

Assessment of Money Laundering and Financing of Terrorism Risks in a Nonprofit Organization

Swati Sarkar^{1*}

¹Ph.D. Fellow, International Islamic University Malaysia (IIUM), Malaysia

DOI: [10.36347/sjebm.2021.v08i08.006](https://doi.org/10.36347/sjebm.2021.v08i08.006)

| Received: 11.07.2021 | Accepted: 14.08.2021 | Published: 17.08.2021

*Corresponding author: Swati Sarkar

Abstract

Review Article

Nonprofit organizations (NPOs) handle enormous sums of cash and routinely transfer monies across countries. NPOs have historically functioned under fewer formal regulatory controls and a less rigorous administrative and financial management style. Criminal and terrorist misuse is said to be more likely in the industry. The abuse of nonprofits by terrorist entities has a long history, business, and financial indicators. They are often utilizing in industries where prevention is critical. Indicators can improve forewarning, allowing for the mitigation of dangers before they materialize or detecting existing misuse. Numerous elements were founded in the case studies that showed that an NPO was being abused or was at high risk of being abused. These elements have been compiled in this chapter to assist all stakeholders, including nonprofits, government actors, financial institutions, and designated non-financial businesses or professions (DNFBPs), in identifying and investigating potential cases of abuse within a specific NPO the more significant NPO sector. While the list of indicators provided here is extensive and global in scope, it is not exhaustive; there are likely to be additional indications peculiar to certain settings found within specific national jurisdictions, as per FATF Recommendation 1 (national risk assessment).

Keywords: Money laundering, Financing, Terrorism, Risks NPO.

Copyright © 2021 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

INTRODUCTION

Non-profit organizations (NPOs) are defined according to their goals, their reliance on support donations and the larger community's confidence in them. They manage enormous amounts of cash and even shift funds between countries. Moreover, NPOs usually functioned within less formal regulatory limitations and in an administrative and financially less stringent way. As a result, criminal and terrorist misuse is more likely in the company (Charity Commission 2009a; FATF 2004a, 2004b) [1]. To assist paramilitary finance and familiar or suspected charitable exploitation by organizations like Hamas, Hezbollah and Tamil Eelam Liberation Tigers (LTTE; Flanigan 2008; Ghandour cited in Ly 2007; Levitt 2006) [2]. Terrorist organizations, in particular charities (Winer 2008), have a long history of misuse of NPOs, as shown by fundraising activities (IRA). Only on 11 September 2001 were NGOs regarded "particularly suspect of concealing or providing terrorist money" as targets for counter-terrorist financing operations (McCulloch & Pickering 2005: 472) [3]. In order to finance terrorism, nations should implement several specific recommendations published by the Financial Action

Task Force and updated 40 guidelines on prevention of money laundering. It suggested that nations change their NPO policies and regulations to safeguard the sector from exploitation. Terrorist groups, who are actual entities, utilize lawful organizations to promote terrorism and cover up covert transfer of money to terrorist organizations, on legal grounds (FATF 2004a). FATF promotes more openness in the non-profit sector and fosters constructive cooperation with regulatory and law enforcement agencies. States should also support these organizations promote a thriving non-profit sector in order to collaborate with non-profit organizations.

- To put in place processes concerning financial accounting, program specifics, and administrative and other kinds of control while also improving financial accounting standards and practices;
- use formal economic systems to transfer funds; and
- Carry out comprehensive inspections and research on your partners, customers and suppliers and your foreign operations.

In November 2005, FATF (an international intergovernmental body responsible for establishing

anti-money laundering/counter-terrorism financing standards) [4]. Conducted a mutual evaluation of Australia's anti-money laundering/counter-terrorism financing regime and warned that the current regulatory system could be inefficient. The country had not taken additional measures to protect the nonprofit sector from misuse. The Australia-United States Mutual Evaluation conducted in 2005 concluded that Australia's AML/CTF Act of 2006 should implement. Not all of the services provided by NPOs should classify as a designated service. However, NPOs must undertake AML/CTF risk assessments, perform due diligence, and report specified transactions to AUSTRAC. Along with creating guidelines and other educational programs to help NPOs do risk assessments and minimize vulnerability to money laundering/terrorism funding (ML/TF)-related exploitation, the Government has also instituted risk assessment and mitigation measures. In this article, risk issues for nonprofit organizations are explored, and those about NPOs in Australia are also presented. In Bricknell *et al.* [5]. The concepts of regulatory responses are studied in-depth.

Methods of misuse

Nonprofit entities may be exploited in a variety of ways (Charity Commission 2009a; FATF 2008, 2004b).

Misuse of funding

NPO money may be misused in any one of several ways. At first, funding may be raised under the banner of a legal NPO; however, money may be dispensed for terrorist causes instead of charity. Also, NPOs can be used to move money between various places or clean money that may have been earned illegally. Funds may be utilized for other purposes by the beneficiaries. The NPO might be either involved in or unaware of the abuse that occurs in any of these circumstances.

Using company assets improperly

Agents can convey themselves, money, and weapons; they can also employ assets like automobiles and buildings to provide a relatively safe meeting location.

Identity and status abuse

A nonprofit organization could help a group that offers humanitarian relief, yet the latter might also favor terrorist organizations. NPOs may either utilize cash raised for a particular purpose or donate those funds to a terrorist group for use.

Charitable usage is frequently abused.

Criminal or terrorist entities may establish fictitious nonprofit organizations (including a charity) but one which fulfills the required regulatory standards. In the view of critics, NPOs have historically not served philanthropic goals but instead have served as money laundering fronts, funding terrorist acts, or mobilizing sympathy for terrorism.

Gurulé (2008) proposes a fundamental *modus operandi* for non-profit use [6], which identified comparable phony NPOs in the United States. Establish fake agencies that have subsequently been discovered 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 monies to financial institutions abroad and transfer all or part of the funds to terrorism.

A clear case of abuse

There appears to be minimal evidence of abuse of NPOs for ML/TF. Despite their availability, ML/TF opportunities have yet to be widely realized and used. Research studies show that opportunities for ML/TF implementation do exist, but the available research is limited (APG, 2008, 2005; AUSTRAC, 2008; Charity Commission, 2010, 2009b; FATF, 2008, 2004b, 2003; FINTRAC, 2009; OECD, 2008) [7]. While misuse of ML/TF may be widespread in the nations listed, this may point to the fact that overuse is rather rare. That is, there are more instances of unlawful behavior that can be detected using publicly accessible information. Without access to unpublished information, it is impossible to determine which of these two possibilities is more correct. A fake NPO (charity) is established, and then used to launder money in nearly all cases. Only a few examples of money laundering in the world of charitable donations have made it into the public eye. Still, most of the time, charitable donations are being used to generate and transfer cash to support terrorists [8]. But it can only be assumed if this represents a concentration on tracking terrorist financing, whether or not there is genuine prevalence or improved monitoring of how charities are misused. Charity funders found themselves ensnared in a complicated web of charities, donors, legitimate and illegitimate enterprises, and people in which money flowed between various accounts.

Table-1: Examples of nonprofit abuse.

Terrorism financing
Case study 1 (Canada)
In the aftermath of the accusations of a charity funding terrorist group in another nation, authorities began investigating whether or not a charity was funding and dispersing money to these terrorist groups. A charity located overseas coordinated the movement of "significant" numbers of electronic financial transfers over a five-year period, including to a charity that had been identified as being involved in covert support of a terrorist organization. A substantial quantity of money was placed into the charity's accounts during the same five-year period, while several credits were made. It is uncertain where the monies originated and who remitted the credits. Immediately following the deposit of cash, the charity bought drafts on bank accounts or moved funds to abroad locations (FINTRAC 2009 Annual Report).
Case study 2 (Russia)
This tiny firm, which reportedly offered consulting services to many charities, was collecting numerous monetary deposits from the charities, which two residents allegedly made of locations where terrorism was common. The source of these monies was unclear, and this is one of the instances where this money was deposited below the reporting level. After a short period of time, the money in the company accounts was transferred to a charity that was situated in a part of the world experiencing unrest. The money was then given to other, apparently legal charities and a so-called "Welfare Unit" affiliated with a violent group whom many state bodies had already labeled as terrorists. The welfare unit was therefore closed (Annual Report on Sustainable Development Work in The OECD - OECD 2008).
Money laundering
Case study 1 (England)
An economically successful family started a charity with the ostensible aim of supporting a religious group in order to provide them with employment. The charity also supplied annual financial statements that showed that a tiny amount of money was being earned to satisfy regulatory requirements. Only disclosing the income from one cash till to the taxman, the family operated the entire business using numerous cash tills. Due to a large number of funds being found in the charity's bank accounts and family members posing as charity trustees, it was revealed that the family was laundering the proceeds of their tax evasion to support their lifestyle (FATF-Financial Action Task Force Annual Report 2008-2009).
Case study 2 (Australia)
Some of the money was stolen from a church and laundered through a scam to defraud a private corporation. This case is built on a firm's finances in which one of the individuals under investigation was directly responsible for managing the financial arrangements. Before the money was disbursed, the cash was deposited into a bookies account, which was moved into a succession of private and third-party accounts, including one located outside of the country. By the second accused, the cash deposited into an offshore account was immediately transferred back into a local trust account belonging to the first accused. The trust account took in around \$350,000, and the funds were placed into the church fund. The funds were sent to overseas-based accounts in the event of discovery (AUSTRAC-Typologies and case studies report 2008).

One of the main ways that charities distribute donations is through wire transfers, cash payments, and remittance programs. Table 1 presents several misuse typologies. US-based cases of charity fraud are prevalent. Several charity groups (including Benevolence International Foundation, Global Relief Foundation, and Holy Land Foundation for Relief and Development) were allegedly helping Al Qaeda and Hamas disguise their terrorist activity as charitable work (Roth, Greenberg & Wille 2004). There were at least 26 US terrorism-related lawsuits filed from November 2001 to March 2008, in which people or charities were accused of supporting terrorist groups (CLS 2008) [9]. Unlike the UK, the countries that have suffered cases of terrorist financing-related charity misuse have not found a clear and consistent approach to dealing with the issue. The Charity Commission (England and Wales), a key factor in identifying and punishing non-compliant organizations, also plays a prominent part in the whole process. It took the Charity Commission, which is responsible for investigating

nonprofits suspected of connections to terrorist organizations, a total of 18 months to investigate all of them (Charity Commission 2010, 2009b) [10]. As often happened, there was no concrete proof to link these occurrences, but trustees that raised concerns were dismissed in certain cases, and the organization was urged to strengthen its internal controls and reporting procedures (Charity Commission 2010, 2009b) [11].

NPO-SECTOR and the risk of terrorist abuse worldwide environment

Environmental uncertainty is on the rise both for legal and illegitimate international players because of globalization, but it also present significant possibilities and threats.

Nonprofit organizations have benefited from technology improvements in fundraising and advertising, allowing them to coordinate their work effectively. Transportation and financial networks have become increasingly interconnected, resulting in money

transfers or products moving worldwide, to offices, partnerships, or directly to recipients. On the other hand, as a result of globalization, new pressures have emerged on NPOs, particularly those that conduct humanitarian missions, which forces them into politically and socially unstable places.

Since NPOs are genuine international players, they may take advantage of the benefits of globalization to their benefit, including:

- Increased mobility;
- The interconnectedness of networks;
- Expanded and deepened access to areas of conflict or low governance;
- Diversified financial services and logistical networks;
- Decentralized communications and management;
- Increased ability to engage the public.

However, terrorists also attempt to make these same gains, but they do so covertly. Moreover, Al Qaeda's continued durability stems in great part from its capacity to decentralize communications and administration, diversify its logistical, financial, and recruitment networks, and to disperse its cadres and leaders throughout the globe.



Fig-1: Threat and Vulnerability

For instance, see Swiss Info (2014), FATF (2013a), p.7.

Case studies in this study provide evidence of misuse, which is above and above the norm, in the NPO sector. It is important to examine both the vulnerabilities of the NPO sector and trends in the terrorist threat at the strategic level in order to have a complete understanding of how misuse happens. The pressing problems become even more complex when considering the security danger posed by groups like Al Qaeda, alongside nongovernmental organizations (NGOs), international or national governance, and even civil society. With this study, there are no policy suggestions being proposed. This study does not present any new policy proposals; instead, it attempts to provide an analytical framework for future policy discussions on a national or international level.

Australian cases

One of three major techniques by which terrorist money is collected in Australia was the use of donations via official charity contributions, according to

Additionally, the LTTE has used several NPOs and charities to provide the logistics of its global operations. The seemingly unending supply of humanitarian groups on the internet persisted until the end of the Liberation Tigers of Tamil Eelam's armed wing. A challenging target for terrorists trying to reap the advantages of a worldwide society. Terrorist and NPO organizations exist in the same global context, frequently seeking to attract the same demographics. Most humanitarian nonprofits engage with communities impacted by war to carry out their good works. At the same time, terrorist groups use these populations to fuel the fight and find people to sympathize with their cause. There are several initiatives to serve larger populations that may result in rehabilitation for people.

FATF has identified several vulnerabilities situated at either the organizational or sectoral level and labeled them "potential targets" or "capabilities" that the danger may exploit. Consider external factors, such as nonprofit organizations, and inside players, such as employees, who may exploit NPOs for their own gain. Enabling inappropriate groups known as "sham" NGOs to join the sector and act on their behalf enables the emergence of sectoral vulnerabilities. This graph, illustrated in Figure 21, shows the link between threat, vulnerability, and the misuse of nonprofit organizations.

AUSTRAC (2010: 8) [12]. However, it appears that this type of exploitation of NPOs being used in money laundering schemes has seldom, if ever, been reported in the media. In December 2009, Aruran Vinayagamoorthy, Sivarajah Yathavan and Armugan Rajeeva accepted their guilt by admitting as their co-conspirators. He was also accused of helping Tamil Eelam Liberation Tigers (LTTE) by creating electrical parts that might be utilized for about \$97,000. Providing assets (directly or indirectly) to the LTTE, an organization prohibited by law as a terrorist group, are punishable violations under the Charter of the United Nations Act, 1945 (Cth). It was stated that the defendants had a part in the \$1,030,259 in contributions that were collected and then transferred to the LTTE between December of 2002 and October of 2004. Coghlan stated that it was probable that the defendants knew the LTTE was a banned entity in other countries, given the "complex structure" employed to transfer cash, as well as the LTTE's recognition as a proscribed organization in these other countries. (Record of proceedings, The Case of Vinayagamoorthy and Others, Coghlan J., March 31, 2010: 13) [13]. While the court allowed this, it decided that the money was provided for humanitarian aid, not intentionally supporting terrorism. From the transcript of the proceedings in the Supreme Court of Victoria in the case of Vinayagamoorthy and Others v The Commonwealth of Australia: In accordance with the jury's recommendation, Yathavan and Rajeevan was given a term of one year in jail but were freed on good behavior bonds of three years. A three-year prison sentence but given a four-year good

behavior bond (R v Vinayagamorthy & Ors [2010] VSC 148, March 31 2010) [14].

Nachum Goldberg organized it, and others Goldberg's family engaged in a money-laundering operation that is estimated to have funneled around \$48 million from Australia to Israel between 1990 and 1997. United Charity, a fake business that has not been established as a charity or firm, created an account in Goldberg's name. To cover the profits that had not been reported to the Australian Taxation Office (CDPP 2001) [15]. The Goldberg family deposited cash into one of four Israeli banks, which were the sole beneficiaries of this money. Later during the scheme's existence, other merchants, who were Jews, donated checks to Jewish charities, and these checks were used to buy cash instead.

The bank's management account status was lost following a manager change at the branch where the account was created, and a withdrawal was then made. After the account's status changed, it was caught by AUSTRAC's surveillance, which also found an unusually significant number of transactions to be occurring. The sitting judge at the appeal said that the usage of an account with this kind of activity showed that Goldberg had significant knowledge of AUSTRAC and banking procedures, as well as probable collaboration from the bank (DPP (C'th) v Goldberg [2001] VCSA 107; 2001184 ALR 387). The Commonwealth Director of Public Prosecutions (DPP) succeeded in having Goldberg convicted to a seven-year prison sentence, and Goldberg was incarcerated. Additionally, he was ordered to pay restitution to the Commonwealth of \$15 million together with his wife and two sons.

Risks to the Australian nonprofit sector

Australia has around 600,000 registered nonprofit organizations (the Productivity Commission estimates that at the end of 2010). Some of them are associations, charities, churches, clubs, foundations, groups, and unions. This wide collection of organizations includes entities that can be legally established under various laws, regulations, and various capabilities to fulfill financial and administrative management requirements are charities that are why these are thought to be especially vulnerable:

- are closely aligned to particular cultural or religious movements;
- frequently move funds or other resources to areas of conflict;
- rely on overseas-based organizations to deliver funds;
- deal in cash or alternative remittance systems (ARS); and/or

"It's more difficult to spot suspicious transactions when you have really sophisticated

financial resources" (Home Office & HM Treasury 2007).

As with any nonprofit sector, the nonprofit sector in Australia is equally vulnerable to these problems. Additional participants at roundtables at the AIC discussed characteristics that lead to NPOs' susceptibility to misuse. Studies suggest that organizations relying on informal means of financial transfer, particularly those in the unincorporated sector and smaller unincorporated companies are more vulnerable. These small NPOs don't fall under federal regulation and so are less likely to be aware of AML/CTF concerns. In addition, their makeup typically indicates that they do not have the financial or intellectual resources to undertake risk mitigation methods (as mentioned below). In light of their data, the participants agreed that there was little that could be feasibly accomplished to protect this category of NPOs from misuse, and they were concerned that weakness in outreach and education was largely to blame.

Organizations reliant on informal funding sources such as informal charity organizations, particularly those affiliated with certain religions or community groups might make their NPOs more vulnerable to fraud. With respect to the AML/CTF Act, ARS providers are referred to as "designated services." The provision of financial services providers in Australia is under the purview of the AUSTRAC. The entities must register with AUSTRAC and put in place customer identification procedures, implement an AML/CTF program, and file annual reports with AUSTRAC on their compliance with the AML/CTF Act. This means that while all providers must be registered with AUSTRAC, not all comply or are aware that they should.

An Australian AIC study that investigated the threat that ML/TF-enabled AML/CTF compliance processes pose to ARS found varying levels of compliance knowledge. Among smaller entities, some providers admitting to difficulties in meeting AML/CTF regulations especially related to the time-consuming and complex nature of reporting requirements (Rees 2010). A number of big public ARS suppliers were considered to be highly expensive by users. Therefore, the usage of services from smaller or unaffiliated providers may result in lower expenses for small nonprofits. Corrupted or poorly-run NPOs will certainly accomplish the same goal. In a 2011 assessment of oversight of Australia's anti-money laundering (AML) regime, AUSTRAC noted that smaller or unaffiliated providers are more difficult to track. The threat of misuse is potentially highest for such firms. A corporation, even one larger, cannot be entirely immune to attack. Non-profit organizations in abroad countries are primarily related to create NPOs, gained tax-exempt status and collected huge quantities of money. When nonprofit organizations attended a roundtable

discussion, they spoke about how bigger NPOs strictly followed standards and codes of behavior that help reduce exploitation chances. Although for worldwide nonprofit organizations, confirming the credentials of abroad partners was not always practicable, particularly in the event of disaster assistance and other instances of rapid reaction.

The adoption of mitigation strategies

Risk management methods aren't in place to guard against misuse of machine learning (ML/TF). A recent study conducted in the UK concluded that nonprofit organizations tended to have poor uptake of critical. Risk management protocols and procedures, such as fraud policies, and a general disregard for financial management protocols (e.g., auditing, segregation of duties, fraud reporting policies). The adoption of these protocols, together with well-designed governance mechanisms, is important in the fight against criminal and terrorist misuse (Charity Commission 2010).

NPOs in Australia have found that similar patterns have emerged. According to the findings of an NPO study, a documented risk management policy was either not established by the NPOs or was unknown to them (PPB 2010). A study in which respondents from 272 companies said that 29% of them used a fraud control policy, 13% a fraud control strategy, 26% a fraud risk assessment, and 13% a whistleblower policy (BDO Chartered Accountants and Advisors 2010) [17]. The Australian Government has published recommendations to protect organizations from ML/TF threats called *Safeguarding Your Organizations against Terrorism: A Guidance for Nonprofit Organizations*. Organizational integrity, good governance, and financial management and reporting are available in conventions via organizations such as the Australian Council for International Development and Fundraising Institute of Australia.

Balancing risk with response

The misuse of nonprofits is apparent. One of the most recorded instances of abuse for ML/TF has been creating a fake organization, which has historically always been a charity. For the most part, illegitimate charities did not use genuine charities for their ends. It is pretty common for charities to be registered with regulatory or tax authority, making their network of cash transfers part of a complicated web of money transfers via recognized channels. Despite recorded incidents of nonprofit misuse, nonprofit organizations that don't employ official systems for transferring cash or rely on informal means of payment remain at the greatest danger of exploitation. There could be a purposeful attempt to create or conceal an already existing registered entity to conceal the true purpose and nature of the organization. The case studies also demonstrate that smaller companies are more likely to

be targeted than assumed without regular or systematic surveillance.

The real danger to the Australian nonprofit sector looks to be small, but the potential risk to the industry's operations appears significant. From these roundtables and public documents, we may conclude this was how nonprofit, law enforcement, and academic participants saw the AIC's activity. An Australian NPO has been linked to financing terrorist operations in a limited number of cases. In one of these cases, it progressed to trial. It is investigating whether or not nonprofit organizations aid money laundering will provide mixed results. Risk, though, is frequently a determining factor in the decision. The nonprofit sector claims that the overall danger to the sector has been overstated. Two differing views have arisen in the UK on the appropriateness of the procedures that were implemented to limit abuse. One significant fear of the industry is that increased attention on NPOs may further stigmatize the sector and negatively impact sector activities (Crimm 2008). Although the encapsulation of authorized services utilized by NPOs under the AML/CTF Act does offer a reasonable level of security, the existing regulatory system for the nonprofit sector does not emphasize ML/TF concerns.

Nevertheless, publicly accessible information indicates that Australian-based NPOs do not have a higher ML/TF exploitation risk. By incorporating government-sponsored rules, carrying out sector outreach, and utilizing peak body standards of conduct, Australia has chosen to encourage the sector to use risk and financial management instruments while also educating the group about them. Although industry studies point to the need for further progress, it is unclear how much of the sector has really implemented these initiatives. The regulation of the Australian nonprofit sector has been criticized (e.g., see Productivity Commission 2010) [14, 15]. Australian charities and not-for-profit commissions may perhaps install a national regulator in the future (Australian Government 2011). Nonprofit sector participants of the NPO roundtable did not appear to have a hard time supporting increased regulation; participants in favor of a more stringent regulatory system stated. That the current system was ineffective in identifying non-compliant and criminal behavior modifications were needed. Despite this, there was a worry that a generalized strategy may be used to prevent a possible danger that affects only a small percentage of the industry but would still leave out companies not under present regulatory supervision. In order to avoid this kind of consequence, nonprofits should think about implementing and utilizing risk-based risk management techniques. Additionally, the Government may financially pursue initiatives that help the sector better educate itself by providing information and guidance that is based on relevant, particular intelligence instead of general weaknesses.

RECOMMENDATIONS

This paper increases our awareness of the danger presented by terrorist organizations to nonprofit organizations. These findings will be reinforced by more study. For instance, to expand our awareness of individual jurisdictions, we must conduct national-level studies on domestic violence. This will help us identify those jurisdictions with a higher risk of terrorist activity. The first recommendation that the FATF (Financial Action Task Force) has put out, which mandates all member nations to perform a national risk assessment, supports the idea of doing this sort of study. This research will aid in the investigation of new indicators and linkages. A second, related concern is that it is important to analyze the various threats (including both hazards and vulnerabilities) between net beneficiary nations and net donor jurisdictions. Finally, there is also a focus on examining NPO resources that depart the organization to defend against diversion. To sum up, more investigation and analysis on NPO resources to prevent any connection to terrorist groups or terrorist action is also required.

CONCLUSION

This study includes an increase in our understanding of the terrorism danger to non-profit organizations. This comprehension may be enhanced by more study. An excellent example of this is the necessity for comprehensive national research on child abuse in order to enhance our awareness of higher-risk jurisdictions, such as those situated in states near known terrorist organizations. When the FATF recommends that all member governments do a national risk assessment, this research is made much easier. This research will reveal previously unknown factors and look for more linkages. To further enhance assessment of NPO service-receiving vs NPO service-donating countries, there is a need to evaluate the varied threats (in terms of both risks and vulnerabilities) across those jurisdictions [18]. Additionally, this study stresses the need to scrutinize NPO resources that depart to keep them from being misused. But this doesn't mean that more study and analysis are required to eliminate any relationship with terrorist groups or activities, and therefore maintain the integrity of the NPO sector.

REFERENCES

1. (Charity Commission 2009a; FATF 2004a, 2004b). All URLs were accurate in June of 2011.
2. APG releases an annual typologies report that contains the latest money laundering developments in the Asia/Pacific region. 60 Report was issued in 2009.
3. Each year, the APG creates and releases typologies reports on money laundering patterns in Asia/Pacific. [3].
4. Asia-Pacific Group on Money Laundering (APG) presented a study in 2005 describing types of money laundering for 2005. 3.3 percent of

- Americans don't hold regular jobs and another 3.3 percent don't hold full-time jobs.
5. Current through the end of the year The Australian government's second budget proposal is available on this page. Get this, free: Treasury.gov.au.
 6. AUSTRAC typologies and case studies report 2010. Here you go:
 7. In 2008, the Australian Transaction Reports and Analysis Centre (AUSTRAC) offered this insight: Austrac typologies and case studies in 2008 described the organization's four quadrants. The document is here:
 8. The BDO Chartered Accountants and Advisers survey was completed in 2010. BDO's survey on non-profit frauds, 2010. The 2010 Not-for-Profit Fraud Survey
 9. In the paper by Bricknell, McCusker, Chadwick, and Rees, the following sentence may be found: To date, Australian nonprofit organizations have been placed at danger by money laundering and terrorism. A sequence of articles, books, and policy papers. Cairns: National Australia Museum
 10. New charity standards: Charity Commission, 2010. Charities are back on track, as seen in the results of the compliance work conducted by the Charity Commission during 2009–10. download (pdf)
 11. (Charity Commission 2010). Foundation for Enterprise Development 2012b. To help charities avoid damage, use the Compliance Toolkit. Module 3: What avenues are available to terrorists to misuse a charity? Voluntary sector grants
 12. Volunteer Centre. (2016). Charities are back on track: themes and lessons from the Charity Commission's compliance work, which took place between 2008 and 2009, are described. "Charitable organization."
 13. Annual report 2000–01 from the Commonwealth Director of Public Prosecutions (CDPP). Criminal Property Prevention Partnership, Crimm & Nelson, CDPP 2008. A measure against terrorism financing comes with its own set of moral dangers. A threat to civil society and national interests. Procedural Fairness in Adjudication:
 14. "The 2008 FATF Recommendations on Terrorist Financing." Funding for terrorists. A high ranking, neutral government agency that oversees compliance with financial regulations (FATF) 2004 nonprofit organizations should follow Nonprofit Organization Practice Recommendation VIII from the FATF. The suggestion and interpretive remark from the examiner's office Paris: Organization for Economic Co-operation and Development/Financial Action Task Force (FATF) 2004 The second half of the presentation is focused on money laundering typologies in 2003-2004.
 15. Athens: World/European Organization for Economic Cooperation and Development/FATF Financial Action Task Force (FATF) a 2003 study on money laundering typologies done in 2002–03 was conducted. The FATF Financial Transactions

and Reports Analysis Centre of Canada is located in Paris (FINTRAC) 2009. Typologies and trends in Canadian banking, as seen in the above excerpt: May 2009. Tracking People: FINTRAC

16. Flanigan Construction. (2008). The instance of Hizballah and the Tamil Tigers' use of a type of nonprofit services known as insurgent groups. Explosive Releasing as a Counterterrorism Strategy: a Literature Review
17. Is considered significant in cosmology Terrorism should not be funded by the government, and a legal reaction should be employed to make that

point. Edward Elgar: Home Office & HM Treasury at Cheltenham, UK, and HM Treasury in Northampton, MA 2007. In this publication, we present detailed analysis of protections for the charitable sector (England and Wales) against terrorist abuse. Folk etymology: London: the Home Office

18. The L-Factor the basic principle of Hamas is politics, charity, and terrorism combined for the sake of jihad. Yale University Press: The borough of New Haven, Connecticut.