GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

FINANCIAL INTELLIGENCE UNIT

MINISTRY OF FINANCE

FIU REFERENCE: GN/004/2019

ANTI-MONEY LAUNDERING/COUNTER FINANCING OF TERRORISM/ PROLIFERATION FINANCING (AML/CFT/PF) GUIDANCE NOTE FOR NON-PROFIT ORGANISTIONS (NPOs)

PURPOSE

The Financial Intelligence Unit ("the FIU") provides the following overview of the obligations under the Anti-Money Laundering/Counter Financing of Terrorism ("AML/CFT") regime of Trinidad and Tobago for Non-Profit Organisations ("NPOs"). The purpose of this document is to provide industry specific guidance for NPOs in Trinidad and Tobago on their legal obligations to detect and deter Money Laundering (ML), Financing of Terrorism (FT) and Proliferation Financing (PF) activities using a risk based approach. It is provided as general information only. It is not legal advice, and is not intended to replace the Anti-Money Laundering/Counter Financing of Terrorism/Proliferation Financing (AML/CFT/PF) Acts, Regulations and Orders.

The use of the word **"must"** indicates a mandatory requirement, **"should"** indicates a best practice and the word **"may"** indicates an option for you to consider.

This guidance includes:

- An explanation of ML, TF and PF;
- The role and function of the FIU in the AML/CFT/PF regime;
- The main AML/CFT/PF legal obligations and how these should be applied;
- How to identify suspicious transactions and "red flags" specific to NPOs;
- Links to FIU Publications and Forms which provide additional detailed guidance:
  - Customer Due Diligence guide;
  - STR/SAR reporting Form and guidelines;
  - Terrorist Funds reporting Form and guidelines;
  - Economic Sanctions reporting Form and guidelines;
- How to build an effective compliance programme
- Model compliance programme; and
- Offences and penalties.

CONTENTS

PART A

INTRODUCTION AND BACKGROUND

Money laundering, financing of terrorism and proliferation of weapons of mass destruction (ML/FT/PF) continue to be global threats to the security of States and financial systems. The Financial Action Task Force (FATF)[1] which is an independent inter-governmental body that develops and promotes policies to protect the global financial system against (ML/FT/PF) developed the **FATF 40 Recommendations**[2]- the globally recognised anti-money laundering (AML), counter financing of terrorism (CFT) and counter proliferation financing (CPF) standards. As a member of the Caribbean Financial Action Task Force (CFATF), Trinidad and Tobago aims to implement the FAFT 40 Recommendations to address the said crimes.

NPOs by their nature are also vulnerable to crimes. An NPO may be set up as a sham business to bring illegally obtained funds into the financial system. Also, legitimately obtained funds can be abused by terrorists to finance terrorist activities. For example, a NPO may organise fundraising activities where the contributors to the fundraising activities believe that the funds will go to relief efforts abroad, but, some or all the funds are actually transferred to a terrorist group.

In light of the vulnerability of NPOs to ML/FT/PF, **Recommendation 8 of the FAFT 40 Recommendations** requires countries to review the adequacy of their laws and regulations that relate to NPOs identified as being at risk to terrorist financing abuse, and those countries should apply focused and proportionate measures in line with a risk based approach. In taking a risk based approach, countries should use all relevant sources of information in order to identify features and types of NPOs, which by virtue of their activities or characteristics are likely to be at risk for terrorist abuse. The objective of this Recommendation is to ensure that NPOs are not misused by terrorists or terrorist organisations to: (i) pose as legitimate entities; (ii) exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes but diverted for terrorist purposes. With the aim of complying with **Recommendation 8,** the Parliament of Trinidad and Tobago has enacted the **Non- Profit Organisation Act, No. 7 of 2019 ("the NPOA").** The NPOA was made to provide for the registration of NPOs, the establishment and maintenance of a register of NPOs, the obligations of NPOs and for other related matters. It was assented to on April 23, 2019.

The NPOA brings NPOs under the AML/CFT/PF regime of Trinidad and Tobago. By adopting a risk based approach Section 4(1)(a) of the NPOA specifies that only those NPOs with a gross annual income of more than five hundred thousand dollars ($500,000) will be supervised by the Financial Intelligence Unit of Trinidad and Tobago ("the FIU") for compliance with AML/CFT laws. All other NPOs are required to:

- assess their risk based on the nature of transactions, payment methods and jurisdictions they conduct transactions;
- implement mitigating measures to protect themselves from being abused; and
- report to the FIU once they identify a suspicious transactions or confirm they have received property from a designated individual or entity.

[1] http://www.fatf-gafi.org/

[2] http://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)

PART B

REGISTRATION

All NPOs must be registered as NPOs under the NPOA. To be registered under the NPOA, the controller must complete an application as prescribed under Section 5(4) of the NPOA and submit to the Registrar General. The penalty for operating a NPO that is not registered with the Registrar General is liable on conviction on indictment to a fine of fifty thousand dollars ($50,000) and to imprisonment for seven (7) years.

Under the NPOA, a NPO is defined as:

- a body of persons incorporated or unincorporated which is established primarily for the promotion of patriotic, religious, philanthropic, charitable, educational, cultural, scientific, literary, historical, artistic, social, professional, fraternal, sporting or athletic purpose or some other useful object and raises or disburses funds for that purpose or object;
- which carries on its business without pecuniary gain to its members or officers except as reasonable compensation for services rendered; and
- restricts the use of any of its profits or other accretions to the promotion of its purpose or object.

Further, all non-profit companies registered under the **Companies Act Chap 92:01** are deemed to be registered as a NPO under the NPOA.

Thus, if you are the owner or controller of an organisation which falls within the above definition of an NPO, **you must make an application for registration to the Register General.**

PART C

DO THESE OBLIGATIONS APPLY TO YOU?

AML/CFT/PF is everyone's responsibility. It is important to note that whilst all citizens of Trinidad and Tobago are subject to the AML/CFT/PF legislation and orders, further obligations are imposed on business sectors which face a greater risk of coming across illicit proceeds and terrorist property than others. Some of the business sectors which have been identified as more vulnerable by FATF include Attorneys-at-Law and Accountants when performing certain specific functions, Real Estate agents, Private Members Club, Dealers in precious metals and precious stones and Trust and Company service providers and now, certain **NPOs.** These business sectors are identified as "Listed Businesses" under the First Schedule to the **Proceeds of Crime Act, Chap. 11:27** as amended (POCA). The FIU in accordance with the **Financial Intelligence Unit of Trinidad and Tobago Act ("the FIUA")** and Regulations has the responsibility of AML/CFT/PF compliance supervision of non-regulated financial institutions and listed business collectively called "Supervised Entity".

Regarding NPOs, the FIU is responsible for the AML/CFT/PF supervision of NPOs with a gross annual income of more than five hundred thousand dollars ($500,000) using a risk based approach, and the FIU has the powers and duties conferred on it by the NPOA, the FIUA, POCA, ATA and any other written law to implement its supervisory role. In accordance with Section 2 of the NPOA, *Gross Annual Income* means any of the following received by the NPO in a financial year:

a) income from the provision of goods and services;
b) rental income;
c) interest or other income received from investments;
d) donation, grants or subventions;
e) loans; and
f) other income, cash or monetary worth of property and assets acquired.

Therefore, if you operate a NPO with a gross annual income of more than five hundred thousand dollars ($500,000) you are a Listed Business and therefore are required to comply with legal obligations under the AML/CFT/PF laws of Trinidad and Tobago on a risk-sensitive basis, or in other words, using a risk based approach. Under the risk-based approach, the greater the risks, the more controllers have to do to ensure that they have discharged their duty of care and other legal duties. The FIU as your AML/CFT/PF Supervisory Authority monitors your AML/CFT/PF compliance.

The FIU will use a risk based approach to determine the level of supervision required for the NPOs, meaning that if your NPO engages in activities which pose a greater risk to ML, TF and PF your organisation may have more obligations to comply with AML/CFT/PF laws, regulations and orders than a lower risk NPO.

PART D

ABOUT THE FIU

The FIU is Trinidad and Tobago's Financial Intelligence Unit. The FIU was established under the FIUA in accordance with Recommendation 29 of the 40 Recommendations of the FATF. Recommendation 29 mandates all its member jurisdictions to have a FIU to serve as the information related arm in efforts to combat ML/FT/PF and related crimes.

The FIU was created as an administrative type FIU, in that it does not have law enforcement or prosecutorial powers. Rather, it is a ***specialised intelligence agency*** which is legally responsible for ***producing financial intelligence*** for Law Enforcement Authorities ("LEAs"). The FIU became operational in 2010 upon proclamation of the FIUA. It is an autonomous department within the Ministry of Finance.

The FIU works in very close partnership with individuals and entities that have obligations under the AML/CFT/PF regime. Financial Institutions and Listed Businesses (individuals and entities) have specific obligations to report information to the FIU known as "Reporting Entities". NPOs have such obligations and are therefore considered a Reporting Entity.

PART E

WHAT THE FIU DOES

(1) ANALYSES AND PRODUCES INTELLIGENCE REPORTS

Essentially, the FIU is responsible for **producing financial intelligence** that is then disclosed to foreign FIUs and LEAs for ML/FT investigations. To do this, the FIU receives and requests financial information from various Reporting Entities such as, banks, credit unions and other financial institutions, accountants, NPOs, Attorneys-at-Law, money services businesses, art dealers, motor vehicle sales, real estate, and private members' clubs.

On receipt of a suspicious transaction/ suspicious activity report (STR/SAR), the FIU analyses it and looks for links between the information received, other relevant information from different sources, intelligence provided by LEAs, as well as other international partners. Once the analysis leads to the belief that the transaction is related to the commission of a ML/FT or related criminal conduct, the FIU sends an intelligence report to LEAs who will investigate the matter. The LEAs to whom the FIU may send a report to carry out any criminal investigations are the Commissioner of Police, Comptroller of Customs and Excise, Chief Immigration Officer and Chairman of the Board of Inland Revenue.

The FIU receives many STRs/SARs from Reporting Entities, but within those reports there can be legitimate transactions. The FIU's analysis is therefore, to ensure that only those transactions on which there are reasonable grounds to suspect are related to ML/FT are disclosed to LEAs. Only transactional information and information relating to the suspicion of ML/FT are contained in the Intelligence report. For example, the name and other information on the person who actually submitted the report would not be provided to LEAs.

(2) SUPERVISES FOR AML/CFT/PF COMPLIANCE

Another important function of the FIU is the responsibility of ensuring compliance with obligations under the POCA as amended, the ATA as amended and the Regulations under those Acts and the Economic Sanction Orders. The FIU is the Supervisor for Listed Businesses and Non-Regulated Financial Institutions which have obligations under those Acts and Regulations and is responsible for ensuring that they meet those obligations.

Activities related to our compliance mandate would be educating and providing guidelines (such as this), enhancing public awareness of ML/FT/PF to allow entities who have AML/CFT/PF obligations to be aware and know exactly what they need to do in terms of meeting their obligations. The FIU also conducts compliance examinations on a risk based approach and takes action to ensure compliance with the AML/CFT/PF laws by supervised entities.

PART F

WHAT IS MONEY LAUNDERING?

The offence of ML is the process by which illegally obtained funds are given the appearance of having been legitimately obtained. ML begins with the commission of criminal activity which resulted in benefits/gains (illegal funds) to the perpetrator. The perpetrator will then try to disguise the fact that the funds were generated from criminal activity through various processes and transactions which may also involve other individuals, businesses and companies. There is no one single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g., cars or jewellery) to passing money through legitimate businesses and "shell" companies or as in the case of drug trafficking or other serious crimes. The proceeds usually take the form of cash which needs to enter the financial system by some means.

There are three (3) acknowledged methods in the ML process. However, the broader definition of ML offences in the POCA includes even passive possession of criminal property.

(1) Placement

'Placement' refers to the process by which funds derived from criminal activity are introduced into the financial system. Examples of Placement are depositing cash into bank accounts or using cash to purchase assets. Techniques used include "structuring" or "smurfing", where instead of making a large deposit transaction and in order to avoid suspicion or detection the illegal receipts are broken up into smaller sums and deposited into single or multiple accounts sometimes using other persons to deposit the cash.

(2) Layering

'Layering' takes place after the funds have entered into the financial system. It involves the movement of the money. Funds may be shuttled through a complex web of multiple accounts, companies, and countries in order to disguise their origins. The intention is to conceal, and obscure the money trail in order to deceive LEAs and to make the paper trail very difficult to follow.

(3) Integration

The money comes back to criminals "cleaned", as apparently legitimate funds. The laundered funds are then used to fund further criminal activity or spent to enhance the criminal's lifestyle.

Successful money laundering allows criminals to use and enjoy the income from the criminal activity without suspicion which is why the AML/CTF/PF legislative and compliance regimes are important crime fighting tools.

PART G

WHAT IS FINANCING OF TERRORISM?

FT is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike ML, funds can come from both legitimate sources as well as from criminal activity. Funds may come from personal donations, profits from businesses and charitable organisations e.g., a charitable organisation may organise

fundraising activities where the contributors to the fundraising activities believe that the funds will go to relief efforts abroad, but, all or part of the funds are actually transferred to a terrorist group. Funds may also originate from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Unlike ML, which usually involves proceeds derived from criminal activity, FT involves both legitimate funds as well as funds derived from criminal activity being used in support of executed and planned terrorist activity.

Similar to money launderers, terrorist financiers also move funds to disguise their source, destination and purpose for which the funds are to be used. This is to prevent leaving a trail of incriminating evidence, to distance the funds from the crime or the source, and to obscure the intended destination and purpose thereby avoiding suspicion or detection.

CASE STUDIES

The case studies [3]in **Appendix I** 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 FATF Report "Risk of Terrorist Abuse in Non-Profit Organisations" dated June 2014.

PART H

WHAT IS PROLIFERATION OF WEAPONS OF MASS DESTRUCTION?

PF is the manufacture, acquisition, possession, development, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use for non-legitimate purposes), in contravention of national laws or international obligations. It includes technology, goods, software, services or expertise.

To combat this crime, targeted financial sanctions relating to the prevention, suppression and disruption of PF and its financing should be implemented, according to FATF Recommendations. Targeted financial sanctions means asset freezing and prohibitions, without delay, to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.

[3] Source - FATF Report 2014: Risk of Terrorist Abuse of Non Profit Organisations - http://www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html

PART I

YOUR AML/CFT/PF OBLIGATIONS

The AML/CFT/PF laws of Trinidad and Tobago in which you will find your obligations are:

(1) **Proceeds of Crime Act, Chap: 11:27 as amended ("the POCA")** – establishes procedures for the confiscation of proceeds of crime and for the criminalizing of money laundering;

(2) **Anti-Terrorism Act, Chap: 12:07 as amended ("the ATA")** - establishes several offences about engaging in or facilitating terrorism, including raising or possessing funds for terrorist purposes, providing property or making available property to commit a terrorist act, recruiting a person to participate in the commission of a terrorist act and knowingly agreeing to provide instruction or training for the purpose of engaging in a terrorist act;

(3) **Financial Intelligence Unit of Trinidad and Tobago Act, Chap 72:01 ("the FIUA") as amended**- established the FIU and sets out its powers and functions;

(4) **Financial Intelligence Unit of Trinidad and Tobago Regulations, 2011 as amended-** subsidiary legislation to the FIUA and further details the FIU's powers and functions;

(5) **Financial Obligations Regulations, 2010 as amended ("FORs")-** made under section 56 of the POCA. The FORs contains measures and procedures which Reporting Entities must implement to enable them to detect and deter money laundering and to report suspicious transactions/activities to the FIU;

(6) **Financial Obligations (Financing of Terrorism) Regulations, 2011-** made under section 41 of the ATA. This ensures that the obligations stipulated under the FORs for money laundering apply equally to financing of terrorism;

(7) Legal Notice No. 184 of 2018, **The Economic Sanctions (Implementation of United Nations Resolutions on the Democratic People's Republic of Korea) Order, 2018-** made for the purpose of suppressing the financing of proliferation of weapons of mass destruction by providing for the implementation of targeted financial sanctions on Korea;

(8) Legal Notice No. 185 of 2018, **The Economic Sanctions (Implementation of United Nations Resolutions on the Islamic Republic of Iran) Order, 2018-** made for the purpose of suppressing the financing of proliferation of weapons of mass destruction by providing for the implementation of targeted financial sanctions on Iran. **;** and

(9) **The Non-Profit Organisations Act, 2019 Act No. 7 of 2019 ("the NPOA") -** provides for the registration of NPOs, establishment and maintenance of a register and the obligations of NPOs.

These laws are available on the FIU's website www.fiu.gov.tt

As the controller of a NPO, your main obligations under the AML/CFT/PF laws are summarized below:

(1) *Register with the Registrar Generals' Department (RGD);*
(2) *Submit Reports to the FIU;*
(3) *No "Tipping-off";*
(4) *Keep Records;*
(5) *Obtain donor/beneficiary/partner due diligence information;*
(6) *Appoint a Compliance Officer and Alternate Compliance Officer;*
(7) *Develop an effective Compliance Programme and implement its systems and controls; and*
(8) *Conduct periodic reviews by means of an internal and/or external (compliance) audits.*

1) REGISTRATION WITH THE RGD

You must register with the RGD for the purpose of identifying yourself as an NPO. The FIU is responsible for the AML/CFT/PF supervision of NPOs with a gross annual income exceeding five hundred thousand dollars.

Your application for registration under section 5(4) of the NPO Act, No. 7 of 2019 must be submitted to the RGD and must include the following:

- *a prescribe form from the RGD;*
- *copies of constituent documents of the NPO;*
- *copy of photo identification (i.e. passport, drivers' permit or national identification card) of the controller;*
- *a completed AML/CFT/PF risk assessment questionnaire;*
- *a fee prescribed by Rules; and*
- *such other information as may be prescribed by Rules.*

Offence – failure to register
A person who fails to register as an NPO under the NPO Act with the RGD commits an offence and is liable on conviction on indictment to a fine of fifty thousand dollars ($50,000) and to imprisonment for seven (7) years.

2) SUBMISSION OF REPORTS TO THE FIU

You are required to submit three (3) types of reports to the FIU:
a) reports of Suspicious Transactions or Activities (STR/SAR form);
b) reports of Terrorist Funds in your possession (TFR form); and
c) reports of Financing of Proliferation of Funds in your possession (ESR form).

The relationship between Reporting Entities and the FIU is a key one, because the FIU can only perform its analytical function to produce financial intelligence to law enforcement if the various Reporting Entities report the critical information they have.

Failing to report to the FIU knowledge or suspicion of crime proceeds or terrorist property is a criminal offence. If you continue to deal with such a transaction or funds knowing or having reasonable grounds to believe that the funds are criminal proceeds or terrorists' funds and you do not report it to the FIU then you may have committed the offence of ML/FT/PF.

Internal Reporting Procedure

Registered NPOs must establish internal reporting procedures (Regulation 8 of the FORs) which require their officers to report any information that they know or have reasonable grounds to suspect that someone is engaged in money laundering or the financing of terrorism, to their compliance officer. Officers of the NPO's must know who the compliance officer is and be aware of the procedures for reporting suspicious activity. Each registered NPO must decide for itself what those procedures will be, with their level of structure and formality determined using a risk based approach.

The compliance officer is responsible for assessing any information disclosed to determine whether it may indicate that money laundering or the financing of terrorism is being engaged in, or provides a suspicion of such activities. The internal reporting procedures must authorise the compliance officer to request any information that he requires to assist him in assessing the information disclosed. If the compliance officer determines that the information disclosed to him does indicate that money laundering or the financing of terrorism is taking place, or causes him to suspect so, the procedures must specify that he should file a report to the FIU and keep a written record of such reports.

a) Reporting Suspicious Transactions/Activities

i. You **must submit a** STR/SAR to the FIU where you know or have reasonable grounds to suspect:

- ❖ that funds being used for the purpose of a transaction are the proceeds of a crime; or
- ❖ a transaction or an attempted transaction is related to the commission or attempted commission of a money laundering offence; or
- ❖ that funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism.

The STR/SAR must be submitted as soon as possible or within fourteen (14) days of the date that the transaction was deemed to be suspicious.

Once you file a STR/SAR in good faith, you are exempted from criminal, civil or administrative liability, whether or not the underlying criminal activity was known or any illegal activity occurred.

ii. You **must submit a STR/SAR to the FIU immediately** if a listed entity* attempts to enter into a transaction or continue a business relationship. **You must not enter into or continue a business transaction or business relationship with a designated entity.**

**A designated entity means any individual or entity and their associates designated as terrorist entities by the Security Council of the United Nations, the 1267, 1989 and 2253 Committee or the 1988 Committee.*

You may access **the Security Council of the United Nations List ("the UN list") by clicking here** and **the Trinidad and Tobago Consolidated List of Court Orders** by **clicking here.**

iii. *Defining Knowledge and Suspicion*

The first criterion provides that, before you become obliged to report, you must know or have reasonable grounds for suspecting, that some other person is engaged in ML or FT.

If you actually 'know' that one of your donors, employees or beneficiaries is engaged in ML, then your situation is quite straightforward – the first criterion is met. However, knowledge can be inferred from the surrounding circumstances, so, for example, failure to ask obvious questions may be relied upon by a jury to imply knowledge.

You are also required to report if you have 'reasonable grounds' to suspect that someone is engaged in money laundering or financing of terrorism. By virtue of this second, 'objective' test, the requirement to report will apply to you if based on the facts of the particular scenario, a person of your qualifications and experience would be expected to draw the conclusion that those facts should have led to a suspicion of money laundering or financing of terrorism. The main purpose of the objective test is to ensure that NPOs are not able to argue that they failed to report because they had no conscious awareness of the activity, e.g. by having turned a blind eye to incriminating information which was available to them, or by claiming that they simply did not realise that the activity concerned amounted to money laundering or financing of terrorism.

iv. *Attempted Transactions*

You also have to pay attention to **suspicious attempted transactions**. If a member, or donor attempts to conduct a transaction, but for whatever reason that transaction is not completed, and you think that the attempted transaction is suspicious, you must report it to the FIU.

Example of suspicious attempted transaction: a donor wants you to send funds to a charity in conflict zone for him. He is vague on what are the proposed company's business activities and he presents you with $ 10,000 in cash. You ask him for identification and he delays in providing it but keeps pressing you to send the funds; you ask him for beneficial ownership identification of the company and he subsequently terminates the transaction. If you think that this transaction is related to some crime you have to report that attempted transaction to the FIU. On the other hand, a donor simply seeking your advice on how to make donations to assist in a worthy charity cause would not be sufficient for being an attempted transaction.

NOTE: It is only when you know or reasonably suspect that the funds are criminal proceeds or related to money laundering that you have to report: you do not have to know what the underlying criminal activity is or whether illegal activities actually occurred.

You must report suspicious transactions/activities **on the STR/SAR Form which you may access by clicking here. Click here** for **Guidance Note on Suspicious Transaction/Activity Reporting Standards to guide you in completing the STR/SAR form.**

v. ***How to Identify a Suspicious Transaction/Activity***

You are the one to determine whether a transaction or activity is suspicious based on your knowledge of the NPO. You are better positioned to have a sense of particular transactions which appear to lack justification or cannot be rationalized as falling within the usual parameters of legitimate business. You will need to consider factors such as; is the transaction normal for that particular donor, beneficiary or employee, or is it a transaction which is unusual.

The set of circumstances giving rise to an unusual transaction or arrangement, and which may provide reasonable grounds for concluding that it is suspicious, will depend on the person and the transaction in question. Industry specific indicators would also help you and your employees to better identify suspicious transactions whether completed or attempted.

b) Reporting Terrorist Funds/Property

i. You **must report immediately** to the FIU the existence of funds within your NPO where you know or have reasonable grounds to suspect that the funds belong to an individual or legal entity who:

- commits terrorist acts or participates in or facilitates the commission of terrorist acts or the financing of terrorism; or is a designated entity.

ii. You **must report immediately** to the FIU where you know or have reasonable grounds to believe that a person or entity named on the UN list or the list circulated by the FIU, has funds in Trinidad and Tobago.

iii. You must not enter into or continue a business transaction or business relationship with such a person or entity.

To report the existence or suspicion of terrorist funds on the **Terrorist Funds Report,** the **FIU TFR Form** may be accessed by **clicking here**.

You may access the **Security Council of the United Nations List ("the UN list")** by **clicking here and the Consolidated List of Court Orders** by **clicking here**

Click here for **Guidance Note on Procedures for Reporting Terrorist Funds** to assist you in completing the TFR form.

c) Reporting of Financing of Proliferation of Funds

i. You **must report immediately** to the FIU where you know or reasonably suspect that any entity named in an order has property your NPO and you must disclose to the FIU all information relating to the property or property of the listed entity.

ii. You **must report immediately** to the FIU where there is a transaction being conducted by a person involving property owned or controlled, whether directly or indirectly by a listed entity and you must disclose to the FIU all information of the transaction conducted.

To report the existence or suspicion of property of a listed entity the **Economic Sanctions Reporting (ESR) Form** may be accessed by **clicking here**
You may access the **Security Council of the United Nations List ("the UN list")** by **clicking here and the Consolidated List of Court Orders by clicking here.**

Consider the following Red Flags for Reporting STRs/SARs:

Donations

- Unusual or substantial one-time donations are received form unidentifiable or suspicious sources
- If a series of small donations are received from sources that cannot be identified or checked
- Where donations are made in a foreign currency or foreign sources where financial regulation or legal framework is not as rigorous
- Where payments received from a known donor but through an unknown party
- Where donations are received from unknown or anonymous bodies
- Where payments received from an unusual payment mechanism where this would not be a typical method of payment
- Where donations are conditional to be used in partnership with particular individuals or organisations where the NPO has concerns about those individuals or organisations
- If conditions attached to a donation are as such that NPO would merely be a vehicle for transferring funds from one individual or organisation to another individual or organisation
- Where a NPO is asked to provide services or benefits on favourable terms to the donor or a person nominated by the donor

Beneficiaries

- Where a NPO provides assistance, services or support on the basis of certain sum of money per beneficiary and the numbers are relatively high
- Where a NPO provides services to larger numbers or beneficiaries, where it may be easier to disguise additional beneficiaries
- Where there may appear signs that people may have been placed on distribution and aid lists by providing kickbacks and bribes to officials
- Lists of beneficiaries contain multiple manual corrections, multiple names may appear, may contain more family members
- Evidence that third parties or intermediaries have demanded payment for recommending or nominating beneficiaries

- Fake or suspicious identity documents
- Beneficiaries with identical characteristics and addresses or multiple identical or similar names and signatures

Employees

- Indications that staff may be living beyond their means or appearing at unusual times
- Staff carrying out tasks or jobs they should not be, or other unusual staff behaviour or conduct
- Sudden or increased staffing costs

Projects

- Invoices and paperwork have been tampered with, altered in crucial aspects with handwritten amendments
- Inventory shortages
- The project is vague or lacks adequate financial or technical details
- Missing key documents or only copies can be reproduced
- Lack of evidence to show fair and transparent tendering or procurement procedures
- Invoices and papers recording a higher cost for goods or services than expected or agreed
- Signatures confirming receipt or payment are missing or the invoice unsigned or undated
- Receipts have been signed and dated a long time after the good s or services should have been delivered
- Repeated excuses of system crashing, losing records or paperwork
- Discrepancies between budgeted needs and payments requested
- Requests for payments in cash to be made to an unknown third party or other organisation
- Funds are not being banked or accounted for
- Emails from new or unusual email addresses not in the partner's domain name or from someone who is not a previously agreed contact point
- Inconsistencies between narrative reports and financial claims and reports

Partners

- The structure or nature of the proposed project makes it difficult to identify the partner and verify their identity and details
- The proposal includes delegating work to other unknown partners or newly formed organisations
- Partners request unnecessary or unusual levels of privacy and secrecy
- Requests by partners to use a particular auditor or accountant
- The project involves unusual payment mechanisms, requests for cash, or for money to be paid into an account not held in the name of the partner, or in country in which the partner is not based and not where the project is being carried out

It is important to note that it is not only cash transactions may be suspicious. ML includes the layering and integrating stages where there is no more cash, but only funds that are moved around while trying to confuse the money trail. It can also be of any amount. If you know or have reasonable grounds to suspect a $1,000 transaction (donation/gift) is suspicious, you must report it to the FIU.

(3) NO TIPPING-OFF

When you have filed a STR/SAR to the FIU, you or any member of your staff must not disclose that you have made such a report or the content of such report to any person. It is an offence to inform any person, including a donor or beneficiary, that your NPO has filed a STR/SAR about his/her transactions/activities. You must also not disclose to anyone any matter which may prejudice ML/FT/PF investigation or proposed investigation. The prohibition applies to **anyone,** including persons acting, or purporting to act, on behalf of a NPO.

(4) RECORD KEEPING

Record keeping is important for use in any investigation into, or analysis of, possible ML/FT/PF. Records must be kept in a manner which allows for swift reconstruction of individual transactions and provides evidence for prosecution of money laundering and other criminal activities.

The controller of an NPO must ensure that proper financial accounts and records are kept including:

a) All sums of cash received and expended and the matters in respect of which the receipt and expenditure relate;
b) All gifts, sales and purchases of property;
c) All sums of cash raised through fundraising;
d) Non-monetary transactions of property as may be prescribed by Regulations; and
e) All assets and liabilities.

The controller must also keep the following records in electronic or written form for a period no less than six (6) years:

i. All domestic and international transaction records;
ii. Source of funds declaration, where applicable;
iii. Identification data obtained through the customer due diligence process;
iv. Copies of internal STRs/SARs submitted by staff to the Compliance Officer;
v. A register of copies of STRs/SARs filed with the FIU;
vi. A register of all enquiries (containing - date, nature of enquiry, name of officer, agency and powers being exercised) made by law enforcement authorities;
vii. The names, addresses, position titles and other official information pertaining to your staff;
viii. All wire transfer records (originator and recipient's identification data);
ix. Account files and business correspondence; and
x. The results and any analysis undertaken related to a donor, beneficiary or transaction.

(5) OBTAIN DUE DILIGENCE INFORMATION

A NPO as a Listed Business must comply with the requirements under the FORs to conduct customer due diligence where it engages in a financial/donor transaction. The NPO must obtain relevant identification documentation which can include a valid passport, national identification card or driver's licence to verify the identity of a donor or beneficiary.

The Risk Based Approach

NPOs are defined by their purpose, their reliance on contributions from donors and the trust placed in them by the wider community. Not all NPOs are inherently high risk organisations, and it is desirable to identify the high risk NPOs, i.e. NPOs which by virtue of their activities, characteristics, asset size, international and geographical activities are likely to be at risk for terrorist financing abuse, for the purpose of proper risk management.

High Risk NPOs

NPOs that are assessed as high risk are subject to AML/CFT/PF compliance examinations by the FIU pursuant to section 18F of the FIUA, which empowers the FIU to monitor and supervise as well as, conduct onsite AML/CFT/PF examinations of NPOs. NPOs that are selected for compliance examinations on a risk based assessment will be notified in advance of the examination and provided with a list of items that the FIU officers will be seeking to verify. The main purpose of the compliance examination is to test the effectiveness of AML/CTF/PF systems and controls implemented by the NPO. Feedback is provided verbally and in writing which states the findings of the examination and provides recommendations for rectification of any deficiencies identified.

All NPOs must have, as a minimum:

- some form of appropriate internal and financial controls in place to ensure that all their funds are fully accounted for and are spent in a manner that is consistent with the purpose of the charity. What those controls and measures are and what is appropriate will depend on the risks and the NPO
- proper and adequate financial records for both the receipt and use of all funds together with audit trails of decisions made. Records of both domestic and international transactions must be sufficiently detailed to verify that funds have been spent properly as intended and in a manner consistent with the purpose and objectives of the organisation
- given careful consideration to what due diligence, monitoring and verification of use of funds they need to carry out to meet their legal duties
- taken reasonable and appropriate steps to know who their beneficiaries are, at least in broad terms, carried out appropriate checks where the risks are high and have clear beneficiary selection criteria which are consistently applied.

Know Your Donors:

- Before receiving funds from a donor, NPOs must establish that the donor is not placed on the United Nations' list of persons who are linked to terrorist financing or against whom a ban, sanction or embargo subsists.
- NPOs shall undertake best efforts to document the identity of their significant donors. NPO must collect and maintain record or correct and complete identification particulars of major donors.
- NPOs shall conduct, on a risk-based approach, a reasonable search of public information, including information available on the Internet, to determine whether the donor or their key employees, board members or other senior managerial staff are suspected of being involved in activities relating to terrorism, including terrorist financing.

Know Your Beneficiaries and Partners:

- NPO must ascertain correct and complete identification particulars of each of its beneficiary (person, group of persons or organisation etc.) who receives cash or services or in-kind contributions.
- In case the beneficiary is an organization/ group of persons, the donor NPO must have knowledge of detailed profile and particulars of such organisation. NPO shall ensure that its beneficiaries are not linked with any suspected terrorism activity or any link with terrorist support networks.
- In case where the projects are implemented through partnership agreements with other partners, the NPO shall make it a part of its project agreements that partners shall maintain and share beneficiaries' information.
- NPOs must ensure that the partner organisations shall not be from any such organisation whose license has been revoked or registration cancelled by other authorities.

Know your Employees:

NPO must maintain records of particulars of its employees (both Trinidad and Tobago nationals or foreign nationals), including but not limited to permanent address, present address, copy of National ID Card, passport number, nationality, personal email ID, phone or mobile number, past experience, etc.

See Appendix II for Illustrative Characteristics of Higher Risk NPOs.

(6) APPOINT A COMPLIANCE OFFICER AND ALTERNATE COMPLIANCE OFFICER

The NPO must appoint a designated Compliance Officer ("CO") and an alternate CO ("ACO") for the NPO who must be either a controller, senior officer or other competent professional as. The individuals you appoint must be approved in writing by the FIU and will be responsible for the implementation of your compliance regime. The ACO must discharge the functions of the CO in his absence.

Where an external party (competent professional) is the designated CO or ACO the responsibility for compliance obligations will be that of the NPO.

If you wish to change your CO or ACO you must submit the required application to the FIU immediately and get the FIU's approval for the new CO and ACO.

If you are a small NPO, employing five (5) persons or less, the CO must be the person in the most senior position. If you are the owner and do not employ anyone, you can appoint yourself as CO to implement a compliance regime.

In the case of a large NPO (employing over five (5) persons), the CO should be from senior management and have direct access to senior management. Further, as a good governance practice, the appointed CO in a large NPO should not be directly involved in the receipt, transfer or payment of funds.

Your CO should have the authority and the resources necessary to discharge his or her responsibilities effectively. The CO's responsibilities include:

i. Having full responsibility for overseeing, developing, directing, updating and enforcing the AML/CFT/PF Programme;
ii. Being competent and knowledgeable regarding ML/FT/PF issues and risks and the AML/CTF/PF legal framework;
iii. Submitting STRs/SARs, TFRs and ESR to the FIU and keeping relevant records;
iv. Acting as Liaison officer between your NPO and the FIU;
v. Ensuring the training of employees, volunteers and directors on AML/CFT/PF obligations; and
vi. Ensuring independent audits of your Compliance Programme are conducted.

Depending on your type of NPO, your CO should report, on a regular basis, to senior management, or to the owner or chief operator of the organisation. The identities of the CO and ACO must be treated with the strictest confidence by you and your employees.

For consistency and on-going attention to the compliance regime, your appointed CO may choose to delegate certain duties to other employees. For example, the CO may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented at that location. However, where such a delegation is made, the CO retains full responsibility for the implementation of the compliance regime.

Click here for **Guidance Note on the Appointment and Approval of the Compliance Officer and Alternate Compliance Officer of a Supervised Entity.**

(7) DEVELOP A WRITTEN COMPLIANCE PROGRAMME

After you have registered with the Registrar General as an NPO, you must develop a written Compliance Programme ("CP"). The CP has to be approved by senior management.
Click here for a CP Check list.

The CP is a written document which include a risk assessment of your particular NPO and which sets out your system of internal procedures, systems and controls which are intended to mitigate the vulnerabilities and inherent risks identified by you which can be exploited by money launderers and terrorism financiers. Your CP will contain measures that ensure that you comply with your reporting, record keeping, customer due diligence, employee training, and other AML/CFT/PF obligations. These policies, procedures and controls, must be communicated to all your members, and when fully implemented, will help reduce the risk of your organisation being used for ML/FT/PF. The CP must be reviewed every two (2) years.

A well-designed, applied and monitored CP will provide a solid foundation for compliance with the AML/CFT/PF laws. As not all individuals and entities operate under the same circumstances, your compliance procedures will have to be tailored to fit your individual needs. It should reflect the

nature, size and complexity of your operations as well as the vulnerability of your business to ML/FT/PF activities.

The following five (5) elements must be included in your compliance regime:

a) The appointment of a staff member as CO and ACO and his/her responsibilities;
b) Internal compliance policies and procedures such as reporting suspicious transactions/activities to the CO; the implementation of CDD, EDD and record keeping;
c) Your assessment of your risks to ML/FT/PF, and measures to mitigate high risks;
d) Ongoing compliance training for all members at the level appropriate for their job duties; and
e) Periodic documented review of the effectiveness of implementation of your policies and procedures, training and risk assessment.

Click here to access the **Guide to Structuring an AML/CFT/PF Compliance Programme.**

(8) IMPLEMENT AND TEST YOUR COMPLIANCE PROGRAMME

Your obligations include implementing your written CP. The FIU may conduct an onsite examination to determine whether the measures outlined in your CP are effectively implemented.

All employees involved in the day-to-day business of a NPO should be made aware of the policies and procedures in place in the organisation to prevent ML/FT/PF risks. You must conduct internal testing to evaluate compliance by your staff with your CP, in particular, CDD, record keeping and suspicious transactions reporting. Best practice indicates that internal testing should be carried out by someone other than the CO, to avoid potential conflict since the CO is responsible for implementation of the CP, its measures and controls.

External testing must also be carried out to test the effectiveness of your systems, controls and implementation of same by someone not employed in your organisation.

If you are the CO as well as the most senior employee, an external independent review will satisfy compliance with your obligation to test your implementation of your AML/CFT/PF obligations.

Such reviews (both internal and external) must be documented and made available to the FIU.

PART J

OFFENCES & PENALTIES FOR NON-COMPLIANCE

Non-compliance with your obligations under the AML/CFT/PF laws and regulations may result in criminal and or administrative sanctions.

Criminal penalties include fines and terms of imprisonment and civil and administrative penalties include the issuance of directives and court orders to compel compliance.

Click here to access a summary of the Offences and Penalties under AML/CFT laws and regulations of Trinidad and Tobago.

PART K

ADDITIONAL RESOURCES

This summary is intended to guide you in fulfilling your legal obligations under the AML/CFT/PF laws.

Additional reference materials include:

- The AML/CFT/PF laws available on the FIU's website, www.fiu.gov.tt under **"Legal Framework".**
- The FATF recommendations at www.fatf-gafi.org/recommendations.
- FATF Report 2014: Risk of Terrorist Abuse of Non Profit Organisations - http://www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html

Dated this 30th July, 2019

Nigel Stoddard
Director (Ag.)
Financial Intelligence Unit

APPENDIX I

CASE STUDIES[4]

1. The following case involves an NPO directing official taking cash donations intended for the NPO and depositing them into an unrelated company account. From there, the funds were believed to be transferred to a foreign terrorist organisation.

Diversion of Funds by Actors Internal to NPOs

Collection Phase

A domestic 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. The funds were immediately transferred to foreign-based companies.

An investigation by the national FIU 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 on 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 domestic company was a front company being used as a conduit to transfer funds on behalf of the NPO linked to a foreign terrorist group.

2. In another case, NPO officials willingly worked with foreign organisations in controlled areas that were suspected of supporting terrorism in order to gain access and provide humanitarian assistance.

Diversion of Funds by Actors Internal to NPOs

Transfer Phase

A domestic NPO was established to provide a place of religious worship for a diaspora community that had come from an area of conflict, and to raise and disburse funds for humanitarian causes.

The national NPO regulator became suspicious when the NPO's mandatory reporting indicated that it had sent funds to organisations that were not legally prescribed beneficiaries. These funds were sent ostensibly in response to a natural disaster that had affected the diaspora community's homeland. One of the beneficiary organisations, however, was believed to be the domestic branch of an international front organisation for a foreign terrorist group operating in the diaspora community's homeland.

The regulator audited the NPO and discovered that it had sent funds to five organisations or individuals that were not legally prescribed beneficiaries. This included USD 50 000 sent to the international front organisation through the domestic branch, and USD 80 000 sent directly to the front organisation's headquarters branch located in the area of conflict.

While the audit was ongoing, the regulator received two leads from the public regarding the NPO. Both leads cited concerns regarding the opacity of the NPO's leadership, and that decisions to send funds overseas had circumvented normal accountability procedures set out in the NPO's governing documents. One of the leads indicated that a shift in the demographic of the diaspora community had meant a new faction had gained control of the NPO's board of directors. This faction was more sympathetic to the

[4] http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf

cause of the foreign terrorist organisation. While these issues had already been noted through the regulator's audit, the leads supported the regulator's concerns regarding the NPO's management.
The NPO leadership replied to the regulator's concerns by stating that the urgent need to respond to a natural disaster had led the NPO to bypass some internal procedures and to work with whichever organisations could operate in the affected areas. Taking this into consideration, the NPO retained its registration but was forced to pay penalties. The NPO also entered into a compliance agreement with the regulator that would enforce strict due diligence and accountability standards.

3. In another case of diversion of funds involving external actors, the transferred funds meant for humanitarian relief were systematically passed on to persons or organisations which were part of, or affiliated with, a known terrorist organisation.

Diversion of Funds by Actors External to NPOs
Transfer Phase
A domestic NPO was established to support charitable work in foreign areas of conflict.
An investigation by the national FIU, 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 domestic NPO and the terrorist organisation could not be substantiated.

4. An NPO was established to advance religion and education, both charitable purposes in the jurisdiction in which it operated. However, this activity was manipulated by advancing philosophies designed to promote recruitment to a terrorist organisation.

Abuse of Programming
Delivery of Programmes Phase
An NPO was carrying out religious and educational activities domestically, with no foreign activities. Information provided by the national FIU 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. It was subsequently revealed that a former student of the NPO's school had been charged in another country with terrorism offences. The student had also met with several other individuals who were later convicted of terrorism offences.
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.

5. In the case study detailed below, two individuals were observed falsely representing themselves as members of a well-known NPO in order to raise funds to support a militant fighting abroad.

False Representation

Collection Phase

Two individuals were raising funds domestically for a family member who was fighting alongside a listed terrorist organisation abroad. The individuals, claiming to be representatives of a well-known domestic humanitarian aid NPO, were raising the funds by way of public street collections. The collection efforts were in breach of the domestic law.

The individuals in question did not have the consent of the domestic NPO to solicit donations on its behalf nor did they deliver to funds raised to the NPO. Once a sizeable amount of money had been collected, it was sent to the family member abroad using wire transfers.

As a result of a joint investigation between the FIU, NPO regulator, and law enforcement authorities, the two individuals were arrested and convicted of terrorist fundraising and sentenced to jail.

APPENDIX II

Illustrative Characteristics of Higher Risk NPOs

No.	Risk Parameter	Risk characteristics
1	Zone	Operating in conflict ridden and/or border zones including, but not limited to tribal agencies/ merged areas, sensitive areas of any province, and areas/regions which have experienced terrorist attacks. However, this does not preclude the possibility of soliciting financial support by the terrorists from other areas.
2	Activity	Primarily working in service activities including: • Social services or social welfare • Housing • Health • Education
3	Legal status/level of formality	• Unincorporated NPOs (High likelihood, low consequence) • Incorporated/registered NPOs meeting criteria 1 and 2 (Low likelihood, high consequence)
4	Revenue/Quantum of donations	Large size NPOs with annual grants/income/subsidies/donations of $500,000 and above
5	Funding Source	• Foreign funding from unknown sources • Foreign funding from high-risk countries or those characterized by lower AML/CFT/PF compliance • Major collection in the form of public/street donations, donation boxes, from anonymous donors, etc.
6	Geo-political factors	Having nationals from unfriendly countries as sponsors or volunteers of NPOs
7	Legal Compliance	• Serious non-compliance by registered NPOs • Involvement of sponsors/directors/officers of NPOs in unlawful activities through other companies or business entities
8	Financial misconduct by NPOs or sponsors/ directors	• Violation of licensing conditions by licensed NPOs • Failure to observe accounting and auditing principles in the recognition, measurement and disclosure through financial statements • Serving as conduit in respect of illicit financial transactions

Source: Compliance toolkit: Protecting Charities from Harm, Charity Commission, UK

****