

**GUIDE FOR COMPANIES LIMITED BY
GUARANTEE CONCERNING MONEY
LAUNDERING AND TERRORISM
FINANCING**

Table of Contents

1.	INTRODUCTION	2
2.	FINANCIAL ACTION TASK FORCE INITIATIVES AGAINST MONEY LAUNDERING AND TERRORISM FINANCING, AND THE IMPACT ON NPOs, INCLUDING CLG-NPOS	2
2.1	Overview of the FATF and Singapore’s commitment.....	2
2.2	Scope of FATF Recommendation 8 and its application to NPOs, including CLG-NPOs	3
2.3	The impact of money laundering and terrorism financing and the differences between them.....	4
2.4	The important role of NPOs, including CLG-NPOs, in the global community and their vulnerability to being abused by terrorists	5
2.5	Legislation concerning anti-ML and counter-TF in Singapore.....	6
3.	METHODS AND RISK OF ABUSE OF NPOs, INCLUDING CLG-NPOs, AND CASE STUDIES.....	6
3.1	How CLG-NPOs may be abused by money launderers and terrorist financiers.....	6
3.1.1	Diversion of funds.....	6
3.1.2	Affiliation with a terrorist entity.....	7
3.1.3	Abuse of programming.....	7
3.1.4	Support for recruitment	7
3.1.5	False representation or sham entities.....	8
3.2	Case studies of NPOs which were abused.....	8
3.2.1	Diversion of funds by actors internal to NPOs (Collection phase)	8
3.2.2	Diversion of funds by actors internal to NPOs (Retention phase).....	8
3.2.3	Diversion of funds by actors external to NPOs (Transfer phase)	9
3.2.4	Abuse of Programming (Delivery of programmes phase)	9
3.2.5	False front	9
4.	HOW CAN CLG-NPOs PROTECT THEMSELVES AGAINST ML/ TF RISKS	10
4.1	Maintaining strong corporate governance and financial transparency	10
4.2	Knowing key donors and beneficiaries	10
4.3	Accepting and applying funds in a manner consistent with the CLG-NPO’s objects.....	11
4.4	Conducting financial transactions through regulated financial channels.....	11
4.5	Reporting suspicious transactions to the Suspicious Transaction Reporting Office (STRO)	11
4.6	Fund Raising for foreign charitable purposes	12
5.	EXAMPLES OF SUSPICIOUS INDICATORS OF ML AND TF	12

GUIDE FOR COMPANIES LIMITED BY GUARANTEE CONCERNING MONEY LAUNDERING AND TERRORISM FINANCING

1. INTRODUCTION

1.1 This guide is prepared for directors and other officers of companies limited by guarantee (CLG), which are also non-profit organisations (NPOs). A CLG-NPO may be at risk of being abused for money laundering (ML) or terrorism financing (TF) or other forms of terrorist support by virtue of its characteristics or activities. This guide provides more information about these risks, and provides examples of good practices that CLG-NPOs can adopt to help them to identify and manage its exposure to such risks.

1.2 A NPO is defined as “a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of ‘good works’.”¹

2. FINANCIAL ACTION TASK FORCE INITIATIVES AGAINST MONEY LAUNDERING AND TERRORISM FINANCING, AND THE IMPACT ON NPOs, INCLUDING CLG-NPOS

2.1 Overview of the FATF and Singapore’s commitment

Singapore is a member of the Financial Action Task Force (FATF). The FATF is an independent inter-governmental body which establishes international standards (known as “FATF Recommendations”) that develop and promote policies to prevent ML and TF, and the proliferation of weapons of mass destruction. The FATF monitors the progress of its members in implementing these standards, and promotes the adoption and implementation of international co-operation and appropriate measures. As a member of the FATF, Singapore is committed to implementing the FATF Recommendations and is evaluated by FATF for our level of compliance with these Recommendations.

¹ *Best Practices Paper on Combating the Abuse in Non-Profit Organisations (Recommendation 8)*, FATF (2015), p.7.

2.2 Scope of FATF Recommendation 8 and its application to NPOs, including CLG-NPOs

2.2.1 FATF Recommendation 8 requires that countries review their laws and regulations to ensure that NPOs will not be abused for TF; “NPOs are particularly vulnerable, and countries should ensure that they cannot be abused:

- by terrorist organisations posing as legitimate entities;
- to exploit legitimate entities as conduits for TF, including for the purpose of escaping asset-freezing measures; and
- to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.”²

2.2.2 FATF studies have found that the NPOs most at risk appear to be those engaged in ‘service’ activities³, for example, those engaged in programmes focused on providing housing, social services, education or health care.⁴ Specifically, ‘service’ NPOs principally engaged in the provision of humanitarian services are the most desirable targets for terrorists because of the types of resources involved in their operations, the geographic breadth of their operations, and their access to vulnerable populations.⁵ NPOs operating in environments or populations that terrorist movements actively target are also at a higher risk of abuse.⁶

2.2.3 Notwithstanding this, FATF emphasises that “measures adopted by countries to protect the NPO sector from terrorist abuse should not disrupt or discourage legitimate charitable activities.”⁷ The ultimate purpose of taking these measures is to “promote transparency, integrity and public confidence in the management and

² *Recommendation 8*, in FATF (2012), p.13.

³ As opposed to ‘expressive activities’ referring to programmes focused on sports & recreation, arts & culture, interest representation or advocacy such as political parties, think tanks and advocacy groups.

⁴ ‘*Best Practices Paper on Combating the Abuse in Non-Profit Organisations (Recommendation 8)*’, FATF (2015), para.16, p. 13.

⁵ *Ibid.*

⁶ *Ibid.*

⁷ ‘*Interpretive Note to Recommendation 8 (Non-Profit Organisations)*’ in FATF (2012), para.3, p.54.

functioning of all NPOs, and are integral to ensuring the sector cannot be abused for terrorist financing.”⁸

2.3 The impact of money laundering and terrorism financing and the differences between them

2.3.1 ML occurs as a result of a criminal act and is a process which the illegitimate sources of property or proceeds are disguised in order to make it appear legitimate, so that money launderers can benefit from their crimes and avoid detection by law enforcement authorities. TF refers to the facilitation of the financing of acts of terror. Investigations into ML are led by law enforcement authorities and are primarily about gathering evidence to prosecute criminal offenders, whereas investigations into TF are more preventive in nature and intelligence led.

2.3.2 A commonality between ML and TF is that concealing the proceeds of crime is similar to concealing the usage of terrorist funds. However, the difference lies in the fact that funds from TF can come from both legitimate and illegitimate sources. Legitimate sources of funds include funds raised by a CLG-NPO that may in turn be used to support terrorist activities or terrorist organisations. NPOs are also targeted by terrorists because NPOs can easily and legitimately access materials, funds and networks which terrorists require.

2.3.3 While ML has an impact on society over time, TF’s impact on the public is greater and felt more immediately if the financing enables a terrorist attack. Thus, even if TF has a lower probability of occurrence, due to the severity of impact it causes, FATF recommends that the risk of TF should be mitigated earlier than the risk of ML.

2.3.4 ML and TF activities may have a detrimental impact on Singapore’s economy and security. In an increasingly global economy, the impact of ML and TF may have far-reaching effects. With the expansion of both physical and electronic financial infrastructure, ML and TF activities are becoming more and more sophisticated and challenging to detect. As funds can now move across borders more conveniently,

⁸ *ibid.*

regulatory authorities and enforcement agencies within and across countries have to co-operate and co-ordinate effectively to address emerging risks. To help build and maintain Singapore's strong reputation as a well-regulated financial hub, everyone plays an important role in combating ML and TF.

2.3.5 More information about anti-ML or counter-FT can be obtained from <http://www.cad.gov.sg/aml-cft>. You may also obtain a copy of the Commercial Affairs Department's anti-ML and counter-FT Handbook at <http://www.cad.gov.sg/publications/cad-anti-money>.

2.4 The important role of NPOs, including CLG-NPOs, in the global community and their vulnerability to being abused by terrorists

2.4.1 NPOs play a vital role in the world economy, complementing national economies and social systems by providing essential services. Their efforts complement the activities of governmental and business sectors in providing essential services, comfort and hope to those in need around the world. Unfortunately, terrorists are exploiting the NPO sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations. Therefore, protecting the NPO sector from terrorist abuse is necessary to fight terrorism to preserve the integrity of NPOs and to retain donor confidence.⁹

2.4.2 NPOs are attractive to terrorists for various reasons:

- enjoys public trust; or
- have access to considerable sources of funds, often cash-intensive; or
- may have a global presence that provides a framework for national and international operations and financial transactions; or
- may often be subject to little or no governmental oversight; and
- may require few formalities for creation.¹⁰

⁹ *Ibid*, para.1, p.54.

¹⁰ *Ibid*, para.2, p.54.

2.5 Legislation concerning anti-ML and counter-TF in Singapore

- 2.5.1 The primary legislation for ML in Singapore is the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) and the Terrorism (Suppression of Financing) Act (TSOFA).
- 2.5.2 The CDSA criminalises the laundering of proceeds derived from drug trafficking, tax evasion and other serious offences. Under the CDSA, it is mandatory for any person to lodge a Suspicious Transaction Report (STR) if he knows or has reason to suspect that any property may be connected to a criminal activity. The failure to do so may constitute a criminal offence.
- 2.5.3 The TSOFA not only criminalises TF but also imposes a duty on a person to provide information pertaining to TF to the police. The failure to do so may constitute a criminal offence. Under the TSOFA, any person shall lodge a STR if he has possession, custody or control of any property belonging to any terrorist or if he has information about a transaction or any transaction in respect of, or any property belonging to any terrorists.

3. METHODS AND RISK OF ABUSE OF NPOs, INCLUDING CLG-NPOs, AND CASE STUDIES

3.1 How CLG-NPOs may be abused by money launderers and terrorist financiers¹¹

The following are some methods identified by FATF in which NPOs may be abused.

3.1.1 Diversions of funds

This means that an NPO, or an individual acting on behalf of an NPO, diverts funds into a known or suspected terrorist activity. For example, funds raised by NPOs for humanitarian programmes are diverted to support terrorism at some point through the NPO's business process. Both internal and external individuals may act as fundraisers to raise funds in the name of the NPO to support terrorist purposes, with

¹¹ 'Risk of Terrorist Abuse in Non-Profit Organisations' in FATF (2014), p.36.

or without its knowledge. An NPO might also be used to launder money or be used as a legitimate front to move funds from one place to another.

3.1.2 Affiliation with a terrorist entity

This means that an NPO or an individual acting on behalf of an NPO maintains an operational affiliation with a terrorist organisation or supporters of terrorism. For example, individuals supporting terrorist organisations may work as staff of a NPO while maintaining contact with fellow terrorist representatives, with or without the NPO's knowledge. Affiliations range from informal personal connections involving NPOs directing officials and terrorists, to more formalised relationships between NPOs and terrorists. The resources and facilities of the NPO may be used or are used to create an environment which supports or promotes terrorism recruitment related activities.

3.1.3 Abuse of programming

This means that NPO-funded programmes meant to support legitimate humanitarian purposes are manipulated at the point of delivery to support terrorism. For example, a NPO may be established to advance religion and education in the jurisdiction in which it is operating. However, such activities could be manipulated by advancing philosophies designed to promote recruitment to a terrorist organisation.

3.1.4 Support for recruitment

This means that NPO-funded programmes or facilities are used to create an environment which supports and/or promotes terrorism recruitment activities. For example, NPOs may be involved in transferring funds to terrorists, providing financial support to families of terrorists, organising and hosting events that support terrorists, and publishing materials supporting terrorism or terrorists. They may also use their facilities to recruit and train individuals to engage in acts of terror, provide meeting places for terrorists, and host speakers that advocate terrorism.¹²

¹² 'Risk of Terrorist Abuse in Non-Profit Organisations' in FATF (2014), para.118 & 119, p.46.

3.1.5 False representation or sham entities

This means that under the guise of charitable activity, an organisation or individual raises funds and/ or carries out other activities in support of terrorism. Terrorists may try to set up organisations as a sham front, raising funds, promoting causes and carrying out activities in support of terrorism. Companies may also be set up as a shell or front company to launder funds.

3.2 Case studies of NPOs which were abused¹³

3.2.1 Diversion of funds by actors internal to NPOs (Collection phase)

A company was established with very broad commercial purposes. Numerous small deposits were made to the company's account by the individual who had signing authority on the account. These funds were immediately transferred to foreign-based companies. An investigation by the national financial intelligence unit revealed that the individual with signing authority on the company's account was also a directing official of an NPO. It was suspected that the small deposits made into the company's account originated from fundraising by the NPO. Law enforcement information indicated that the NPO was known to have ties to a terrorist group. A second directing official of the NPO, who was also a manager of the company, also had ties to the terrorist group. The investigation concluded that the company was a front company being used as a conduit to transfer funds on behalf of the NPO linked to a foreign terrorist group.

3.2.2 Diversion of funds by actors internal to NPOs (Retention phase)

A NPO was raising funds supposedly for humanitarian relief in an area of conflict. The NPO used collection boxes outside religious institutions to solicit donations. The funds raised were held in a bank account. The founder of the NPO was suspected of diverting the funds to facilitate terrorism rather than using them for the stated humanitarian activities. A law enforcement investigation resulted in the arrest of the founder of the NPO for terrorism facilitation offences. The case is still under

¹³ *Ibid*, p.36. Note that the case studies are from foreign jurisdictions.

investigation. While to date there has been no conviction, USD 60,000 in collected funds have been seized.

3.2.3 Diversion of funds by actors external to NPOs (Transfer phase)

A NPO was established to support charitable work in foreign areas of conflict. An investigation by the national financial intelligence unit, initiated by suspicious transaction reporting, revealed that locally collected funds were being transmitted to foreign-based charitable organisations. The investigation also uncovered that, once the funds were received by the foreign-based charitable organisations, they were systematically passed on to persons or organisations which were part of, or affiliated with, a known terrorist organisation. While there were established connections between the foreign-based charitable organisations and the terrorist organisation, direct links between the NPO and the terrorist organisation could not be substantiated.

3.2.4 Abuse of Programming (Delivery of programmes phase)

A NPO was carrying out religious and educational activities with no foreign activities. Information provided by the national financial intelligence unit indicated that the NPO had received over USD 13,000 from a foreign organisation known to provide support to a foreign terrorist group. Subsequent open source research indicated that the NPO's education programs espoused an ideology that was shared by several foreign terrorist groups. Concerns arose that this shared ideology was being exploited for recruitment purposes for a terrorist organisation. The NPO was audited by the national regulator, and the audit found that the NPO could not account for the origin of much of its income and expenditures. Based on this, the NPO was deregistered.

3.2.5 False front

A NPO established as a cultural youth association was the recipient of several government grants. A law enforcement investigation into the operations of the NPO found that it was a front organisation for a terrorist group. The real activities of the

NPO included raising and managing funds for the terrorist group and disseminating the group's extremist message through the Internet. While the NPO had a formally constituted governing body, it was created and directed by members of the terrorist group. The principal individuals involved were arrested and the NPO and its website were shut down.

4. HOW CAN CLG-NPOs PROTECT THEMSELVES AGAINST ML/ TF RISKS

4.1 Maintaining strong corporate governance and financial transparency

CLG-NPOs should maintain robust financial management and have internal processes that promote transparency and accountability to safeguard themselves against ML/TF risks. CLG-NPOs are also encouraged to conduct regular reviews of their internal controls, policies and procedures, key charitable programmes and partnerships to protect themselves from ML/TF risks. For example, does the CLG-NPO have proper internal control systems with proper procedures for key processes, such as procurement and payment, revenue and receipts, and a system to ensure proper delegation of authority and appropriate limits of approval? Are there measures in place to ensure proper segregation of duties and adequate checks and balances, especially over financial matters such as the collection, handling of cash, depositing, transfer of funds and the issuing of receipts?

4.2 Knowing key donors and beneficiaries

4.2.1 CLG-NPOs should carry out reasonable due diligence checks on their key donors and beneficiaries, while respecting donor confidentiality.

4.2.2 To facilitate compliance, please subscribe to the Monetary Authority of Singapore Targeted Financial Sanctions website for updates.

<http://www.mas.gov.sg/regulations-and-financial-stability/anti-money-laundering-counteracting-the-financing-of-terrorism-and-targeted-financial-sanctions/targeted-financial-sanctions.aspx>

4.3 Accepting and applying funds in a manner consistent with the CLG-NPO's objects

CLG-NPOs should always know what their funds are being accepted and used for, and review their expenditure to ensure that funds are channelled towards causes which are in line with their objects. For example, is the CLG-NPO's name being used to support a person or causes which it is not familiar with? If the CLG-NPO is in partnership with another organisation on charitable projects, does it have a clear written agreement outlining the activities which will be undertaken and how they will be monitored and accounted for, and that the agreement is complied with?

4.4 Conducting financial transactions through regulated financial channels

CLG-NPOs should check that financial transactions are conducted through regulated financial channels to minimise any potential abuse while the funds are in transit.

4.5 Reporting suspicious transactions to the Suspicious Transaction Reporting Office (STRO)

4.5.1 A CLG-NPO should lodge a STR if there is a reasonable suspicion of ML or TF activities during the course of its administration or operations. STRs provide useful information to law enforcement authorities for the detection of criminal wrongdoings.

4.5.2 Under the CDSA and TSOFA, it is mandatory for any person to lodge a STR if he has:

- reason to suspect that any property represents the proceeds of, or is connected to a criminal activity; or
- possession, custody or control of property or information about any transaction (or proposed transaction) relating to any property belonging to terrorists.

4.5.3 A STR may be lodged in writing to:

Head, Suspicious Transaction Reporting Office
Commercial Affairs Department
391 New Bridge Road #06-701

Police Cantonment Complex Block D
Singapore 088762

4.5.4 Alternatively, if a CLG-NPO has a valid user account on the STR On-line Lodging Systems (STROLLS), its authorised officer may lodge an STR via STROLLS. Please email STRO@spf.gov.sg to find out if your CLG-NPO has a valid STROLLS account.

4.6 Fund raising for foreign charitable purposes

If CLG-NPOs wish to conduct fund-raising for foreign charitable purposes, they must first apply to the office of the Commissioner of Charities for a permit. To apply for the permit, they must be organisations (be it incorporated or unincorporated) in Singapore and submit the application at least 30 days before the commencement of the fundraising appeal. The CLG-NPO concerned will be asked to submit the following documents during its application:

- proof that the beneficiary is a bona fide organisation in its country;
- letter from the beneficiary acknowledging that fund-raising activity is being held in its name; and
- governing instrument of the charity or intended beneficiary.

For more information, please refer to the [Charity Portal](#).

<https://www.charities.gov.sg/Fund-Raising/Pages/Fund-Raising%20for%20Foreign%20Charitable%20Purposes.aspx>

5. EXAMPLES OF SUSPICIOUS INDICATORS OF ML AND TF

5.1 The following are a non-exhaustive list of suspicious indicators of ML:

- (a) The donor or beneficiary is unwilling to provide complete information about its beneficial owners or underlying beneficiaries;

- (b) A large number of fund transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements; or foreign exchange transactions performed on behalf of donors or beneficiaries;
- (c) The goods or services purchased by the beneficiary do not match the needs of the operations; or payment for goods or services made by cheques are not drawn from the beneficiary's corporate account; or
- (d) Large donations are made using a personal account or donor makes large contributions which do not seem to commensurate with the donor's known background or income.

5.2 The following are a non-exhaustive list of suspicious indicators of TF:

- (a) No logical purpose in the financial transactions or there appears to be no link between the stated charitable activities of the beneficiary and the parties in the transaction;
- (b) A large number of donations made through fund transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements, or foreign exchange transactions performed on behalf of donors or beneficiaries, followed by fund transfers to locations having no apparent connection with the donors or beneficiaries or to high risk terrorist areas; or
- (c) Multiple accounts used to collect and channel funds to a small number of beneficiaries, particularly in high risk terrorist areas or transactions involving foreign currency which are subsequently transferred to high risk terrorist areas within a short period of time.

If you have any queries on this guide, please email us at Contact_CERD@acra.gov.sg.

CORPORATE SERVICE PROVIDERS ENFORCEMENT & REGULATORY DEPARTMENT (CERD)
ACCOUNTING & CORPORATE REGULATORY AUTHORITY

31 OCTOBER 2015