Banking Non-Profit Organizations (NPOs)—How Financial Institutions can Avoid Wholesale De-Risking NPOs by Mitigating Money Laundering and Terrorist Financing Risks Posed by the Sector

Chris Galloway, CAMS-FCI
Abstract

Financial institutions (FIs) across the globe are under increasing pressure from their governments to assist with the fight against money laundering and terrorist financing (ML/TF). This scrutiny has led to the issuance of financial penalties in multiple jurisdictions in response to either noncompliance with regulations related to anti-money laundering and counter terrorist financing (AML/CTF) or FIs having inadequate risk controls that allow ML/TF to be less detectable. Consequently, many FIs have begun to implement wholesale de-risking practices by either no longer providing financial services or exiting relationships with correspondent bank partners or high-risk business sectors. One of the sectors that has been majorly affected is the nonprofit organization (NPO) sector, particularly the NPOs that provide humanitarian assistance in higher risk jurisdictions. This problem of de-risking has caught the attention of the G7, the Financial Action Task Force (FATF) and the Financial Crimes Enforcement Network (FINCEN); governments around the world are working with FIs and affected industries to try to come up with a solution. In the U.K. the government has been working closely with trade associations such as the Charity Finance Group (CFG) in order to develop strategies to ensure that NPOs receive the financial services that they require to continue their legitimate and valuable work.1

“It’s great to see the government taking de-risking seriously; charities are working all over the world in the most challenging and difficult environments, to ensure that help is given to those that need it most—but we need access to financial services. Unfortunately, some have lost access as a result of steps taken by banks to reduce risk.

Caron Bradshaw, Chief Executive of the Charity Finance Group (UK), March 26, 2015

While NPOs need access to financial services, FIs need to ensure that they manage any relevant ML/TF risks when providing that access. In order avoid a Catch-22 scenario, NPOs need to provide FIs with a greater level of transparency of operations so that FIs can understand the activity that they facilitate for their NPO clients. Adopting strong know your customer (KYC) processes can help FIs to ensure that they have the data they require to make informed and fair decisions when considering to offer financial services. Furthermore, this data can help drive an FI’s specific risk-based approach (RBA) to conducting business with NPOs so as to focus all efforts on those relationships that truly do present potential ML/TF risks.

---

1 https://www.gov.uk/government/news/economic-secretary-seeks-agreement-on-further-action-to-address-bank-de-risking
Before following an RBA, FIs will need to conduct a risk assessment of the NPO sector’s vulnerabilities to ML/TF. This paper will start by expanding on FATF’s recommendation 8 that specifically addresses this subject. The role of NPOs in funding the Islamic State of Iraq and the Levant (ISIL) will also be addressed, as will increased focus on the link between tax evasion, money laundering and NPOs. The main focus of this paper is to present a risk framework that FIs can adopt in order to provide services to legitimate NPOs and to outline the following AML/CTF areas and how they relate to NPOs:

- **Building a Risk-Based-Approach** – How FIs can avoid a one-size-fits-all approach to risk rating NPOs.
- **Risk Mitigation for NPOs** – What internal controls, generic risk mitigation and risk focused measures are applicable when conducting business with NPOs?
- **Ongoing Monitoring for NPOs** – What transaction monitoring strategies apply to NPO business on a product, geographic or client level?
- **Enhanced Due Diligence (EDD) for NPOs** – What EDD tasks can be used to obtain information to further mitigate or explain activity?

There are options available to FIs in order to avoid the need to de-risk and mitigate the risk presented by NPOs, even those that are inherently high risk by nature. While de-risking is a complicated subject and one that requires FIs to balance their own internal needs with those of others, there are solutions to the balancing act between whether to de-risk or not to de-risk. Taking a practical approach that considers de-risking on a case-by-case basis is most desirable for all parties. Legitimate NPOs can continue to receive financial services that filter through legitimate channels and FIs can manage their risk in order to appease regulators and, when necessary, provide valuable intelligence to law enforcement if they do detect ML/TF activity.
Background

In 2012, FATF consolidated its original 40 recommendations, 9 special recommendations (SR) and interpretative notes into one set of 40 recommendations. The inclusion of Recommendation 8 in the new document was an acknowledgement by FATF of the continued threat posed by certain NPOs.\(^2\) FATF states that countries should review the adequacy of their laws and regulations as they relate to NPOs, which can be particularly vulnerable to misuse in the following circumstances:\(^3\)

I. By terrorist organizations posing as legitimate entities;
II. To exploit legitimate entities as conduits for TF, including for the purpose of escaping asset freezing measures; and
III. To conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

While FATF outlines an approach specific to NPOs financing terror, this paper will address the threat of money laundering through such entities. According to the Organization for Economic Co-operation and Development (OECD), money laundering, specifically tax fraud through the abuse of charities is a serious and increasing risk in many countries.\(^4\) Whilst the processes of ML/TF are not necessarily interchangeable, there is ability for FIs to leverage synergies in the ML/TF risk mitigation strategies that they use when they offer their services to NPOs. However, rather than looking to mitigate the risk posed by NPOs, some FIs have made the decision to ‘de-risk’ their transaction activity, or the sector as a whole, based upon broad geographic de-risking.\(^5\)

This type of de-risking is not necessarily in alignment with the spirit of FATF’s guidance which, while highlighting the vulnerability of the NPO sector, also stresses the importance in the protection of the NPOs’ legitimate activities.\(^6\) Accordingly, to ensure that the charitable or other legitimate activities are not discouraged or disrupted unnecessarily, FIs should look to avoid comprehensive de-risking of the NPO sector. Consequently, when dealing with NPOs, FIs should consider adopting a RBA, which will not only help to ensure that legitimate entities can receive

\(^2\) Just after 9/11 concerns relating to the financing of terror through NPOs were originally outlined in SR VIII.
\(^3\) Adapted from FATF recommendation #8: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
\(^4\) www.oecd.org/dataoecd/30/20/42232037.pdf
\(^5\) http://www.cfg.org.uk/Policy/banking/bank-de-risking.aspx
\(^6\) http://www.fatf-gafi.org/topics/fatfrecommendations/documents/bpp-npo-2013.html
banking services, but also eliminate the FIs’ reputational risk of the association with publicized wide-ranging de-risking practices.

**To De-risk or Not to De-risk, That is the Question**

The practice of de-risking by FIs is one that has been recognized as a major problem for the NPO sectors; in a March 2015 briefing that came from the U.K.’s CFG, the organization stated that 16 of its 26 members currently believe that FIs are becoming more risk averse to the sector. In addition, this briefing states that the most common problems cited by CFG members of include delays or cancellations of international money transfers, requests for further information and the freezing of funds or closing of accounts. As a result, some charities have attempted to adopt measures to avoid or mitigate these actions, but others have resorted to having to send staff abroad with cash. Furthermore, CFG has reported that its members have incurred additional costs and time delays from dealing with these issues; it has recommended that FIs should invest more resources in learning about their NPO clients and give them proactive warnings when enhanced measures are required. In an attempt to avoid de-risking, CFG recommends that NPOs should build good relationships with their FIs and proactively provide transparency in their work.

NPOs have also been affected by the FIs’ process of de-risking money services businesses (MSBs), specifically in regards to transactions or remittances to certain jurisdictions. As a result of the spiralling failure of Somalia, Barclays’s well-publicized de-risking of transactions to that state had a major impact on NPOs that provide assistance within that jurisdiction. However, due to an enforcement crackdown and rising penalties being issued to FIs for sanctions violations, it is not surprising that they are wary of conducting business in blacklisted or so-called failed states such as Somalia. Adam Szubin, director of the U.S. Treasury’s Office of Foreign Assets Control (OFAC), the lead agency for the enforcement of U.S. financial sanctions, acknowledged this process of de-risking as understandable, considering the potential consequences. According to Szubin, the de-risking of certain customers or lines of business could be considered the correct response, especially when the risk outweighs the benefit.10

---

7 [http://www.cfg.org.uk/Policy/banking/~/media/Files/Policy/Banking/Briefing%20%20Impact%20%20of%20banks%20derisking%20activities%20on%20charities%20March%202015.pdf](http://www.cfg.org.uk/Policy/banking/~/media/Files/Policy/Banking/Briefing%20%20Impact%20%20of%20banks%20derisking%20activities%20on%20charities%20March%202015.pdf)
8 [http://www.thirdsector.co.uk/charity-finance-group-adds-its-voice-concerns-bank-de-risking/article/1338058](http://www.thirdsector.co.uk/charity-finance-group-adds-its-voice-concerns-bank-de-risking/article/1338058)
9 [http://www.ft.com/intl/cms/s/0/54aca3a4-c557-11e3-89a9-00144feabdc0.html#axzz3VdUYmg1P](http://www.ft.com/intl/cms/s/0/54aca3a4-c557-11e3-89a9-00144feabdc0.html#axzz3VdUYmg1P)
“It is not at all uncommon for me to hear that a compliance overhaul was done and certain customers, certain lines of activity were deemed too risky to persist. That may be exactly the right response to a situation where the risk outweighs the benefit.” Adam Szubin, Director of the U.S. Treasury’s Office of Foreign Assets Control (OFAC)

While Szubin accepts that de-risking may be a necessary action, he makes a distinction between de-risking and what he calls ‘extreme de-risking,’ where broad sectors are deemed too risky because of the activities of a group within that sector. This distinction is a key one, and Szubin alludes to the fact that FIs should look to follow a more granular RBA and consider providing services on a case-by-case basis. The opinion that FIs should follow an RBA is one that is also supported by FATF,11 FINCEN12 and the World Bank.13 In its statement from October 2014, FATF suggests that de-risking can inadvertently increase overall money laundering and terrorist financing risk by forcing illegal or terrorist funds to be transferred through undetectable channels. FATF believes that allowing the movement of such funds through legitimate channels enables the ability to detect and even freeze as may be appropriate.

“Moving funds through regulated, traceable channels facilitates the implementation of anti-money laundering / countering the financing of terrorism (AML/CFT) measures.”

FATF statement from October 23, 2014

De-risking is a complicated problem; in order for FIs to feel comfortable with providing services to higher risk sectors such as NPOs, there needs to be cooperation from all parties. FIs should follow an RBA and look at taking a case-by-case approach to dealing with higher risk organizations for which they are capable of accepting and managing accounts. It is also the responsibility of regulators of FIs to provide guidance on how to manage such risk. Lastly, in order for FIs to follow a ‘good’ de-risking approach, it is the responsibility of NPOs to be open and transparent so as to provide real insight into their business and help lead to effective long-term risk management for their FI partners.

ML/TF Risks for NPOs

The abuse of NPOs for ML or TF purposes presents specific challenges for the FIs that provide services for them. In order to ensure that FIs practice the process of ‘good’ de-risking, they need to be aware of what risks are presented by NPOs, how they can be abused and what activity is considered to be normal for such entities. First and foremost, there is a need to recognize that NPOs can be structured in many different forms, which can also be influenced by jurisdiction. FATF states that it recognizes that NPOs can be associations, foundations, fundraising committees, community service organizations, corporations of public interest, limited companies and public benevolent institutions, to name but a few. Correspondingly, FIs should also acknowledge that NPOs are not all the same and, therefore, ensure that they do not risk-rate them in the same manner. Consequently, the understanding of specific risks presented by various NPOs can help FIs to create and adopt a commensurate RBA and ensure that they do not disrupt or discourage the charitable or legitimate activities of NPOs. In FATF’s June 2014 report *Risk of Terrorist Abuse in NPOs* and the OECD Report on Abuse of Charities for Money Laundering and Tax Evasion, a good detailed account of the vulnerabilities of the sector is given, which is summarized in Figure 1.2 below:

---

**Figure 1.2: ML/TF Vulnerabilities of the NPO Sector**

<table>
<thead>
<tr>
<th>Who... are the NPOs that are most at risk of abuse by money launderers and terrorist entities?</th>
<th>Terrorist Financing</th>
<th>Money Laundering/Tax Evasion</th>
</tr>
</thead>
</table>
| • ‘Service’ NPOs engaged in humanitarian efforts are at higher risk of exploitation by terrorist organizations.  
• NPOs operating in the same geography, environment or populations that terrorist organizations also act are higher risk. | | • Registered NPOs who willfully participate in tax evasion ML schemes for benefit of organizers or directors.  
• NPOs that are unknowingly abused by individuals who prepare false charitable receipts. |
| What... is the nature of the threat posed by criminal and terrorist entities to the NPO sector? | | • A criminal organization will pose as a registered NPO in order to perpetrate a tax fraud scheme.  
• Funds from criminal activity can be comingled with legitimate funds and laundered by the NPO. |
| When... are NPOs most at risk of abuse by money launderers and terrorist entities? | • ‘Service’ NPOs at time of war or natural disaster when additional funds are needed are especially vulnerable. | • NPOs can be at risk at any time by money launderers or those looking to benefit from tax evasion. |
| Where... are NPOs most at risk of abuse by money launderers and terrorist entities? | • NPOs are at risk of abuse at all phases of their operations both domestically and operationally. | • NPOs are at risk of abuse in jurisdictions where there are limited regulations relating to NPOs.  
• In jurisdictions where tax credit schemes exist. |
| Why... are NPOs at risk of abuse by money launderers and terrorist entities? | • NPOs and terrorist entities operate in the same environments.  
• NPOs are targeted because they can easily and legitimately access materials, funds or networks that can also be useful for terrorist networks. | • NPOs can provide the cover of legitimacy for criminal groups.  
• NPOs can be extorted or abused due to their sometimes ‘loose’ governance structures. |

---

15 Adapted from FATF and OECD
These vulnerabilities indicate that ‘Service’ NPOs in particular are at risk of abuse by terrorist entities; below, Figure 1.3 provides eight activity types, which further detail those organizations most at risk:

*Figure 1.3: NPO Activity Types that are most vulnerable to terrorist entities*¹⁶

<table>
<thead>
<tr>
<th>Service Activities</th>
<th>Expressive Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Housing</td>
<td>Sports and Recreation</td>
</tr>
<tr>
<td>Social Services</td>
<td>Arts and Culture</td>
</tr>
<tr>
<td>Education</td>
<td>Interest Representation</td>
</tr>
<tr>
<td>Health Care</td>
<td>Advocacy</td>
</tr>
</tbody>
</table>

The OECD outlines that NPOs are especially vulnerable to money launderers or tax evaders when either the registered government status is abused for tax fraud or when illegal funds are commingled with legitimate funds. Scenarios where fraudsters pose as NPOs or tax return preparers who falsify tax returns to defraud governments are a particular vulnerability of the sector. Governments across the globe have reported major revenue losses; in Canada, for example, the government has estimated NPO-related tax abuse at approximately $200 million per annum.¹⁷ As a consequence, the Canadian government has issued stricter controls on NPO activity, resulting in a greater scrutiny on FIs that provide services to them.¹⁸

**Specific risks relating to the ‘War on Terror’ and the Fight Against the Islamic State of Iraq and the Levant (ISIL)**

Since 9/11, multiple NPOs have been forced to close operations following the discovery of links to suspected terrorist organizations. While this has been a global phenomenon, it has been particularly apparent in the U.S.—many of the charities that have been affected had established operations in regions affected by the ‘war on terror.’¹⁹ These charities have a domestic footprint as well; Figure 1.4 depicts the states that have housed NPOs with suspected links to terrorist groups:

---

¹⁷ http://www.oecd.org/dataoecd/30/20/42232037.pdf p.15
¹⁹ http://www.charityandsecurity.org/background/US_harities_designated_shut_down_by_Treasury
With the emergence of the terrorist threat posed by ISIL, the vulnerability of NPOs to being abused by terrorist entities will remain. While financing from NPOs for ISIL is considered to be minimal in comparison to other sources, there are still opportunities for abuse and a potential for foreign donor activity to raise in value; as such, FIs should continue to be well informed in order to mitigate such activity. The following five methods and risks of abuse of NPOs identified by FATF continue to be prevalent and relevant for the fight against ISIL:

1. **Diversion of funds** – Legitimate funds were ‘diverted’ by terrorist actors within the legitimate NPO
2. **Affiliation with terrorism** - NPOs have an affiliation with a terrorist entity

---

20 https://www.aclu.org/blocking-faith-freezing-charity-map
3. **Support for recruitment** - NPOs abused to provide support for recruitment efforts by terrorist entities

4. **Abuse of programming** - Legitimate NPO programs were targeted for abuse by terrorist entities

5. **False representation** - Terrorist entities started ‘sham’ NPOs

According to FATF, the most commonly observed method is the diversion of funds, with 54 percent of the many case studies used as examples involved some form of diversion by terrorist actors. The studies relating to ISIL also prove the involvement in the diversion of funds and specifically relate to the diversion of legitimate donations, which were used for terrorist actions rather than humanitarian aid. On account of these examples, FIs should take extra care in dealing with transactions to geographic locations in proximity of ISIL-controlled territory. Nonetheless, FATF does stress that while higher levels of due diligence are required, not all transactions initiated by NPOs that are destined for these areas are high risk. Consequently, FIs need to follow an RBA, ensure that they do not hinder the legitimate operations of NPOs or force them to use alternative means to transact, and make sure that they mitigate the risk presented by NPOs to guarantee that de-risking is a last and necessary resort.

"While certain payments, from, to or through NPOs operating in areas within or near ISIL controlled territory may require higher due diligence, they are not meant to imply that all transactions to or through NPOs operating in these areas are high risk."

Adapted from FATF report on Funding of the Terrorist Organization ISIL (p.20)

**Following an RBA and Mitigating ML/TF Risks Posed by NPOs**

In order to attempt to prevent, detect and report suspicious ML/TF activity, there are multiple benefits for a FI to follow an RBA. These benefits include, but are not limited to, the ability to focus due diligence and investigative processes more cost effectively for situations that warrant a greater degree of scrutiny. The RBA should be conducted on an enterprise basis; considering the potentially higher risk nature of the NPO sector, it means FIs should consider a specific RBA for NPOs.
Prior to establishing an RBA that addresses activity with NPO clients, FIs should understand how the RBA cycle depicted in Figure 1.5 applies to NPO business. The following is a summary of how these five steps can apply to NPOs:

1. **Identify risk** – Understand the risk factors for the NPO sector and ensure that adequate due diligence information is obtained at client onboarding.
2. **Set risk tolerance** – Understand what is considered to be unacceptable risk – e.g., NPOs operating in countries subject to sanctions.
3. **Mitigate risk** – Understand risk-focused measures and mitigation strategies that are appropriate for different risk levels and types of NPOs.
4. **Calculate residual risk** – Understand the risk remaining after mitigation and ensure commensurate ongoing monitoring is conducted to detect potential suspicious activity.
5. **Assess effectiveness of RBA** – Ensure that ongoing monitoring and risk mitigation strategies are commensurate with the inherent risk identified. This analysis should further drive overall risk tolerance and the methods to identify risk.
### Client Onboarding for NPOs

Obtaining adequate customer due diligence (CDD) information at the start of any banking relationship is of paramount importance to an FI that is looking to manage ML/TF risks. Understanding the purpose and intended nature of the business relationship is the starting point to help anticipate the activities and transactions of that client. Accordingly, for NPOs, due diligence questions should be customized to ensure that enough information is obtained at the beginning of a relationship so as to understand ‘what is normal’ for NPOs. *Figure 1.6* below outlines sample questions that NPOs could be asked at onboarding that are linked to ML/TF risk factors:

*Figure 1.6: Sample Due Diligence Questions for NPO Onboarding*

<table>
<thead>
<tr>
<th>Risk Factors</th>
<th>Sample Due Diligence Questions</th>
</tr>
</thead>
</table>
| Products, Services & Delivery Channels | • What type of business relationship does the NPO require?  
• What level and type of activity is expected from the NPO? |
| Geography                           | • Where is the NPO located?  
• Where does the NPO operate?  
• Where does the NPO solicit funds?  
• Who will the NPO wish to transact with and where are they located? |
| Client Information                  | • What is the purpose of the NPO?  
• What is the governance structure of the NPO?  
• Is the NPO a government registered entity?  
• Who controls the NPO?  
• How is the NPO funded (source of funds)?  
• Who are the expected beneficiaries of the funds collected by the NPO?  
• Are there any known close associates to the NPO? |

Using information from the answers to these types of due diligence questions can help drive the inherent risk rating for NPOs. Below, *Figure 1.7* depicts NPO attributes that would result in a higher or lower inherent risk rating and help drive the mitigation and monitoring measures that are required to keep the relationship within the risk tolerance of the FI:
Figure 1.7: Higher vs. Lower Risk Attributes for NPOs

**Higher Risk**
- Non-registered NPOs
- Solicit funds from the public
- Operate in high-risk international jurisdictions
- Provide 'service' activities
- Complicated governance structure

**Lower Risk**
- Registered NPOs
- Obtain funding from trusted or known sources (e.g., government)
- Operate domestically
- Less complicated operations
- Known governance structure
**Risk Mitigation for NPOs**

Risk-focused mitigation is additional to general AML/CTF internal controls, such as the provision for adequate supervision of employees that handle transactions. Any mitigation strategies that are used should be commensurate and applicable to the higher risks posed by clients such as NPOs. Figure 1.8 below lists some examples of generic risk mitigation measures as well as risk focused measures that could be implemented:

*Figure 1.8: Generic Risk Mitigation and Risk-Focused Measures for NPOs*

- **Generic Risk Mitigation**
  - Enhanced NPO risk-specific training for NPO client facing staff
  - Increased risk review of NPO accounts
  - Increased frequency of ongoing monitoring for NPO accounts
  - Review internal controls for NPO accounts

- **Risk Focused Measures**
  - Establish transaction limits (geographic limitations or dollar amounts)
  - Limit transaction methods (e.g., face-to-face transactions only)
  - Escalate approval for NPO accounts or higher risk transactions

These types of controls are a good starting point in order to reduce inherent risk and to ensure that any residual risk is within the FI’s risk tolerance. The implementation of controls can help to build whatever EDD measures may be required either at the time of onboarding or as a result of ongoing monitoring. In addition, these controls will help to build an ongoing monitoring framework that can be product-, geography-, and type-of-business- or even client-specific, as required.
Ongoing Monitoring for NPOs

The likelihood of detecting ML/TF activity is dependent on the utilization of effective ongoing monitoring systems and the employment of intellectual talent to be able to decipher and investigate the results. The starting point for setting rules for ongoing monitoring is to first understand what is normal so that activity that falls outside of this sphere is easily identifiable. The ability to comprehend what is normal is dependent on the quality of KYC information and the use of transaction monitoring systems so the FIs are able to set rules specific to product-, geography- or client-level risk factors.

1. **Product level** – Enhanced monitoring for higher risk products used by NPOs (e.g., international wire transfers).

2. **Geography level** – Enhanced monitoring for higher risk geographies in which NPOs operate (e.g., countries that have a high incidence of terrorism [see Figure 1.9 below] or known tax havens).

3. **Client level** – Monitoring that ensures that transactions are in line with expected source of funds, destination of funds and level of activity as a result of risk review of NPO accounts.

*Figure 1.9: Global Terrorism Index Map of the World*\(^{23}\)

---

**EDD for NPOs**

In the event of inadequate KYC information, or even as a result of an alert from ongoing monitoring, EDD is required in order to further mitigate risk. Dependent on the size and complexity of an FI, investigators will often be tasked with conducting EDD; a major part of EDD is to obtain as much information about the NPO client in question from its operational and relationship management team. As well as requesting further information from the first line of defence (or in the U.S., initiating the 314(b) process), investigators can also obtain additional information from the NPO themselves or from open source or paid subscription services. Figure 1.10 outlines some of the tasks to consider for EDD of NPOs:

*Figure 1.10: EDD Tasks for NPOs*

<table>
<thead>
<tr>
<th>Generic EDD Requirement</th>
<th>EDD tasks for NPOs</th>
</tr>
</thead>
</table>
| Obtain additional information about the client | ✓ Request proof of entity existence (e.g., financial records/bill of goods or services)  
✓ Request NPO tax records  
✓ Conduct Internet site search (e.g., valid IP etc.)  
✓ Conduct internet search/negative news search—using tools available (e.g., Google, social networking) |
| Obtain information on the source of funds or source of wealth of the client | ➢ Ask NPO for more details of financial status including those of beneficial owners/related individuals  
➢ Obtain documentation relating to funding methods  
➢ Verify using background searches/document requests |
|-----------------------------|-------------------------------------------------------------------------------------------|
| Obtaining information on the reasons for intended or conducted transactions | ➢ Ask NPO for more details of volume and reasons projected transactions (and product type) at account opening  
➢ Ask NPO for more details at time of or after transaction as to intended purpose  
➢ Conduct due diligence/background check in relation to relevant beneficiary parties of transactions |

**NPO Case Study – Red Flags that Can Help with Detection of Potential ML/TF Activity**

**Terror Financing Suspect Headed Local NPO**

A 44-year-old Ontario man who pleaded guilty to Canada's first TF charge once headed a Vancouver NPO that Canada's intelligence service alleges was a front for the illegal Tamil Tigers.

Canadian resident Prapaharan Thambithurai was convicted with TF for raising money for the Liberation Tigers of Tamil Eelam (LTTE) in Canada’s first case involving fundraising for a banned terrorist group. Thambithurai admitted receiving between $2,000 and $3,000 in donations between late 2007 and March 2008, acknowledging that he knew part of the money would go to the LTTE, which was banned in Canada in 2006. This case also relates to $75,000 that was raised in Vancouver by an NPO.

---

following the Boxing Day 2004 Tsunami in Sri Lanka. This NPO was also suspected of being linked to the LTTE at the time.\(^{25}\)

**Potential Red Flags to Help FIs detect TF activity:**

- EFTs to the benefit of individuals and entities located in high-risk jurisdictions
- Large cash deposits with source of funds either unknown or solicited as donations from the public
- Checks deposited that are made payable to unknown third parties
- Unknown destination of funds and/or remittances to unknown third parties
- Deposits of cash often followed by the purchase of bank drafts to unknown third parties or sent offshore to unknown beneficiaries

**Conclusion**

The NPO sector is growing, and in Canada alone it has doubled in size in terms of revenue and expenditure in just over 10 years. Below, Figure 1.11 shows that total revenue and expenditures in 2009 were over $400 billion combined:

*Figure 1.11: The Growing NPO Sector in Canada*\(^{26}\)


There are similar trends across the globe. In order for NPOs to be able to continue to grow and provide the invaluable services to global populations, they will need to have access to legitimate financial services. While some NPOs are vulnerable to abuse from ML/TF organizations, and those that are, only make up a fraction of the NPOs that operate globally. Accordingly, FIs should not treat all NPOs the same, should not classify all NPOs high risk and most importantly should not practice ‘bad’ de-risking and look to exit relationships or refuse to onboard NPOs based on their status. This type of de-risking is mutually detrimental to both NPOs and FIs with such actions potentially having reputational consequences for FIs. A recent example of negative publicity was the media and public reaction to the wholesale de-risking of transactions to Somalia by Barclays that affected MSBs and NPOs alike.27

FIs need to balance their approach to de-risking. In order to protect their institution from abuse by ML/TF organizations, ensure that they are compliant with regulatory expectations and maintain a good reputation. This balancing act can be achieved by following an RBA and by not implementing wholesale ‘bad’ de-risking practices when dealing with NPOs, or indeed any other business sector. Working in partnership with NPOs to ensure greater levels of transparency and dealing with higher risk scenarios on a case-by-case basis aligns with guidance provided by both

---

FATF and FinCEN. This can be achieved by creating an environment with greater focus on the NPOs that present a higher risk, and the starting point is to understand which NPOs are most vulnerable to ML/TF.

Through a combination of robust KYC, risk mitigation and ongoing monitoring processes, FIs can feel comfortable doing business with higher risk NPOs. In addition, a strong AML/CTF compliance regime can increase the likelihood of detecting suspicious activity, which can also help increase the likelihood of law enforcement halting the same activity. This is achieved by FIs ensuring staff understand the risks presented by NPOs through relevant role and risk-specific training and through following a sector-specific RBA with commensurate risk mitigation, ongoing monitoring and EDD processes. Rather than ‘washing their hands’ and potentially allowing suspicious activity to move into an underground economy, FIs can help NPOs continue to carry out their legitimate activities while providing information to law enforcement on those that do not conduct legitimate activity. Following an RBA rather than wholesale de-risking, the NPO sector can help to boost an FI’s reputation with the public, law enforcement and government regulators alike.

References

Book References


Website (& document) References

- http://www.fatf-gafi.org/topics/fatfgeneral/documents/rba-and-de-risking.html
- www.oecd.org/dataoecd/30/20/42232037.pdf
http://www.cfg.org.uk/Policy/banking/bank-de-risking.aspx
http://www.cfg.org.uk/Policy/banking/~/media/Files/Policy/Banking/Briefing%20%20Impact%20of%20banks%20derisking%20activities%20on%20charities%20March%202015.pdf
http://www.thirdsector.co.uk/charity-finance-group-adds-its-voice-concerns-bank-de-risking/finance/article/1338058
http://www.ft.com/intl/cms/s/0/54aca3a4-c557-11e3-89a9-00144feabdc0.html#axzz3VdUYmg1P
http://www.oecd.org/dataoecd/30/20/42232037.pdf
http://www.oecd.org/dataoecd/30/20/42232037.pdf p.15
http://www.charityandsecurity.org/background/US_harities_designated_shut_down_by_Treasury
https://www.aclu.org/blocking-faith-freezing-charity-map
http://en.wikipedia.org/wiki/Global_Terrorism_Index#/media/File:Global_Terrorism_Index.svg