ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Specified Non-Profit Organisation

Sector Specific AML/CFT Guidance Notes

January 2018

Contact:
AML Unit, Enforcement Division
Financial Services Authority
PO Box 58,
Finch Hill House,
Bucks Road,
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000 Fax: 01624 646001
Website: www.iomfsa.im Email: aml@iomfsa.im

Contents

1. Foreword

Specified Non-Profit Organisations ("Specified NPOs" or "S.NPOs") are defined by Schedule 4 to the Proceeds of Crime Act 2008 ("POCA") as:

> "a body corporate or other legal person, trustees of a trust, partnership, other association or organisation and any equivalent or similar structure or arrangement, established solely or primarily to raise or distribute funds for charitable, religious, cultural, educational, political, social or fraternal purposes with the intention of benefiting the public or a section of the public and which has-
>
> (i) an annual or anticipated annual income of £5,000 or more; and
> (ii) remitted, or is anticipated to remit, at least 30% of its income in any one year to one or more ultimate recipients in or from one or more higher risk jurisdictions;"

This means that a non-profit organisation will only be required to comply with the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015 ("the Code") if it has an income (or expected income) of more than £5,000 AND it sends (or is expected to send) 30% or more of its income to a higher risk jurisdiction. Guidance on higher risk jurisdictions is provided at section 7 and further guidance on how to determine whether an organisation is a non-profit organisation is provided at section 3 of this document.

S.NPOs are required to comply with the Code because they are considered to be exposed to increased risk of being inadvertently abused for terrorist financing. S.NPOs may also be abused for money laundering purposes but typology reports indicate that the biggest risk is terrorist financing. Non-profit organisations have been high on the agenda of international bodies such as the FATF in recent years and there are many case studies available to provide examples of how non-profit organisations including charities can be set up for illicit purposes or abused by criminals.

2. Introduction

The purpose of this document is to provide some guidance specifically for the S.NPO sector. This sector specific guidance should be read in conjunction with the AML/CFT Handbook. It should be noted that guidance is not law, however it is persuasive. Where a person follows guidance this would tend to indicate compliance with the legislative provisions, and vice versa.

This document will cover unique money laundering and financing terrorism ("ML/FT") risks that may be faced by the S.NPO sector and will provide further guidance in respect of customer due diligence ("CDD") measures where a one size fits all approach may not work. Also, some case studies are included to provide context to these unique risks. The information included in this document may be useful to relevant persons to assist with their risk assessment obligations under the Code.

This document is largely based on the Financial Action Task Force ("FATF")'s 2013 report *Combatting the Abuse of Non-Profit Organisations*.[1] The Authority recommends that relevant persons familiarise themselves with this, and other typology reports concerning the S.NPO sector.

3. Are you a Specified Non-Profit Organisation?

Schedule 4 to POCA refers to the "business of a specified non-profit organisation". This means the activity is the sole or primary purpose of the organisation. For example, if a shop raises funds for a charity, the shop's primary business is retail and not "raising or distributing funds for charitable, religious, cultural, educational, political, social or fraternal purposes with the intention of benefiting the public or a section of the public". Therefore this organisation is not in the business of being a S.NPO. However if the same shop had a subsidiary or associated organisation whose sole purpose was to raise funds as above, this would be considered its sole or primary business.

If you are unsure as to whether you may be bound by the Code, the following flow chart should assist. If you remain in doubt you may wish to consider seeking legal advice.

Please note that the Code requirements apply to all business relationships and occasional transactions of an S.NPO, not just the transactions made to higher risk jurisdictions.

			Does the AML/CFT Code apply?
1. Is the activity done by way of business (i.e. the organisation's main activity is non-profit work)? If yes go to 2.	No	Not a Relevant Business	**No**
2. Does the organisation raise, or is anticipated to raise over £5,000 in a 12 month period? If yes go to 3.	No	Not a Specified NPO	**No**
3. Is more than 30% of that turnover sent outside the Island? If yes go to 4.	No	Not a Specified NPO	**No**
4. Is that money sent to a higher risk jurisdiction? If yes go to 5.	No	Not a Specified NPO	**No**
5. This is a Specified Non-Profit Organisation			**Yes**

[1] http://www.fatf-gafi.org/media/fatf/documents/reports/Combating_the_abuse_of_NPOs_Rec8.pdf

4. What is Terrorist Financing?

Section 7.3.2 of the AML/CFT Handbook provides general guidance on terrorist financing, and Appendix L includes further detailed guidance. Further detail is provided below about the dangers faced by NPOs specifically.

Section 7.3.2 of the main body of the Handbook provides a general definition as to what constitutes terrorist financing. The term is a generic one which is not defined in any Isle of Man Statute, but was set out in the United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention) 1999 and includes the financing of terrorist acts, terrorist organisations or individual terrorists. The various terrorist financing offences can be found in Part III of the Anti-Terrorism and Crime Act 2003. These include the offences of:

- Fund raising (section 7);
- Use and possession (section 8);
- Facilitating funding (section 9);
- Financing travel (section 9A);
- Money laundering (section 10); and
- The Failure to Disclose: regulated sector offence (section 14).

It is particularly important to note that whilst the *mens rea*[2] for the other offences require knowledge or reasonable cause to suspect use for terrorist purposes, the offence of Facilitating funding can also be committed when the *offender has failed to exercise due diligence as to whether it will or may be used for the purposes of terrorism*.

The direct (estimated) costs involved in carrying out terror attacks have been quite widely reported. The table below gives an indication of the approximate costs of some of the more recent high profile attacks.

Date	Attack	Country	Estimated Cost
12 October 2000	USS Cole bombing	Aden (Yemen)	USD 10,000
12 October 2002	Bali bombings	Bali	USD 50,000
11 March 2004	Madrid train bombings	Spain	USD 10,000
7 July 2005	London transport bombings	UK	GDP 8,000

[2] 'guilty mind', having awareness that the act is criminal

13 November 2015	Paris attacks	France	EUR 27,000
14 July 2016	Nice truck attack	France	EUR 2,500
22 May 2017	Manchester Arena bombing	UK	Investigation ongoing
3 June 2017	London Bridge attack	UK	Investigation ongoing

As can be seen the direct cost of each of these attacks is relatively low and appears to be decreasing, particularly with the recent use of unsophisticated, inexpensive but effective *modus operendi*.

Because of the high profile given to the direct costs, it is easy to obscure the bigger picture. The broader operational costs which underpin terrorist activity are significantly higher and include:

- The costs involved in promoting a militant ideology;
- Paying operatives and often their families expenses such as subsistence;
- Death in service – when terrorists die, the terrorist organisation often supports the family;
- Arranging for travel for training and to stage attacks;
- Training new members;
- Buying or renting safe houses;
- Forging documents;
- Paying bribes; and
- Acquiring weapons.

Many of these expenses will, by necessity, be incurred in secret and will therefore incur a "clandestine premium". In addition, the source of the funds used must be obscured to prevent that source being disrupted. As these operational costs are quite high, terrorist organisations are dependent on a steady, sustained funding stream.

5. Why are S.NPOs Vulnerable?

High intensity of cash:
NPOs, especially charities, tend to be highly cash intensive with the majority of funds being raised from a high number of relatively small donations. Large volumes of cash transactions undertaken by NPOs are routine and therefore are not considered unusual by either Banks or Money Transmission Services ("MTS"). In countries where many NPOs operate, the financial

services infrastructures are often rudimentary and underdeveloped, making cash (most commonly USD or EUR) the medium of choice. This makes it almost impossible to trace where funds are being raised from, and where they are actually going, making it the perfect medium for clandestine operations.

Cash donations can be either unreported or under-reported and so diverted to third parties with no trace or records. As above, cash movements are considered normal with NPOs and so would not trigger the same concern should an individual attempt to send a large quantity of low denomination cash to a higher risk jurisdiction.

Reputable:
The fact that most NPOs are highly trusted not only by donors, but also government bodies, due to the nature of their selfless works, means that they are may be subject to less scrutiny than other organisations. It is this vulnerability to abuse for FT that that threatens the sector as a whole. When cases are reported where NPOs have been using charitable funds for FT, this has an effect on donor confidence and trust. Following the aftermath of the September 11 attacks in 2001, donations to international charities fell, and those to Muslim charities fell dramatically.[3]

Logistics:
Having a global presence with a high turnover of volunteers can lead to NPOs being infiltrated by terror groups and resources pilfered or otherwise redirected. Also, a global network allows the relatively easy movement of assets and personnel between branches all over the world, in the event that an NPO has been compromised, this network can be used by terrorists to travel and move equipment with less scrutiny than they may do otherwise.

6. Complicit vs Exploited

It is understood that there are two types of NPO that can become involved in criminal activities; those that are complicit and those that are exploited.

Complicit:

A complicit NPO is one established or knowingly used for the purpose of supporting terrorist organisations. Types of support include:

(a) raising funds from legitimate donors and transferring them through a network to terror cells;
(b) the provision of a vehicle through which to launder the proceeds of crime;
(c) raising of funds for legitimate causes and payment of a portion of the money to the genuine beneficiaries while funnelling the remainder to terrorists; and/or
(d) operational support.

[3] http://www.ustreas.gov/press/releases/reports/js5071.pdf

NPOs can be used to provide operational support to terror networks by providing terrorists with a front to travel to and from terrorist training camps and bases located in high risk countries without arousing the attention of the authorities. NPO's operational areas are frequently located in countries which have a higher risk of terrorist activity, often because their work is providing services and resources that the government should do, but is incapable of doing so. As an extension to this, the NPO can also be used as a vehicle to transport equipment, supplies and even weapons, often trading on the trusted status normally given to NPOs to avoid detailed scrutiny.

Relevant persons should exercise caution when dealing with correspondent NPOs. Guidance on the Code requirements in respect of correspondent NPOs is provided at section 12.2 of this guidance.

Exploited (non-complicit):

Legitimate NPOs can be exploited by those who would wish to commit harm in many different ways, the three most commonly reported however are:

(a) where branch offices are unknowingly compromised by terrorists or where one or more officers have infiltrated the organisation, either at a senior level to direct resources, or at a grassroots level to divert resources on the ground. These issues are a more significant risk for larger NPOs where there are a high number of volunteers and workers around the globe;

(b) smaller NPOs will usually be made up of a small handful of close associates making infiltration impractical or impossible, however due to the size of small NPOs, transferring resources to where they are needed often requires the use of correspondent NPOs or other persons on the ground. A number of cases have been reported in FATF and World Bank typologies where well-meaning NPOs have sent funds to correspondents who are affiliated with terror groups posing as charitable organisations;

(c) some terror organisations may attempt to pass themselves off as workers or officers of a legitimate NPO while actually having nothing to do with it.

7. Higher Risk Jurisdictions

The Code makes reference to two lists of higher risk jurisdictions, List A and List B, which are explained further below. S.NPOs should also consider the risks posed by jurisdictions not included in these lists as there may be additional jurisdictions that pose a higher risk to the NPO sector. S.NPOs should take into consideration typology reports for their sector, their own experience in the sector and publically available information and news sources.

LIST A – "the High Risk List" (a copy is provided at Appendix D(a) of the AML/CFT Handbook)

List A specifies jurisdictions regarding which the FATF (or a FATF-style regional body) has made a call on its members and other jurisdictions to apply countermeasures to protect the international finance system from the ongoing and substantial risks emanating from the jurisdiction.

Any customer (or in the case S.NPOs, a beneficiary) resident in, located in or engaged in business activity in a jurisdiction in List A must be treated as higher risk.

LIST B – "the May-Be High Risk List" (a copy is provided at Appendix D(b) of the AML/CFT Handbook)

List B specifies jurisdictions with strategic AML/CFT deficiencies or those considered to pose a higher risk of ML/FT.

Any customer (or in the case S.NPOs, a beneficiary) resident in, located in or engaged in business activity in a jurisdiction in a List B jurisdiction may pose a higher risk of ML/FT. This means that they do not have to be considered as higher risk but the Authority would expect the S.NPO to be able to demonstrate why this higher risk factor did not result in them being classified as higher risk.

8. Application of the Code

The Code is broken down into the following sections:

Part 1 – Introductory	Applies to all sectors
Part 2 – General requirements	Applies to all sectors
Part 3 - Risk assessment and ongoing monitoring	Applies to all sectors
Part 4 – Customer due diligence	Some parts apply*
Part 5 – Specified non-profit organisations	Applies only to S.NPOs
Part 6 – Simplified due diligence	Parts may apply to S.NPOs
Part 7 – Reporting and disclosures	Applies to all sectors
Part 8 – Compliance	Applies to all sectors
Part 9 – Miscellaneous	Not relevant to S.NPOs
Part 10 – Offences and revocations	Applies to all sectors

*Customer due diligence:

Paragraph 10 – New business relationships	Does not apply to S.NPOs
Paragraph 11 – Continuing business relationships	Does not apply to S.NPOs
Paragraph 12 – Occasional transactions	Does not apply to S.NPOs
Paragraph 13 – Beneficial ownership and control	Does apply with the exception of 13(5)
Paragraph 14 – Politically exposed persons	Does apply to S.NPOs
Paragraph 15 – Enhanced customer due diligence	Does apply to S.NPOs

Guidance on each of the above listed sections is available in the AML/CFT Handbook. Additional guidance, specific to the S.NPO sector is provided in the following sections of this document.

9. Who is your Customer?

Throughout the Code the term "customer" is used. In respect of S.NPOs, customer is defined as:

> "the persons, or groups of persons, who receive benefit (either directly or indirectly) for charitable, religious, cultural, educational, political, social or fraternal purposes. For the purposes of paragraphs 17 and 18, a customer is considered to be establishing a relationship."

For clarity:

A beneficiary or group of beneficiaries – is your customer and you will have established a business relationship. You are required to do a customer risk assessment, conduct due diligence in line with paragraph 17 (and 18 in respect of continuing relationships) of the Code and conduct ongoing monitoring of the business relationship in line with paragraph 9 of the Code.

A donor – is not your customer. You do not have to do a customer risk assessment but donors should feature in your business risk assessment (paragraph 6 of the Code). Donors conduct occasional transactions and you must conduct due diligence in line with paragraph 19 of the Code. Paragraph 9 (ongoing monitoring) does not apply as this is not a business relationship, however, your business risk assessment must be regularly reviewed, amended and kept up-to-date.

A correspondent NPO – is the term used to describe an NPO that acts as an intermediary between a S.NPO and its customers (beneficiaries). A correspondent NPO is not your customer but you will be considered to have established a business relationship. You do not have to do a customer risk assessment but correspondent NPOs should feature in your business risk assessment (paragraph 6 of the Code). You are required to conduct ongoing monitoring of the business relationship in line with paragraph 9 of the Code.

Further detail on the risk assessment, ongoing monitoring, due diligence requirements for customer, correspondents and donors are provided later in this document.

10. Risk Assessment and Ongoing Monitoring

The Code requires risk assessments and ongoing monitoring in relation to both ML and FT to be undertaken. This section focuses primarily on FT risks as typology reports indicate that this

is the primary risk for the NPO sector. General guidance in relation to the risk assessment and ongoing monitoring of both ML and FT risks can be found in the AML/CFT Handbook.

10.1. Business risk assessment

In order to adequately assess the risk of FT, the NPO should examine how terrorists raise funds, move funds and use funds and how the NPO's services may be abused or hijacked for FT purposes. NPOs should also strive to keep this knowledge current and ensure that education within the organisation is kept up to date. The Authority will continue to conduct outreach and update this guidance on an ongoing basis to assist with this.

The business risk assessment should include a review of relationships with correspondent NPOs and donors who donate over the threshold of €15,000[4] (or currency equivalent).

Please refer to section 3.1 of the AML/CFT Handbook for general guidance on business risk assessments.

10.2. Customer (beneficiary/beneficiaries) risk assessment

The customer risk assessment process is undertaken to determine the level of ML/FT risk a customer (beneficiary or group of beneficiaries) poses and therefore determines whether standard or enhanced CDD is required.

A customer risk assessment must be undertaken prior to sending funds to them, or if this is impractical or impossible due to urgency or other exceptional circumstances, this may be undertaken while the funds are being raised and completed as soon as possible afterwards. In these instances, the S.NPO should document the reasons why this delay was necessary.

Please refer to section 3.3 of the AML/CFT Handbook for general guidance on customer risk assessments.

10.3. Ongoing monitoring

Paragraph 9 of the Code requires an S.NPO to perform ongoing and effective monitoring of any business relationship. This includes customers (beneficiaries and groups of beneficiaries) and correspondent S.NPOs.

For S.NPOs ongoing monitoring should include an element of public domain checks. Names should be regularly checked against sanctions lists and for negative press that would alert the S.NPO to any allegations of illicit activity such as connections to terrorism.

General guidance on sanctions can be found at section 7.3.5 of the AML/CFT Handbook.

[4] Occasional transactions of an S.NPO under €15,000 (whether a single transaction or a series of linked transactions) fall under the Code definition of an exempted occasional transaction. This means that the requirement to verify the identity of a donor is disapplied.

General guidance on customer screening in relation to sanctions and negative press can be found at section 3.4.3 of the AML/CFT Handbook.

General guidance ongoing monitoring can be found at section 3.4 of the AML/CFT Handbook.

11. Customer Due Diligence

Paragraphs 10 to 12 and 13(5) of the Customer Due Diligence requirements in Part 4 of the Code do not apply to S.NPOs. Instead they must comply with paragraphs 16 – 18 under Part 5 of the Code.

Paragraphs 14 (politically exposed persons) and 15 (enhanced customer due diligence) of the Code do apply to S.NPOs. Paragraph 13 (beneficial ownership and control) of the Code applies with the exception of 13(5).

General guidance on politically exposed persons is found at section 4.15 of the AML/CFT Handbook.

General guidance on enhanced customer due diligence is found at section 4.3.6 of the AML/CFT Handbook.

General guidance on beneficial ownership and control is found at section 4.3.4 of the AML/CFT Handbook.

12. S.NPO Code Requirements

Part 5 of the Code fundamentally requires S.NPOs to complete the following actions before or during the formation of a business relationship* or occasional transaction. Please note that the Code requirements apply regardless of the risk rating of the transaction or customer relationship or whether it is domestic or international in nature.

Where the Code requirements are not met, the business relationship or transaction should proceed no further and the S.NPO should consider making an internal disclosure in line with paragraphs 26 and 27 of the Code.

12.1. CDD – Beneficiary/group of beneficiaries

Paragraph 17 (and 18 in respect on continuing relationships) of the Code require the S.NPO to:

(a) identity the customer (beneficiary or group of beneficiaries)

(b) take reasonable measures to verify that identity using reliable, independent sources; and
(c) obtain information on the nature and purpose of the business relationship.

It is expected that in many cases an S.NPO will transfer funds for the benefit of a group of persons, quite often a large group. Where there is a group (or class) of beneficiaries, the NPO should identify the class as a whole – for example "Uganda Orphans" rather than to identify each individual child. Where funds are sent to a sole beneficiary, the identification and verification methods described in section 4 of the AML/CFT Handbook should be adopted keeping in mind a risk based and flexible approach should be taken.

Identifying the objects of the S.NPO is expected to be a relatively straight forward matter. The S.NPO's objects are typically set out in its constitutional documents and, in the case of charities, this will be information filed with the Central Registry. If the S.NPO sends funds to those beneficiaries listed in the constitutional document, then the identification element would be deemed to have been met. The constitutional documents would normally also assist in obtaining information on the nature and intended purpose of the business relationship.

The verification process requires the S.NPO to take reasonable measures to verify the identity of the class of beneficiaries. This could be achieved by taking measures to ensure that the group of beneficiaries are legitimate (not a front for a terrorism organisation, for example) and that the funds are actually going where they are intended to go.

Methods could include:

(a) obtaining receipts from those who are responsible for the allocation and distribution of funds to account for expenditure;
(b) determining whether the apparent expenditure seems reasonable for the proceeds sent;
(c) considering whether feedback and communications from the correspondents and the beneficiaries seem normal based on the S.NPO's previous experience; and
(d) conducting visits to the location or some of the locations where funds are applied to ensure that expenditure seems reasonable for the proceeds sent.

The key to successful verification of the group of beneficiaries and minimising the risk to the S.NPO and its officers is to apply reasonable professional scrutiny to make sure that funds are being applied and accounted for properly.

General guidance on how to identify and verify the identity of both natural and legal persons is provided in section 4 of the AML/CFT Handbook.

12.2. CDD – Correspondent NPOs

Paragraph 17 (and 18 in respect on continuing relationships) of the Code require the S.NPO to:

> (4) in the case of any correspondent non-profit organisation receiving funds on behalf of a customer, identify that correspondent non-profit organisation, and take reasonable measures to verify that correspondent non-profit organisation's identity using relevant information obtained from reliable, independent sources..

The Authority understands that a number of NPOs transfer funds to larger international NPOs, other parts of their wider organisation or to other correspondents in order to ultimately send onto the beneficiaries. The Code requires S.NPOs to identify correspondent NPOs and take reasonable measures to verify their identity using reliable, independent sources. S.NPOs should take reasonable measures to verify that the correspondent is genuine and that the funds are reaching the ultimate beneficiaries and not be subverted.

The Authority would expect correspondent NPOs to be identified and verified using the stand methods detail in section 4 of the AML/CFT Handbook.

Where an NPO is donating money to another NPO without any specific objects for the funds to be applied to, this would not be a correspondent NPO relationship. For example:

A local charity raises £10,000 and gives this money to Save the Children (a UK based charity). This money may be applied for any purposes that Save the Children see fit including applying to its own operational costs. This would not be a correspondent NPO relationship.

Alternatively, a local charity raises £10,000 and gives this money to Save the Children (a UK based charity) to be applied to the children of Syrian refugees. The class of beneficiaries would be the children of Syrian refugees and Save the Children in this case would be a correspondent NPO.

12.3. CDD – Donors

Paragraph 19 of the Code refers to the term "occasional transaction". Where a S.NPO receives funds from a donor over the threshold of €15,000 or currency equivalent (whether as a single transaction or a series of linked transactions[5]), paragraph 19 requires the S.NPO to take reasonable measures to identify and verify the identity of that donor using reliable, independent sources.

This relationship between a donor and S.NPO would <u>always</u> be considered, for the purposes of the Code, to be an occasional transaction and as such would never be considered as "forming a business relationship".

The Authority would not expect an S.NPO to collect full identification information as detailed in section 4 of the AML/CFT Handbook for all donors who donate amounts under the occasional transaction threshold. A risk based approach should be taken to the collection of information giving consideration to the nature, value and ML/FT risks of the transaction.

[5] In respect of linked transactions the Authority would consider 12 months to be a reasonable timeframe in which the transactions have taken place.

The vast majority of donors will, in practice, be those who donate less than €15,000 in which case the occasional transaction exemption under paragraph 19(4) applies, this exempts the S.NPO from having to verify the identity of those donors.

Generally those who donate significant sums will be provided a receipt for tax purposes which will contain identification information that could be used to meet the requirements of the Code.

For finance and other designated businesses, verification of identity would usually be expected to include obtaining certified or verified identification and proof of address documents. In the case of a S.NPO, it is felt that by rigidly applying these standard methods, there is a risk of deterring people from making a donation.

S.NPOs should exercise a level of judgement on what methods they use to verify the identity of a donor. Often for large donations, the donor will be a wealthy individual or a company. For example, the internet can be used as a valuable source of information. The S.NPO should take care to document what verification methods were used and why they were felt appropriate in order that they can demonstrate this to competent authorities if required.

13. Simplified Due Diligence - Acceptable Applicants

Part 6 of the Code provide a number of "concessions" whereby reduced CDD measures may be applied in certain situations. Most of these concessions would not be relevant to a S.NPO, however, they may be able to use the "acceptable applicant" concession for certain corporate donors.

Paragraph 20 of the Code disapplies the requirement to verify the identity of acceptable applicants provided that certain criteria are met. Further guidance on this concession is provided in section 6.3 of the AML/CFT Handbook.

14. Case Studies

The case studies below are real life examples where risks have crystallised resulting in actual cases of ML/FT in respect of NPOs. The case studies included in this document are based on news articles regarding this sector.

14.1. UK Registered Charity linked to Hamas

The Interpal case is well known a series of claims against NatWest by US citizens and the heirs of foreign citizens injured or killed in ten terrorist attacks in Israel in 2002 and 2003. It was claimed that, by having maintained accounts and processed transfers in the UK for Interpal (a

Palestinian charity registered with the UK Charities Authority), NatWest provided material support to terrorist organisations such as Hamas.

At the time the accounts were maintained by NatWest in the UK, Interpal was designated as a terrorist organisation only by the authorities in Israel. It was only later in 2003 that Interpal was placed under sanctions by OFAC. At all material times, NatWest acted lawfully in the UK, where the accounts were operated. Nevertheless, the bank now finds itself defending, at considerable expense, a claim that, whether or not it succeeds, will do nothing to enhance its reputation. If the claims succeed, the US Anti-Terrorism Act's treble-damages provisions are likely to guarantee that the sums in damages will be substantial.

S.NPOs should take away from this case that even a fairly large and well-known UK registered charity can be involved with terrorist financing. It is essential that S.NPOs truly understand who their correspondent NPOs are and conduct research, name screening etc. to check for sanctions or negative press.

14.2. US Registered Charity used to Violate Iranian Sanctions

Mr Y was an Iranian individual residing in the US. In 1994 he set up a US non-profit organisation with the stated intention of providing care for impoverished orphans all over the world. The NPO received tax-exempt status from the IRS in 1995 which required the annual filing of a form. Despite the NPO's claims of its intended purposes, investigation determined that the NPO was in fact used as a means to transport funds to Iran and make investments. A portion of the funds was provided directly to the Government of Iran violating US sanctions laws prohibiting the provision of funds to Iran due to its ongoing support of international terrorism and other illicit activities.

14.3. Diversion of NPO Funds

A registered domestic NPO provided a group of its volunteers with fundraising materials including collection buckets, identity badges and letters of credential. These individuals purported to raise funds and other goods in support of individuals affected by a humanitarian crisis on behalf of the NPO. In addition to fundraising, the volunteers were tasked with distributing the donations to those in need.

The NPO's directing officials had minimal oversight of the activities of its volunteers including the distribution of donations, evidenced by a lack of records. The directing officials were unable to show that the funds and goods raised were distributed for the intended purposes and could only rely on the accounts provided by its volunteers.
A national NPO regulator examination found that one of the volunteers retained control over the NPO's fundraising material in contravention of a domestic designation, which included financial sanctions, based on suspected links to terrorism. The NPO regulator alerted the NPO's directing officials to the designation and advised them to take action to ensure that any property belonging to the NPO was recovered and to prevent further financial activity in breach of domestically-imposed sanctions.

The possibility of the designated individual having used the NPO's fundraising materials to collect and solicit donations in support of terrorism cannot be discounted.