Trends & issues
in crime and criminal justice

No. 424 September 2011

Australian Government
Australian Institute of Criminology

Misuse of the non-profit sector for money laundering and terrorism financing

Samantha Bricknell

Foreword | *The manner in which terrorist organisations finance their activities became a policy focal point after the terrorist attacks of 11 September 2001. Non-profit organisations, and charities in particular, were identified as potentially significant contributors to terrorism financing. This premise was based on known links between charitable giving and prominent terrorist groups, and the vulnerabilities of the non-profit sector to misuse.*

Money laundering and terrorism financing (ML/TF) risks to the Australian non-profit sector are thought to be low. However, the impact of such misuse is inevitably high. One of the underlying premises in combating non-profit misuse has been the application of a response proportionate to risk. Australia has based its response on education, sector outreach and peak body codes of conduct, alongside more conventional forms of regulatory control.

This paper examines vulnerabilities to ML/TF misuse and the publicly available evidence for actual misuse. It is suggested that the Australian response could incorporate a more uniform commitment from the sector to adopting risk-based strategies, with government providing education for the sector that is based on the identification of specific points of vulnerability.

Adam Tomison
Director

Non-profit organisations (NPOs) are defined by their purpose, their reliance on contributions from supporters and the trust placed in them by the wider community. They often process large amounts of cash and regularly transmit funds between jurisdictions. NPOs have also traditionally operated under less formal regulatory control and generally, a less rigorous form of administrative and financial management. It is argued that the combination of these factors exposes the sector to an elevated risk of criminal and terrorist abuse (Charity Commission 2009a; FATF 2004a, 2004b).

The misuse of NPOs by terrorist entities, and in particular charities, has been a long-held practice (Winer 2008), exemplified by the fundraising activities of the Irish Republican Army (commonly referred to as the IRA) to help finance paramilitary activities and the known or suspected exploitation of charitable giving by groups such as Hamas, Hezbollah and the Liberation Tigers of Tamil Eelam (LTTE; Flanigan 2008; Ghandour cited in Ly 2007; Levitt 2006). However, it was not until the terrorist attacks of 11 September 2001 that NPOs were deemed as 'particularly suspicious in terms of concealing or providing terrorist financing' (McCulloch & Pickering 2005: 472) and became a focus of counter-terrorism financing responses.

Chief among these responses was the inclusion of NPOs in the Financial Action Task Force (FATF) series of special recommendations to combat terrorism financing, to be observed by governments alongside the revised Forty Recommendations on the prevention of money laundering. Special Recommendation VIII (SR VIII) advises countries to review their laws and regulations regarding NPOs to protect the sector from misuse:

- by terrorist organisations posing as legitimate entities;
- through the exploitation of legitimate entities as conduits for terrorism financing; and
- by concealing or masking the clandestine diversion of funds intended for legitimate purposes to terrorist organisations (FATF 2004a).

FATF recommends there be increased transparency within the non-profit sector and the implementation of a regulatory scheme that includes sector outreach, sector monitoring, effective intelligence and information gathering, and the establishment or strengthening of cooperative relationships between relevant regulatory and law enforcement agencies. In addition, states were advised to encourage the non-profit sector to:

- adopt methods of best practice with respect to financial accounting, verification of program specifics, and development and documentation of administrative, and other forms of control;
- use formal financial systems to transfer funds; and
- perform due diligence and auditing functions of partners and field and overseas operations respectively.

A 2005 mutual evaluation of Australia's anti-money laundering/counter-terrorism financing regime by FATF cautioned against the potential inefficiency of the current regulatory system and the lack of additional measures Australia had introduced to further safeguard the non-profit sector from misuse. Following the 2005 mutual evaluation, Australia implemented the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) and while only some services provided by NPOs fall within the Act's definition of a designated service, other services that NPOs use (eg financial services) are obliged to undertake AML/CTF risk assessments, perform due diligence and report specified transactions to AUSTRAC. The government has also introduced guidelines and other educative initiatives to assist NPOs to undertake risk assessments and minimise exposure to money laundering/terrorism financing (ML/TF)-related exploitation.

In this paper, an examination is provided of the risks to the non-profit sector more broadly and those that apply specifically to Australian NPOs. Regulatory responses are explored in greater detail in Bricknell et al. 2011.

Methods of misuse

There are multiple ways in which non-profit entities may be misused (Charity Commission 2009a; FATF 2008, 2004b).

Misuse of funding

The misuse of NPO-generated funds may take any one of the following forms. First, funds may be collected in the name of a legitimate NPO but disbursed for terrorist rather than altruistic means. Second, an NPO may be used to launder money or provide legitimate means for the transmission of funds between multiple locations. Finally, funds may be misused by the recipients themselves. In any of these scenarios, the NPO may or may not be complicit in or aware of the abuse being committed.

Misuse of assets

Assets such as vehicles and property could be used to transport or house operatives, money and weapons, and provide relatively safe places where members can meet.

Misuse of name and status

An NPO may provide financial support to an organisation that provides humanitarian aid, for example, but that organisation may also provide succour to terrorist activities. Alternatively, an NPO may raise funds for a particular cause but have those funds dispensed or support provided through a terrorist group.

Misuse of the notion of charitable status

Criminal or terrorist entities may elect to establish a sham NPO (in this case, a charity) but one which is registered and engages in requisite regulatory requirements. The purpose of the NPO is ostensibly to collect and distribute charitable giving but it is in reality a front for the laundering of money, appropriation of terrorism funds or for the rallying support for terrorist activities.

Gurulé (2008) has suggested a general modus operandi for non-profit exploitation, based on sham NPOs in the United States. Such sham agencies were found to:

- incorporate under state law;
- apply for tax-exempt status as a charity or other type of NPO;
- undertake fundraising activities;
- open domestic bank accounts into which proceeds and donations are deposited; and
- transfer funds to overseas financial institutions, diverting all or some of the funds to terrorist activity.

Evidence for misuse

From the publicly available evidence, there is little to suggest that there is substantial misuse of NPOs for ML/TF. Case studies have demonstrated that opportunities exist and are exploited for ML/TF purposes but the number of published case studies is still relatively small (APG 2009, 2008, 2005; AUSTRAC 2008; Charity Commission 2010, 2009b; FATF 2008, 2004b, 2003; FINTRAC 2009; OECD 2008). This could suggest that the prevalence of ML/TF misuse (in the listed countries) is itself low. Conversely, it could indicate there are low detection rates for this kind of illegal activity; that is, prevalence is higher than the publicly available material implies. Without access to material on unpublished matters, it is difficult to confirm which is the more accurate of these two scenarios.

The majority of cases *detected* (and made publicly available) involved either the establishment of a sham NPO (in every case, a charity) or the exploitation of a legitimate entity to raise, transfer, distribute or launder funds. With the exception of a few cases of money laundering, most published cases described incidents of charity misuse to raise and divert funds to support terrorism. Again, it can only be speculated whether this reflects political focus on terrorism financing, actual prevalence or better rates of detecting terrorist financing connections with charity misuse. Many of the implicated charities formed part of a complex financing network where funds were transferred between a series of local and international accounts held by the charity, other NPOs, businesses (legitimate and fictitious) and individuals (APG 2009, 2008, 2005; AUSTRAC 2008;

Table 1 Selected cases of non-profit organisation misuse

Terrorism financing
Case study 1 (Canada)
A charity was suspected of raising and disbursing financial resources for a terrorist organisation based in another country. Over a period of five years, the charity organised a 'substantial' number of electronic funds transfers to overseas-based persons and entities, including a charity that was thought to be operating as a front for a terrorist group. During the same five year period, large sums of cash were deposited into, and multiple credits made to, the charity's accounts. The source of the funds was unknown as was the identity of the remitter for the credits. Cash deposits into the charity's accounts were immediately followed by the purchase of bank drafts or the transfer of funds overseas.
Case study 2 (Russia)
A 'small' company was receiving a 'significant' number of cash deposits from numerous charities (purportedly for consultancy services rendered) and two individuals, both of whom were resident in regions where militant activity was prevalent. The account of one of these two persons showed regular deposits of funds of amounts below the reporting threshold; the source of these funds was unknown. The funds collected in the company accounts were being transferred to a charity operating in a region of unrest, before being disbursed to other, apparently legitimate charities and a so-called 'welfare unit' that was known to be part of a recognised militant group. The welfare unit was subsequently shut down.
Money laundering
Case study 1 (England)
A family, who operated several successful businesses being used for criminal purposes, founded a charity with the alleged objective of providing for members of a specified religious community. The charity was registered with the national regulator and provided annual statement accounts showing that relatively small amounts of money were being generated. The scheme was managed by the family operating multiple cash tills but only declaring the income from one. Intelligence revealed that the family were laundering the proceeds of their tax evasion to fund their lifestyle; more than £2.5m was found in the bank accounts of the charity and family members acting as charity trustees.
Case study 2 (Australia)
A church fund was used to launder assets as part of a scheme to defraud a private company. The funds originated from a company in which one of the alleged offenders was responsible for the management of the company's financial arrangements. The funds were transferred into a bookmakers account before being distributed into a series of private and third-party accounts, one of which was established overseas. Cash sent to the overseas account was wired back into a local trust account held by the second alleged offender. Around $350,000 was drawn from the trust account and deposited into the church fund. At the time of detection, arrangements were being made to send the cash to overseas-based accounts.

Source: AUSTRAC 2008; FATF 2008; FINTRAC 2009; OECD 2008

FATF 2008, 2004b, 2003; FINTRAC 2009; OECD 2008). The charity often served as the origin for funds collection and dispersal, which were transferred using a combination of cash deposits, wire transfers and remittance schemes. Table 1 describes selected typologies of misuse.

Many of the higher profile incidents of charity exploitation come from the United States. Charities such as the Benevolence International Foundation, Global Relief Foundation and Holy Land Foundation for Relief and Development were implicated in providing financial and other assistance to Islamic terrorist organisations (predominantly Al Qaeda or Hamas) in the guise of charitable relief (Roth, Greenberg & Wille 2004). Between November 2001 and March 2008, there were 26 cases in the United States, which involved charges against charities or individuals associated with charities in relation to one or more of four terrorism statutes relating to the provision of financial or material support to terrorist organisations (CLS 2008).

The United Kingdom has also experienced incidents of predominantly terrorist financing-related charity misuse but its model of dealing with this misuse has produced different outcomes. The Charity Commission in England and Wales (the national charity regulator) plays a prominent role in the discovery and sanctioning of non-compliant charities. Between 30 June 2008 and 30 June 2010, the Charity Commission completed 18 inquiries into charities suspected of forming links with terrorist organisations (Charity Commission 2010, 2009b). In most cases, there was no evidence for such a link but trustees for whom there were concerns were removed in some instances and the implicated charity was instructed to improve governance and financial reporting arrangements (Charity Commission 2010, 2009b). Significant action, such as freezing a charity's assets or de-registering/shutting down the charity has been comparatively uncommon (eg Tamil Rehabilitation Organisation).

Australian cases

'Financial contributions through formal charitable donations' was listed by AUSTRAC (2010: 8) as one of three principal methods by which terrorism funds are raised in Australia. Nonetheless, there are few publicly available, documented examples of this kind of exploitation, or of NPOs being used in money laundering schemes.

Aruran Vinayagamoorthy, Sivarajah Yathavan and Armugan Rajeevan

In December 2009, Aruran Vinayagamoorthy, Sivarajah Yathavan and Armugan Rajeevan pleaded guilty to offences under the *Charter of the United Nations Act 1945* (Cth) for making assets available (directly or indirectly) to the LTTE, an entity proscribed for the purposes of that Act. It was alleged that the defendants had played a role in the collection and transfer of $1,030,259 in donations to the LTTE between 13 December 2002 and 12 October 2004. Mr Vinayagamoorthy had also been indicted for making an estimated $97,000 worth of electronic components available to the LTTE over a period of two years. Justice Coghlan noted at sentencing that it was more than probable the defendants knew the LTTE was a proscribed entity in other countries and the 'complex structuring... used to transmit funds suggested as much' (Transcript of proceedings, *R v Vinayagamoorthy & Ors*, Supreme Court of Victoria, Coghlan J, 31 Mar 2010: 13). Nonetheless, the court accepted that the funds were collected to provide humanitarian assistance and 'not purposely to assist terrorist activity' (Transcript of proceedings, *R v Vinayagamoorthy & Ors*, Supreme Court of Victoria, Coghlan J, 31 Mar 2010: 31).

Yathavan and Rajeevan were sentenced to a term of imprisonment of one year, but released on three year good behaviour bonds. Vinayagamoorthy was sentenced

to a term of three years, but released on a four year good behaviour bond (*R v Vinayagamoorthy & Ors* [2010] VSC 148, 31 March 2010)

Nachum Goldberg and others

Between 1990 and 1997, Nachum Goldberg and members of his family operated a money laundering scheme in which an estimated $48m was transferred from Australia to Israel. Goldberg opened an account in the name of United Charity, a fictitious entity that had no legal basis and had not been registered as a charity or company. The account was used to launder cash proceeds from Australian business activity that had not been disclosed to the Australian Taxation Office (CDPP 2001). Cash deposits made by Goldberg or other family members were transferred to one of four banks in Israel. Other businessmen were brought in later during the life of the scheme, who wrote bogus cheques for Jewish charities, which were then purchased for cash.

The scheme was uncovered following a change of manager at the branch where the account had been opened and the withdrawal of the account's status as an internal bank management account. The change of status brought the account under AUSTRAC scrutiny and the subsequent detection of the suspiciously large number of transactions being made. At appeal, one of the presiding judges noted that the use of such an account suggested that Goldberg had extensive knowledge of bank procedures and AUSTRAC processes, as well as possible cooperation from the bank (*DPP (C'th) v Goldberg* [2001] VCSA 107; 2001 184 ALR 387).

Goldberg was eventually sentenced, following an appeal from the Commonwealth Director of Public Prosecutions, to a custodial sentence of seven years (DPP (C'th) v Goldberg [2001] VCSA 107; 2001 184 ALR 387). He was also sentenced, along with his wife and two sons, to make reparations to the Commonwealth of $15m.

Risks to the Australian non-profit sector

The Australian non-profit sector comprises an estimated 600,000 organisations (Productivity Commission 2010), including associations, charities, churches, clubs, foundations, societies and unions. Among this diverse group of entities is a mixture of different legal forms, different regulatory responsibilities and varying capacities to undertake prescribed administrative and financial management practices.

While all NPOs are potentially at risk of ML/TF misuse, those that are considered to be especially vulnerable are entities that:

- are charities;
- are closely aligned to particular cultural or religious movements;
- frequently move funds or other resources to areas of conflict;
- rely on overseas-based organisations to deliver funds;
- deal in cash or alternative remittance systems (ARS); and/or
- have extremely complicated financial resources from which suspicious transactions are more difficult to identify (Home Office & HM Treasury 2007).

The Australian non-profit sector is no less immune to this suite of vulnerabilities. Representatives from law enforcement, academia and the non-profit sector who participated in roundtables held at the Australian Institute of Criminology (AIC) also identified that these characteristics increased Australian NPO exposure to misuse. The part of the sector considered at greatest risk however, were the charities, particularly small, informal unincorporated entities, and organisations which relied on informal methods of funds transfer such as ARS.

Many small NPOs fall outside regulatory scrutiny and are less likely to be familiar with AML/CTF issues. Further, their composition usually means they do not have the resources to implement risk mitigation strategies (as described below), or do not see the merit in doing so. Roundtable participants conceded that less could be practically achieved to minimise misuse among this group of NPOs and believed a deficiency in sector outreach and education was partially responsible for the purported lack of awareness.

A reliance on informal methods of funds collection and disbursal, in particular by the less formal charities tied to specific faith or community groups, further exposes smaller NPOs to misuse. ARS providers are prescribed as a 'designated service' under the AML/CTF Act. Providers are obliged to register with AUSTRAC and implement customer identification procedures, put in place AML/CTF programs, report to AUSTRAC annually regarding their compliance with the AML/CTF Act and undertake ongoing customer due diligence but not all do, or are aware that they should. An AIC study of ML/TF risks to ARS in Australia (Rees 2010) found variable knowledge among smaller providers about their obligations under the Act and some providers admitted to difficulties in adhering to AML/CTF regimes, primarily related to the time-consuming and complex nature of reporting requirements (Rees 2010). Since large ARS providers were seen by users as being very expensive (Rees 2010), smaller NPOs may prefer to use the services of smaller or unaffiliated providers to reduce costs. Sham or corrupted NPOs are likely to do the same. AUSTRAC (2010) has acknowledged that smaller or unaffiliated providers are difficult to formally monitor and the risk of misuse is potentially greatest for such providers.

Larger, incorporated entities are not invulnerable to exploitation. Many of the overseas cases of non-profit misuse (primarily in the United States) involved NPOs that were incorporated, had gained tax-exempt status and raised substantial amounts of cash. NPO roundtable participants stated that the larger NPOs adhered very closely to guidelines and codes of conduct that should minimise opportunities for exploitation. Nevertheless, for NPOs that worked internationally, it was not always possible to confirm the credentials, or manage the operating standards of overseas partners, particularly in situations of disaster relief and other quick-response events.

The adoption of mitigation strategies

Contributing to the non-profit's sector vulnerability to ML/TF misuse is the adoption (or lack thereof) of risk management strategies. Recent UK studies on risk and financial management practices in the non-profit sector found a generally poor uptake of key risk management strategies (eg fraud policies, application of internal controls, whistleblowing policies) and a relatively lax application of financial management protocols (Charity Commission 2010; PKF & the Charity Finance Directors' Group 2009). These protocols, along with strong governance arrangements, are cited as essential for minimising exposure to criminal and terrorist abuse (Charity Commission 2010).

Similar findings were reported for Australian NPOs. Forty-one percent of 291 NPOs surveyed about their organisational risk management practices did not have a documented risk management policy, or were not aware that one existed (PPB 2010). In another sector survey, just 29 percent of the 272 respondent organisations had implemented a fraud control policy, 13 percent a fraud control plan, 26 percent regular fraud risk assessment and 13 percent a whistleblower policy; the majority (88%) did use controls reviews (BDO Chartered Accountants and Advisors 2010).

The Australian Government has produced guidelines—*Safeguarding Your Organisations against Terrorism: A Guidance for Non-profit Organisations*—to educate the sector on ML/TF risks and outline best practice principles to reduce this risk. Peak bodies, such as the Australian Council for International Development and Fundraising Institute of Australia, additionally provide conventions in the form of codes of conduct around good governance, organisational integrity and financial management and reporting.

Balancing risk with response

Abuse of the non-profit sector is evidently occurring. Most documented incidents of misuse for ML/TF involved the establishment of a sham organisation, invariably a charity. The exploitation of legitimate charities was much less common. In many cases, the charity was registered or otherwise known to a regulatory or tax authority and was built into a complex network of funds transfer that used, at some point, registered financial channels.

These reported cases of non-profit misuse sit somewhat counter to the characteristics specified for Australian NPOs considered at greatest risk of misuse, specifically the heightened vulnerability of un-incorporated entities and those that use informal methods of funds transmission. This inconsistency might denote a deliberate choice to form or infiltrate a registered entity in order to instil a veil of legitimacy to the organisation's purpose and operation. It may also show that detection is only practicable with formal or routine monitoring and hence smaller entities sitting outside regulatory scrutiny are being exploited more than the case studies imply.

The potential risk to the Australian non-profit sector is credible but the actuality of exposure appears relatively low. This was the view of non-profit, law enforcement and academic participants at the AIC-held roundtables and what can be deduced from the publicly available evidence. There have been a small number of cases in which an Australian NPO was suspected of procuring funds for terrorist activities and just one case that proceeded to trial. The evidence for non-profit involvement in money laundering is equally slender.

Risk, however, often determines response. It has been argued, mostly by the non-profit sector, that the proposed risk to the sector *as a whole* has been inflated. In the United Kingdom, a difference in opinion has emerged between the regulator and the regulated about the proportionality of the measures introduced to minimise misuse. Just as important to the sector is its concern that the intensified focus on NPOs stigmatises the sector and has the potential to disrupt activity (Crimm 2008).

The current Australian regulatory regime for the non-profit sector does not have an overt emphasis on ML/TF issues, although the encapsulation of designated services used by NPOS under the AML/CTF Act does afford good protection. Nonetheless, the publicly available evidence suggests there is not an elevated risk of ML/TF exploitation of Australian-based NPOs. Australia has taken the approach of providing government-sponsored guidelines, performing sector outreach and relying upon peak body codes of conduct to educate the sector and to encourage the adoption of risk and financial management tools. It is not clear what proportion of the sector has implemented these strategies, although the aforementioned sector surveys indicate more could be done.

The regulation of the Australian non-profit sector has been criticised for its overly complex nature (eg see Productivity Commission 2010). The Australian Government announced in the 2011–12 Federal Budget the establishment of an Australian Charities and Not-for-Profits Commission, with the possible future installation of a national regulator (Australian Government 2011). The Australian non-profit sector does not appear to be averse to strengthened regulation; NPO roundtable participants agreed with law enforcement and academic co-participants that the current regulatory system was not as effective as it could be in identifying non-compliant and criminal behaviour, and that modification to the system was warranted. Nonetheless, there was a concern that a broad-brush approach may be taken to stem a risk scenario that may only apply to a small component of the sector, yet will still exclude entities currently outside regulatory scrutiny. To guard against such an outcome, the non-profit sector should consider developing and engaging fully with appropriate risk-based management strategies. Further, government agencies could profitably aim to better educate the sector through the provision of information and advice based on specific intelligence rather than generic points of vulnerability.

Acknowledgements

The author would like to acknowledge the additional research undertaken by Rob McCusker, Hannah Chadwick and Dave

Dr Samantha Bricknell is a Senior Research Analyst at the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series: Dr Adam M Tomison, Director, Australian Institute of Criminology

Note: *Trends & issues in crime and criminal justice* papers are peer reviewed

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

ISSN 0817-8542 (Print)
1836-2206 (Online)

GPO Box 2944
Canberra ACT 2601, Australia
Tel: 02 6260 9200
Fax: 02 6260 9299

Project no. 0140

Rees for this paper. This paper is a condensed version of the AICs longer report published as Bricknell et al. (2011).

References

All URLs correct at June 2011

Asia/Pacific Group on Money Laundering (APG) 2009. *APG yearly typologies report 2009*. http://www.apgml.org/documents/docs/6/APG Typologies%20Report%202009.pdf

Asia/Pacific Group on Money Laundering (APG) 2008. *APG yearly typologies report 2008*. http://www.apgml.org/documents/docs/6/APG_2008_Typologies_Rpt_July08.pdf

Asia/Pacific Group on Money Laundering (APG) 2005. *APG yearly typologies report 2004–05*. http://www.apgml.org/documents/docs/6/Yearl%20Typologies%20Report%202004-05_PUBLIC.pdf

Australian Government 2011. *2011–12 Australian government budget: Budget paper no 2*. http://cache.treasury.gov.au/budget/2011-12/content/download/bp2.pdf

Australian Transaction Report and Analysis Centre (AUSTRAC) 2010. *AUSTRAC typologies and case studies report 2010*. http://www.austrac.gov.au/files/typ_rpt.pdf

Australian Transaction Reports and Analysis Centre (AUSTRAC) 2008. *AUSTRAC typologies and case studies report 2008*. http://www.austrac.gov.au/files/austrac_typologies_2008.pdf

BDO Chartered Accountants and Advisers 2010. *BDO not-for-profit fraud survey 2010*. http://www.bdo.com.au/__data/assets/pdf_file/0020/113546/2010-Not-for-Profit-Fraud-Survey.pdf

Bricknell S, McCusker, Chadwick H & Rees D 2011. *Money laundering and terrorism risks to Australian non-profit organisations*. Research and public policy series. Canberra: Australian Institute of Criminology

Charity Commission 2010. *Charities back on track: Themes and lessons from the Charity Commission's compliance work 2009–10*. http://www.charitycommission.gov.uk/Library/track10.pdf

Charity Commission 2009a. *Compliance toolkit: Protecting charities from harm. Module 3: How might a charity be abused for terrorist purposes?* http://www.charity-commission.gov.uk/Library/tkch1mod3.pdf

Charity Commission 2009b. *Charities back on track: Themes and lessons from the Charity Commission's compliance work 2008–09*. http://www.charitycommission.gov.uk/Library/track09.pdf

Commonwealth Director of Public Prosecutions (CDPP) 2001. *Annual report 2000–01*. Canberra: CDPP

Crimm NJ 2008.The moral hazards of anti-terrorism financing measures: A potential to compromise civil societies and national interests. *Wake Forest Law Review* 43: 578–626

Financial Action Task Force (FATF) 2008. *Terrorist financing*. Paris: OECD/FATF

Financial Action Task Force (FATF) 2004a. *FATF special recommendation VIII: Non-profit organisations. Text of the special recommendation and interpretative note*. Paris: OECD/FATF

Financial Action Task Force (FATF) 2004b. *Report on money laundering typologies: 2003–2004*. Paris: OECD/FATF

Financial Action Task Force (FATF) 2003. *Report on money laundering typologies 2002–03*. Paris: FATF

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) 2009. *Money laundering and terrorist financing typologies and trends in Canadian banking: May 2009*. Ottawa: FINTRAC

Flanigan ST 2008. Nonprofit service provision by insurgent organizations: The cases of Hizballah and the Tamil Tigers. *Studies in Conflict and Terrorism* 31(6): 499–519

Gurulé J 2008. *Unfunding terror: The legal response to the financing of global terrorism*. Cheltenham, UK & Northamption, MA: Edward Elgar

Home Office & HM Treasury 2007. *Review of safeguards to protect the charitable sector (England and Wales) from terrorist abuse: A consultation document*. London: Home Office

Levitt M 2006. *Hamas: Politics, charity and terrorism in the service of Jihad*. New Haven: Yale University Press

Ly P-E 2007. The charitable activities of terrorist organizations. *Public Choice* 131: 177–195

McCulloch J & Pickering S 2005. Suppressing the financing of terrorism: Proliferating state crime, eroding censure and extending neo-colonialism. *British Journal of Criminology* 45(4): 470–486

Organisation for Economic Co-operation and Development (OECD) 2008. *Report on abuse of charities for money laundering and tax evasion*. Paris: OECD

PKF & the Charity Finance Directors' Group 2009. *Managing risk: Keeping in control. Charities risk survey 2009*. http://www.lambeth.gov.uk/NR/rdonlyres/190ED806-FC40-4CE0-94CF-1439C20530B7/0/managingrisk.pdf

PPB 2010. *Not-for-profit risk survey 2010*. http://www.appichar.com.au/data/files/ppb_notforprofit_risk_survey_2010.pdf

Productivity Commission 2010. *Contribution of the not-for-profit sector. Productivity Commission research report*. Canberra: Productivity Commission

Rees D 2010. *Money laundering and terrorism financing risks posed by alternative remittance in Australia*. Research and public policy series no. 106. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/100-120/rpp106.aspx

Roth J, Greenberg D & Wille S 2004. *Monograph on terrorist financing: Staff report to the Commission. National Commission on Terrorist Attacks upon the United States*. Washington, DC: Government Printing Office

The Center on Law and Security (CLS) 2008. *Terrorist trial report card: Terror financing through charities*. http://www.lawandsecurity.org/publications/TTRCApril08CharitiesFinal1.pdf

Winer J 2008. Countering terrorist finance: A work, mostly in progress. *The Annals of the American Academy of Political Science* 618(1): 112–132