requests and enquiries concerning reproduction and rights for commercial use should be addressed to corporatecommunications@austrac.gov.au

Terrorism financing in Australia 2014

foreword

Terrorism financing poses a serious threat to Australians and Australian interests at home and abroad. At its most damaging, it can fund the activities of domestic extremists, including attacks on Australian soil. More commonly, terrorism financing raised in Australia can help sustain terrorist groups overseas and support foreign attacks and insurgencies.

Terrorism financing also poses a threat to the credibility of Australia's financial institutions and financial system. Even an unwitting association with terrorism financing involving small amounts of money could damage the reputation of Australian financial institutions, companies and not-for-profit organisations and harm Australia's global image.

The extent of terrorism financing in Australia is much smaller than money laundering. Both crimes employ similar techniques to conceal financial transactions, although terrorism financing usually involves smaller amounts of money. This fact makes it more difficult for both authorities and industry to detect suspicious transactions among the significant volume of legitimate transactions that occur every day.

No government, however well equipped, can tackle terrorism financing alone. AUSTRAC and its domestic partner agencies rely on partnerships with industry and the Australian community to help uncover and report suspicious activity.

Cooperation with industry and international counterparts helps deepen Australia's understanding of current and emerging illicit financial activities. This strengthens our ability to combat terrorism financing and ultimately protect the wider community against the threat of terrorist activity in Australia and abroad.

AUSTRAC has produced this public *Terrorism financing in Australia 2014* report to strengthen the nation's defences against terrorism financing by improving industry and public awareness of the risks. The report uses real cases and intelligence to present a consolidated picture of Australian terrorism financing risks, vulnerabilities and methods.

AUSTRAC will continue to work with its partner agencies, industry and international counterparts to create an Australian community that is hostile to terrorism financing, money laundering and associated crime.

John L Schmidt

Chief Executive Officer

AUSTRAC

contents

purpose

AUSTRAC has prepared this *Terrorism financing in Australia 2014* report to raise awareness and strengthen the national response to the serious threat of terrorism financing. The report is based on a classified national risk assessment of the Australian terrorism financing environment completed by AUSTRAC in 2014 in collaboration with a number of key partner agencies, particularly the Australian Federal Police (AFP).

This public report presents a consolidated picture of the Australian terrorism financing environment – current and emerging risks and threats, the channels used to raise and transfer funds, indicators to help identify suspicious activity, and the legal and regulatory framework in place to help deter and detect terrorism financing. While classified and sensitive information has been excluded from this public report, its key findings and terrorism financing methodologies, trends and observations are consistent with the classified national risk assessment.

This information will assist government, industry and the Australian community to better understand terrorism financing risks and vulnerabilities and implement appropriate prevention measures. The report will also educate key community groups on the risks associated with sending funds to high-risk overseas destinations and recipients and promote understanding of AUSTRAC's role and contribution to combating terrorism financing.

Terrorism financing in Australia 2014 complements AUSTRAC's *Money laundering in Australia 2011* report to provide an overall picture of the Australian money laundering and terrorism financing environment. Combined with AUSTRAC's annual typologies and case studies reports, these reports provide AUSTRAC's reporting entities with valuable background information to assess the specific risks affecting their business.

As the global terrorism financing environment is dynamic and rapidly changing, this report should be considered alongside any recent developments that may affect Australia's terrorism financing risk.

How does AUSTRAC combat terrorism financing?

AUSTRAC's purpose is to protect the integrity of Australia's financial system and contribute to the administration of justice through its expertise in countering money laundering and terrorism financing. It does this in two ways: as the national anti-money laundering and counter-terrorism financing (AML/CTF) regulator and as Australia's financial intelligence unit (FIU).

As the regulator, AUSTRAC monitors compliance with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and takes enforcement action where necessary against breaches of the Act.

In its capacity as Australia's FIU, AUSTRAC analyses financial transaction information and works with partner agencies, industry and international counterparts to identify patterns of suspicious activity and contribute to law enforcement operations.

key features of the Australian terrorism financing environment

A risk to Australia's national security

Terrorism financing is a risk to Australia's national security, financial system, commercial organisations and not-for-profit organisations (NPOs). Primarily, terrorism financing is a national security risk as it can directly enable terrorist acts both in Australia and overseas. In Australia, individuals have been convicted of terrorism offences and funds have been raised to support domestic activity and overseas terrorist groups.

In addition to funding individual terrorist attacks and operations, terrorism financing helps establish and maintain terrorist groups in Australia and foreign countries and sustains the networks that connect them. Terrorism financing supports the less violent or obvious aspects of a group's operations by paying for daily living expenses, travel, training, propaganda activities, organisational costs, and compensation for wounded fighters or the families and dependants of terrorists who have died.

Terrorism financing also poses significant risks to any organisation involved in the activity, even if their involvement is unwitting. It can severely damage the reputation of financial institutions misused as part of the process. The integrity and work of non-government organisations such as charities and humanitarian groups can be seriously undermined if they are misused as a cover for terrorism financing activity.

AUSTRAC has identified three key features of the Australian terrorism financing environment:

- **Terrorism financing is largely motivated by international tensions and conflicts.** Communal and sectarian links between groups overseas and individuals in Australia drives Australian involvement in terrorism financing.
- **Use of conduit countries.** In recent cases, those sending funds out of Australia for terrorism financing tend to use conduit countries rather than send the funds directly to high-risk jurisdictions. This makes it more difficult for financial institutions to link the international funds transfers directly to terrorism financing. Conduit countries may also be used in an attempt to evade United Nations Security Council sanctions and Australian autonomous sanctions.
- **Commingling legitimate funds with funds collected for terrorist groups.** This is especially the case for donations collected through charities and NPOs. Commingling can disguise funds raised for terrorism financing among legitimate donations. It can also add to the total pool of funds directed towards a terrorist group.

International dimensions

Australia's terrorism financing environment is largely influenced by international factors, particularly sectarian and other conflict in foreign countries beyond Australia's immediate region. Recent turmoil in parts of the Middle East and Africa raises significant terrorism financing risks for Australia. Links exist between terrorist groups in these regions and radicalised individuals or members of communities in Australia. Overseas conflicts have prompted some Australians to travel abroad to take part in combat and terrorist or paramilitary training or to financially support armed political or terrorist groups.

Currently, the conflicts in Syria and Iraq pose the most significant terrorism financing risks to Australia. Australian terrorism financing risks relating to the Syrian conflict are discussed in more detail below. Yemen and Somalia also pose ongoing terrorism financing risks and Australians have provided financial support to, and travelled to train or fight with, terrorist groups in these countries.

Global terrorism financing risks may change quickly and unexpectedly where extremist groups become involved in regional conflicts. Such scenarios can have a significant impact on the Australian terrorism financing risk environment. The rapidly changing security situation in Iraq is a case in point. At the time of publication, the Islamic State[1] occupied large parts of Iraq and presented a significant threat to the Government of Iraq. With the involvement of some Australians in the conflict in Iraq, the risk of terrorism financing involving Australia in relation to Iraq is likely to have increased.

Syria

Australians have travelled to Syria to illegally engage in the conflict, raising a concern that they will join terrorist groups engaged in fighting. This raises a significant risk that either they or their supporters will raise funds for terrorism-related purposes in Syria. At least two groups listed as terrorist organisations by the Commonwealth Government, Jabhat al-Nusra (al-Nusra) and the Islamic State, are engaged in conflict against the Syrian regime. Hizballah has aligned itself with the Syrian regime, and Hizballah's External Security Organisation is listed as a terrorist organisation in Australia.

Terrorist groups active in Syria have links with radicalised individuals in Australia. The large volume of humanitarian aid and financial assistance sent from Australia to family and community members in Syria provides opportunities for commingling or disguising funds for terrorism financing among the legitimate transactions. Conflict in Syria creates a dynamic environment for terrorism financing, which may lead to the use of new methods of fundraising and transferring funds.

Neighbouring countries including Lebanon, Turkey, the United Arab Emirates and Jordan have been used as conduits to route money destined for terrorist groups in Syria. These jurisdictions are targeted due to the comparative stability of their financial sectors and because funds sent to these countries are less likely to attract attention than those sent directly to Syria. Cash may also be physically couriered into these conduit countries from Australia and carried overland across the border into Syria.

1 Formerly known as Islamic State of Iraq and the Levant (ISIL)

Current and emerging terrorism financing channels

In the short-to-medium term a number of channels are likely to pose an increased risk of being misused for terrorism financing:

» **Self-funding** from legitimate sources being used to pay travel and living expenses for Australians to fight alongside terrorist groups overseas. Family and associates in Australia have also knowingly or unwittingly transferred their own legitimately obtained funds to persons engaged in conflict. There is also a significant risk that self-funding may be used to fund the activities of any 'lone wolf' extremists within Australia. Lone wolf extremists act alone to plan or carry out violent acts in support of a group or ideology, without support or assistance from any group.

» There is a significant risk that the **cross-border movement of cash** may be used as a channel by Australians travelling overseas to fund terrorist groups and activity. The risk is heightened when Australians travel to Syria and neighbouring countries.

» In Australia, the **banking** and **remittance sectors** are used more frequently than other channels to send funds to individuals engaged in foreign insurgencies and conflicts, some of whom are also suspected of engaging with terrorist groups. This largely reflects the central role of the banking sector in Australia and the utility of the remittance sector to move smaller amounts of money to jurisdictions where formal financial channels are less accessible.

» **Online payment systems** may be used to collect donations and transfer funds to extremists in Australia and overseas. The use of online payment systems may correspond with the use of social media by terrorist groups and extremists to radicalise, recruit and communicate with sympathisers.

» **Stored value cards** and credit/debit cards may be used by Australians linked to foreign terrorist groups to access funds overseas.

» **Charities and NPOs** may be used to raise funds for groups engaged in foreign conflict and as a cover to transfer funds offshore. Funds for legitimate humanitarian aid may also be diverted in Australia, or at their destination, and used to support terrorist groups.

Terrorism financing indicators

Terrorism financing indicators are often indistinguishable from money laundering indicators. Terrorism financing often, but not always, involves smaller amounts of money than when illicit criminal funds are laundered. Funds intended for terrorism may also be derived from legitimate rather than illicit sources, making terrorism financing more difficult to detect.

Reporting entities may not always be able to draw a link between suspicious customer activity and terrorism activities. However, any suspicious matter reported to AUSTRAC may provide a small but critical piece of a larger puzzle. Information from reporting entities can be crucial in terrorism financing investigations when linked to other information held by AUSTRAC and its partner agencies.

The presence of a single indicator may not necessarily raise a suspicion, but could warrant further monitoring and examination. Multiple indicators are more likely to result in a suspicion being formed. Additionally, a reporting entity's overall knowledge of a customer, including the customer's established financial transaction history, can be as important as any of the indicators below in forming a suspicion of terrorism financing.

Terrorism financing indicators include:

- Structured[2] cash deposits and withdrawals, and international funds transfers to high-risk jurisdictions.[3] These transactions may be conducted at multiple branches of the same reporting entity
- Multiple customers conducting international funds transfers to the same beneficiary located in a high-risk jurisdiction
- A customer conducting funds transfers to multiple beneficiaries located in the same high-risk jurisdiction
- A customer using incorrect spelling or providing variations on their name when conducting funds transfers to high-risk jurisdictions
- Transfer of funds between business accounts and personal accounts of business officeholders which is inconsistent with the type of account held and/or the expected transaction volume for the business
- Large cash deposits and withdrawals to and from NPO accounts
- Operating a business account under a name that is the same as (or similar to) that used by listed entities[4] in Australia and overseas

2 'Structuring' is a money laundering technique which involves the deliberate division of a large amount of cash into a number of smaller deposits or transfers (including international funds transfers) to evade reporting requirements or other scrutiny.

3 'High-risk jurisdictions' can be destinations or conduits for terrorism financing funds flows from Australia, jurisdictions subject to sanctions or jurisdictions with links to listed terrorist organisations.

4 See section on 'Australia's AML/CTF regulatory framework' for additional information on listed entities and sanctions regimes applicable in Australia.

- Individuals and/or businesses transferring funds to listed terrorist entities[5] or entities reported in the media as having links to terrorism
- Funds transfers from the account of a newly established company to a company selling chemicals that could be used in bomb making
- Multiple low-value domestic transfers to a single account and cash deposits made by multiple third parties, which could be indicative of fundraising for terrorism financing
- Sudden increase in account activity, inconsistent with customer profile
- Multiple cash deposits into personal account described as 'donations' or 'contributions to humanitarian aid' or similar terms
- Transfers through multiple accounts followed by large cash withdrawals or outgoing funds transfers overseas
- Multiple customers using the same address and telephone number to conduct account activity
- Proscribed entities or entities suspected of terrorism using third-party accounts (for example, a child's account or a family member's account) to conduct transfers, deposits or withdrawals

5 Ibid

Australia's counter-terrorism financing framework

Australia's AML/CTF regime

Australia's robust AML/CTF regime is the result of close collaboration between AUSTRAC, Australian businesses, domestic partner agencies, governments and international counterparts.

The AML/CTF Act and *Financial Transaction Reports Act 1988* (FTR Act) provide the foundation for Australia's regulatory regime to detect and deter money laundering and terrorism financing. The AML/CTF Act applies to 'designated services' provided by a wide range of financial institutions, the gambling industry (including casinos, bookmakers and gaming machine venues), bullion dealers and designated remittance service providers.

The FTR Act regulates certain 'cash dealers' and solicitors which are not reporting entities under the AML/CTF Act.

Entities providing a 'designated service' under the AML/CTF Act are 'reporting entities' and are subject to a range of obligations. These include:

- enrolling with AUSTRAC as a reporting entity (and also registering if they provide a designated remittance service)
- conducting customer identification, verification, ongoing due diligence and transaction monitoring
- reporting suspicious matters, threshold transactions (cash or certain e-currency transactions of AUD10,000 or more) and international funds transfer instructions
- conducting a money laundering and terrorism financing risk assessment
- developing and maintaining an AML/CTF program
- conducting AML/CTF training for employees and agents
- making and retaining certain records for seven years.

The AML/CTF Act also requires the reporting of cross-border movements of physical currency (whether carrying, mailing or shipping) and, upon request, bearer negotiable instruments (BNIs) such as cheques, travellers cheques and money orders (when carried by an individual).

Terrorism financing offences

The *Criminal Code Act 1995* (the Criminal Code) creates a number of offences for individuals who engage in, train for, prepare, plan, finance or provide support for terrorist acts. Individuals who are members or supporters of terrorist organisations also commit a criminal offence. An organisation may be found to be a terrorist organisation by a court as part of a prosecution for a terrorist offence, or it may be specified by the Commonwealth Government in Regulations, a process known as 'listing'.[6]

6 A current list of terrorist organisations listed under the Criminal Code is available at www.nationalsecurity.gov.au

Division 103 of the Criminal Code contains specific offences for financing terrorism. In general terms, a person commits an offence if they make funds available to another person, provide funds or collect funds and are reckless as to whether the funds will be used to facilitate, or engage in, a terrorist act. An offence is committed even if a terrorist act does not occur or if the funds will not be used towards a specific terrorist act. A person can be convicted of this offence even if it occurs outside Australia. The maximum penalty is imprisonment for life.

UNSC and Australian autonomous sanctions

United Nations Security Council (UNSC) sanctions regimes, including in relation to Al Qaida and terrorism more generally, are given effect in Australia primarily through the *Charter of the United Nations Act 1945* and corresponding regulations. Of relevance to terrorism financing, these sanctions regimes may impose targeted financial sanctions against listed persons and entities, which include asset freezes and prohibitions on providing funds or other assets to them, and travel bans on listed persons.

Australia also imposes autonomous sanctions regimes, which may supplement UNSC sanctions regimes or be separate from them. Australia's autonomous sanctions regimes are primarily implemented under the *Autonomous Sanctions Act 2011* and corresponding regulations.[7]

Penalties for individuals who breach Australian sanction laws include imprisonment for up to 10 years and/or a fine of AUD425,000 or three times the value of the transaction, whichever is greater. Bodies corporate can be fined AUD1.7 million or three times the value of the transaction, whichever is greater.

Foreign incursion offences

It is an offence for Australians to enter a foreign country with the intention to engage in hostile activities in that country. These offences are contained in the *Crimes (Foreign Incursions and Recruitment) Act 1978*, which also includes offences relating to providing support to other persons intending to enter a foreign country for the purposes of engaging in hostile activities, including the provision of funds and goods.

International AML/CTF standards

Australia's AML/CTF regime is based on international standards developed by the Financial Action Task Force (FATF). These standards, known as the FATF recommendations, form the basis for a coordinated international response to combat money laundering, terrorism financing and proliferation of weapons of mass destruction.[8]

Since 1989, FATF has led international efforts to counter the abuse of the international financial system by criminals. It is the major multilateral body for setting and promoting the implementation of international AML/CTF standards.

7 More information on UNSC and Australian autonomous sanctions regimes can be found at www.dfat.gov.au/sanctions

8 See the 2012 FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, on the FATF website: http://www.fatf-gafi.org

terrorism financing in Australia

'...Terrorism financing in Australia varies in scale and sophistication, ranging from organised fundraising by domestic cells which are part of a larger, organised international network, to funds raised by small, loosely organised and self-directed groups....'

Australia's terrorism financing context

Australia and its offshore interests continue to face terrorist threats from individuals and groups who have identified Australia as a specific target. In the past, Australians have been the specific targets of overseas terrorist attacks, while others travelling and working overseas have fallen victim to terrorist attacks directed at others. Individuals in Australia have also been charged with and convicted of terrorism offences.

The amounts of funds generated to finance terrorism vary between groups. Funds raised by groups that are part of an international network can be significant, particularly those with accounts and business fronts established overseas. These groups have the financial infrastructure to undertake sizeable fundraising and money transfer operations.

Small domestic groups and lone wolf terrorists are also a significant terrorism financing risk. While the amounts raised by these radicalised groups or individuals are much smaller, their intent to undertake violent acts in Australia can pose a direct threat to the Australian community.

What is terrorism financing and how does it occur?

Terrorism financing is the financial support, in any form, of terrorism or of those who encourage, plan or engage in terrorism. It generally falls into two broad categories:

- funding the direct costs associated with undertaking terrorist acts – for example, expenses for travel, explosive materials, weapons and vehicles
- funding required to maintain a terrorist network, organisation or cell.

Terrorism financing in Australia varies in scale and sophistication, ranging from organised fundraising by domestic cells which are part of a larger, organised international network, to funds raised by small, loosely organised and self-directed groups. Smaller groups may raise funds for their own domestic use, as well as provide funding to overseas groups with whom they sympathise.

The terrorism financing process

The terrorism financing process typically involves three stages:

- **raising funds** (such as through donations, self-funding or criminal activity)
- **transferring funds** (to a terrorist network, organisation or cell)
- **using funds** (for example, to purchase weapons or bomb-making equipment, for payment to insurgents, or covering living expenses for a terrorist cell).

Funds also need to be 'stored' at each stage of the terrorism financing process. Storage methods can range from hiding cash in a private residence or in a 'sandooq' (cash box) to depositing funds in a bank account or other financial product.

These stages may not be present or clear-cut in all cases of terrorism financing. For financing of larger terrorist organisations, funds may be transferred through different levels of a network's structure – for example, from an Australian cell that raised the funds, to a governing branch of a terrorist group overseas and then on to a local cell in a foreign country. Simpler cases may involve an Australian individual directly funding an overseas insurgent or their own domestic activity.

Funds used to finance terrorism are considered an 'instrument of crime' (which are either illicit or legitimate funds directed towards a criminal purpose). In this way, funds used to finance terrorism are similar to funds used in the commission of most other crimes (for example, a payment for a drug shipment). The three-stage process described above can also describe the flow of money involved in other crime types. However, one significant difference between terrorism financing and other crime types is that most terrorism financing in Australia originates from ostensibly legitimate sources and activities.

7

raising funds to finance terrorism

'...The risks associated with the misuse of charities and NPOs are high as these organisations offer the capacity for groups to raise relatively large amounts of money over time...'

Terrorism fundraising methods vary based on the sophistication and aim of terrorist groups. Smaller groups and individual actors may require only modest amounts of money which are more difficult to detect through AML/CTF transaction monitoring systems. Groups with a larger support base require larger amounts of funding to support more sophisticated organisational structures and ongoing operational costs (such as the costs of travel, training and combat or staging attacks). These greater costs may require the use of larger scale and more organised fundraising methods.

Key channels used to *raise funds* for terrorism financing in or from Australia include:

- charities and NPOs
- self-funding from legitimate sources
- fraud, theft and drug trafficking
- ransom payments.

Charities and not-for-profit organisations

Some Australia-based charities and NPOs have been exploited by terrorist groups to raise relatively large amounts of money over time. These organisations can be exploited in a number of ways:

- Charities and NPOs can be used to disguise international funds transfers to high-risk regions.
- Funds raised for overseas humanitarian aid can be commingled with funds raised specifically to finance terrorism.
- Funds sent overseas by charities with legitimate intentions can also be intercepted when they reach their destination country and siphoned off for use by terrorist groups.

The risks associated with the misuse of charities and NPOs are high as these organisations offer the capacity for groups to raise relatively large amounts of money over time. However, this risk should be considered in the context of the relatively low incidence of terrorism financing in Australia, and the low value of funds suspected to have been raised in Australia to date. While charities and NPOs are one of the more significant Australian terrorism financing channels, they have not featured in a large number of Australian terrorism financing cases. Rather than representing a sector-wide risk, terrorism financing in Australia has been limited to a handful of charities and NPOs.

Domestic charities and NPOs are at risk of being misused by overseas terrorist groups which have a supporter base among communities in Australia. Some donors may willingly provide donations to support the groups, while other donors, and the charities themselves, may be coerced, extorted or misled about the purpose of funding.

Charities and NPOs which operate in crises and war zones overseas are at risk of being infiltrated and exploited by terrorist groups in these areas. Funds sent to Syria and neighbouring countries for humanitarian aid are at increased risk of being used for financing terrorism if they are sent through less-established or start-up charities and NPOs.

Those wanting to send funds to Syria for family and humanitarian purposes are advised to do so by donating to a United Nations humanitarian agency or to an Australian humanitarian organisation. The Australian Council for International Development website (www.acfid.asn.au) lists a number of Australian humanitarian organisations accepting donations for humanitarian aid in Syria. Further information on providing financial support to family, friends or humanitarian efforts in Syria is available at www.livingsafetogether.gov.au.

Self-funding from legitimate sources

Smaller groups or individuals acting alone may seek to fund their activities themselves using legitimate sources, allowing them to raise small-to-moderate amounts of money relatively inconspicuously.

In these cases, it can be difficult for financial institutions to distinguish transactions intended to finance terrorism activities from ordinary day-to-day transactions – in both cases the funds come from legitimate sources that are unlikely to attract suspicion. For smaller extremist groups and lone wolf actors, self-funding may provide them with sufficient resources to carry out an unsophisticated but high-impact attack.

Self-funding can be as simple as a single extremist using legitimately obtained funds (in cash or from a bank account) to make purchases to support a terrorism-related cause. The purchases could be for travel or training, or equipment needed to carry out an attack; for example, weapons or bomb-making supplies.

Small, loosely organised Australian extremist groups have been observed pooling regular contributions from members. In at least one Australian terrorism case (featured on page 17), a cash box known as a 'sandooq' was used to collect financial contributions. Cash contributions such as these can be easily concealed and do not require interaction with AML/CTF regulated sectors.

case study

Suspects raised funds in preparation for acts of terrorism[9]

Funds associated with the financing of terrorism can be derived from legitimate sources, including the incomes of individuals or community donations, or through the proceeds of non-terrorism related crimes (including fraud or robbery). By using a diversity of funding sources, those planning acts of terrorism may attempt to distance themselves from the origin of the funds generated to finance those acts.

The following two related cases illustrate the challenge of identifying terrorism financing, given that it may model normal patterns of financial behaviour, be undertaken through low-value transactions, or not involve the financial sector at all.

Part A – Sydney

A joint investigation led to the arrest of nine Sydney suspects who authorities suspected were planning an act of terrorism in conjunction with thirteen Melbourne suspects. The group's activities included military-style training and purchasing materials they planned to use to manufacture explosives.

The investigation revealed that the Sydney-based suspects relied mainly on their own incomes and efforts to fund their training activities and purchases, using their own bank accounts. Members of the group were caught shoplifting batteries, maps and electronic timers. Investigating officers also located stolen railway detonators during the execution of search warrants.

The Sydney suspects regularly used false names to register mobile phones when purchasing supplies and materials for their activities. For example, members of the group established companies in false names and used these companies to avoid suspicion when ordering and purchasing chemicals.

Four members of the Sydney group pleaded guilty to various terrorism offences and received sentences of imprisonment ranging between four years and eight months and 18 years and eight months. The remaining five members were found guilty by a jury of conspiring to commit an act in preparation for a terrorist attack under the *Criminal Code Act 1995* and sentenced to periods of imprisonment ranging from 23 to 28 years.

Part B – Melbourne

The same joint investigation also led to the arrest of thirteen Melbourne suspects who, in conjunction with the Sydney suspects, were planning an act of terrorism. The Melbourne group also undertook military-style training and purchased materials to manufacture explosives.

Investigations revealed that the Melbourne-based group funded their planned activities primarily through a series of small cash donations made by the group members to a central fund, known as the 'sandooq' (traditionally a box where all financial contributions were held).

9 *AUSTRAC typologies and case studies report 2011*, Australian Transaction Reports and Analysis Centre, Case 1, pp16–17.

One individual was alleged to have been the treasurer and holder of the sandooq. Another group member approved group members to use funds from the sandooq. All members contributed to the sandooq, with some contributing AUD100 per month. The fund was worth approximately AUD19,000 at the time the group was arrested.

The suspects were also engaged in systematic credit card fraud, whereby they paid taxi drivers to provide them with the credit card numbers of unsuspecting taxi passengers. In addition, third parties provided the group with extra funds raised from a car re-birthing racket.

The group undertook the fundraising activities for the purpose of purchasing weapons and materials for a planned terrorist attack.

Two members of the group pleaded guilty to being a member of a terrorist organisation and were sentenced to five years and five-and-a-half years imprisonment. Seven members of the group were found guilty of terrorism offences and sentenced to between six years and 15 years imprisonment. Four members of the group were acquitted of all charges.

Indicators

- Low-level payments undertaken through accounts and low-value cash withdrawals (below the AUD10,000 threshold)
- Use of false identification to establish Australian companies
- Multiple individuals contributing cash to a central fund (sandooq)

Fraud, theft and drug trafficking

Funds from criminal activity such as fraud, theft and drug trafficking have been linked to Australian terrorism cases. However, in Australia, ostensibly legitimate fundraising activities are more frequently used to fund terrorism than criminal activities. This is in contrast with the international situation, where criminal activity features in a larger number of terrorism financing cases.

The low incidence of terrorism-related criminal activity is one factor that currently distinguishes Australia's risk environment from that of other democratic and economically advanced countries.

Criminal activity can generate large sources of funds reasonably quickly, making it attractive to terrorist groups. In particular, small cells and individual sympathisers may turn to crime if they have no other significant source of income or wider support network. In Australia, members of extremist groups have had existing criminal links rather than turn to crime specifically to raise funds for the group or to fund operations and attacks.

Terrorist groups also face significant risks when raising funds from criminal activity as they face a greater chance of being detected by law enforcement. To obscure the ownership of the funds and distance individuals from the predicate offence, the groups may attempt to launder the criminal proceeds. Attempts to launder money lead to an increased chance of being detected by reporting entities and reported to AUSTRAC via a suspicious matter report (SMR).

Ransom payments

Overseas terrorist groups use ransom payments to raise funds due to the large sums that can be generated. These groups have taken foreign nationals hostage and demanded large amounts of money (from thousands to millions of dollars) from the victim's family, government or employer to secure their release.

Kidnap-for-ransom is most prevalent in areas that are experiencing an active insurgency and are not under effective government control. Australians living and working in these regions are at risk. The Department of Foreign Affairs and Trade (DFAT) regularly updates travel advice for Australians on the worldwide kidnapping threat and lists countries where the threat of kidnapping is particularly prevalent.[10]

Australia's longstanding policy is that it does not make payments or concessions to kidnappers as paying a ransom increases the risk of further kidnappings, including of other Australians.[11]

10 Department of Foreign Affairs and Trade, 'Kidnapping threat worldwide bulletin', 29 November 2013, http://www.smartraveller.gov.au/zw-cgi/view/TravelBulletins/Kidnapping

11 Ibid

transferring funds to finance terrorism

'...Terrorism financing through the banking sector is often small-scale and indistinguishable from the multitude of legitimate financial transactions undertaken each day....'

Most of the funds raised for terrorism in Australia are destined for overseas groups, with only a small portion raised for use in Australia.

For smaller amounts sent offshore, a transfer channel may be used based on its utility and reliability rather than with the expressed purpose of concealing transactions.

For larger amounts, or regular transfers over a period of time, more attention may be given to deliberately concealing transactions. This can be done by attempting to make transactions appear legitimate, or providing false or misleading details to reporting entities.

In Australia, key channels used to transfer funds for terrorism financing include:

» the banking sector

» the remittance sector

» legitimate businesses and 'front' businesses posing as legitimate businesses

» cross-border movement of cash and bearer negotiable instruments

» electronic payment systems, new and online payment methods.

Banking sector

Terrorist groups of all sizes and levels of sophistication may use the Australian banking sector at some point to transfer funds for terrorism financing. This reflects the central role of the banking system in Australia and gives terrorist groups and financiers the opportunity to blend in with normal financial activity to avoid attracting attention.

The Australia-based arms of more organised terrorist groups with global networks have transferred funds through Australian banks to accounts in foreign countries and used third parties to obscure and complicate money trails.

Terrorism financing through the banking sector is often small-scale and indistinguishable from the multitude of legitimate financial transactions undertaken each day. Some cases have involved structured deposits of cash into bank accounts followed by international funds transfers out of Australia. While individual transactions may be small, they can accumulate into significant amounts of funds over time. More complex methods have used Australian business accounts as fronts for sending funds offshore through the banking sector.

Transaction monitoring undertaken by the banking sector has been effective at detecting suspicious transaction patterns that could relate to terrorism financing. In particular, transaction monitoring undertaken by AUSTRAC and industry is likely to detect transactions involving deliberate attempts at concealment, high-risk countries and known terrorism suspects. Customer identifiers included in transaction reports submitted to AUSTRAC can prove critical in terrorism financing investigations.

Australian financial institutions should ensure their transaction monitoring programs are dynamic and updated regularly to reflect current terrorism financing threats. In particular, Australian reporting entities should take into account international conflicts and tensions of concern to the Commonwealth Government because of their potential to affect Australia's terrorism risk environment. Currently:

» funds sent to Syria and neighbouring countries warrant scrutiny for possible terrorism financing activity

» transactions involving other countries facing insurgency or terrorist threats, such as Yemen and Somalia, or neighbouring countries with established financial sectors, may also involve terrorism financing risks.

The remittance sector

The Australian remittance sector is an attractive vehicle for terrorism financing. Along with the banking sector, it carries a higher risk than most other channels of being exploited to transfer funds for terrorism financing. This is due largely to the sector's utility, including its low cost to transfer smaller amounts of funds and its ability to reach high-risk countries and regions where more formal financial channels are less accessible.

Australian authorities have identified that some domestic remittance businesses have been misused for terrorism financing. To date, the amounts involved have been small, reflecting the overall low incidence of terrorism financing in Australia more generally.

Compared to the banking sector, the remittance sector is involved in just a fraction of the total number of international funds transfers involving Australia each year. However, while the total value of funds transferred via the remittance sector is comparatively low, it is sufficient to assist in obscuring low-value transfers associated with terrorism financing.

Remittance channels are commonly used by migrant communities for legitimate purposes, particularly to send funds to family members overseas. The sector exhibits a number of characteristics that increase its risk of being misused for terrorism financing:

» The sector is commonly used to transfer funds to high-risk countries for legitimate purposes, including jurisdictions where formal banking networks may not be available. This can make it easier for transfers involving terrorism financing to these jurisdictions to go unnoticed.

» Remittance dealers who rely on ethnic or cultural links to send funds to high-risk terrorism financing jurisdictions are at greatest risk of being abused. However, these dealers are also well placed to identify and report suspicious behaviour. They often provide a service to customers from their own local community, and may know their customers' financial activities better than many other reporting entities, putting them in a good position to identify unusual and suspicious customer behaviour. These suspicions must be reported to AUSTRAC.[12]

12 See section in this report 'What should I do if I suspect terrorism financing' for further information on suspicious matter reporting obligations.

» It can be difficult to distinguish transfers relating to terrorism financing from legitimate transactions. Funds for terrorism financing are often sent in relatively small amounts, as these are perceived as less likely to attract suspicion, although attempts have also been made to conceal larger transactions and recurring transactions. The methods used to conceal these transfers are generally unsophisticated and involve a customer providing false or misleading identity details when undertaking the funds transfer. In a small number of cases the perpetrators have attempted to use more complex methods to conceal the true nature of the transfers.

Legitimate and 'front' businesses

Both legitimate and 'front' businesses are exploited by larger and better organised terrorist groups, particularly those with an international presence. Similar to the way charities and NPOs can be misused, these groups have set up business accounts in several jurisdictions and used them as a cover to send or receive funds through mainstream financial channels (such as the banking sector). Very large amounts of money can be transferred internationally, disguised as 'business' transactions.

Cross-border movement of cash and bearer negotiable instruments

Cross-border movement of cash and BNIs can be used to courier funds to terrorist groups overseas. Extremists travelling overseas to train or fight may also carry cash or BNIs to cover their own personal expenses.

Australians travelling overseas to train and fight with terrorist groups are more likely to move physical cash offshore (either as Australian or foreign currency), as funds can be carried when departing Australia. Third parties, such as family or local community members and associates of extremist groups, may also be used to move funds across borders to support those active on the ground in conflict regions.

The number of Australians currently travelling to fight alongside terrorist groups in Syria increases the risk of cash being carried out of Australia. Cash may be couriered directly into Syria or, more likely, to neighbouring countries where it can be carried overland across the border.

Electronic payment systems, new and online payment methods

Electronic, online and new payment methods pose an emerging terrorism financing risk which is likely to increase over the short term as overall use of these systems grows. Many of these systems can be accessed globally and used to transfer funds quickly. A number of online payment systems and digital currencies are also anonymous by design, making them attractive for terrorist financing, particularly when the payment system is based in a jurisdiction with a comparatively weaker AML/CTF regime.

Terrorist groups engaged in radicalisation, recruitment and communication online (such as through social media) are a particularly high risk of using online payment systems and digital currencies. These groups may solicit donations via social media or from an online support base, or use payment systems to transfer funds to affiliates or other groups offshore.

Prepaid travel money cards (a type of stored value card) have also been used to transfer funds offshore for terrorism financing.

what should I do if I suspect terrorism financing?

AUSTRAC reporting entities

Reporting entities under the AML/CTF Act must submit an SMR to AUSTRAC if, while dealing with a customer, they reasonably suspect a matter may be related to an offence, tax evasion or the proceeds of crime.

If a suspicion relates to the financing of terrorism, an SMR must be submitted **within 24 hours** of forming the suspicion. SMRs relating to other crimes must be submitted within three business days of forming the suspicion.[13]

Reporting entities should use the information in this report to assist them to identify suspicious matters. Even if the activity appears to be insignificant, it may provide a small part of a bigger picture. AUSTRAC analyses the SMRs it receives from industry and disseminates the results to relevant Commonwealth, state and territory partner agencies and international counterparts.

Individuals and non-reporting entities

Members of the community and businesses who are not reporting entities under the AML/CTF Act can report suspicious activity via the Government's National Security Hotline. Callers may remain anonymous if they wish.

Reporting entities who have submitted an SMR to AUSTRAC may also report suspicions via the National Security Hotline.

National Security Hotline

- Call: 1800 1234 00
- From outside Australia: (+61) 1300 1234 01
- Email: hotline@nationalsecurity.gov.au
- MMS: 0429 771 822
- TTY: 1800 234 889

For police, fire or ambulance response to a life threatening emergency or if a crime is in progress, call triple zero (000).

13 Further information on AML/CTF Act obligations is included in the section of this report on 'Australia's counter-terrorism financing framework'.