COMBATING TERRORIST FINANCING GUIDELINE

For

CHARITIES

AND

NON-PROFIT ORGANIZATIONS

Anti-Money Laundering Authority
December, 2019

CFT Guideline for Charities and Non-Profit Organizations

TABLE OF CONTENTS

AML/CFT Guideline for Charities and NPOs

ANTI-MONEY LAUNDERING/COMBATING TERRORIST FINANCING

Terms Used In This Guideline

AMLA	Anti-Money laundering authority
AML/CFT	Anti-Money laundering and counter financing of terrorism
CDD	Customer Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
MLFTA	Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23
NRA	National Risk Assessment
PEP	Politically Exposed Person
RBA	Risk Based Approach

1.0 INTRODUCTION

1.1 Background

1. The global threats of money laundering, and the financing of terrorism and proliferation of weapons of mass destruction have led countries to strengthen their vigilance to counter these threats and to minimize the possibility of their jurisdictions or institutions becoming involved. Effective enforcement of policies to deter money laundering, and the financing of terrorism and proliferation of weapons of mass destruction, should, inter alia, enhance the integrity of the financial system and reduce incentives for the commission of crime within the jurisdiction.

2. Experience and careful study have taught that the threats of money laundering and the financing of terrorism extend beyond the traditional financial entities which have been receiving attention for control of these activities. It is therefore necessary for non-financial entities, including charities and non-profit organizations to be adequately regulated so as to keep them safe from these nefarious activities, and to protect the legitimate financial system from illegitimately acquired funds that could find their way into the financial system via non-financial entities.

3. The Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23 (MLFTA) empowers the Anti-Money Laundering Authority (AMLA), pursuant to section 26, to issue guidelines with respect to money laundering and terrorist financing activities. This Guideline is so issued for the guidance of persons and entities operating as registered charities and non-profit organizations (NPOs) in Barbados.

1.2 Purpose of Guideline

4. The purpose of this Guideline is to assist registered charities and NPOs in complying with their legal duties and responsibilities as they relate to combatting the financing of terrorism as set out in the Money Laundering and Financing of Terrorism Act 2011-23, the Charities Act Cap 243, the Companies Act Cap 308 and other relevant legislation. It is also designed to help trustees and managers better understand their responsibilities and the approaches to be taken for their respective charity and NPO in order to comply with Recommendation 8 of the Financial Action Task Force (FATF) which states –

    - *Countries should review the adequacy of laws and regulations that relate to non-profit organizations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk-based approach, to such non-profit organizations to protect them from terrorist financing abuse, including:*

        (a) by terrorist organizations posing as legitimate entities;

        (b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and

        (c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.

    This guideline should also be read in conjunction with the above laws.

5. A summary of money laundering and terrorism financing sanctions and offences, including non-compliance with this guideline are found at **Appendix 1**.

2.0 APPLICATION

6. This Guideline applies to all charities registered under the Charities Act Cap 243 and Non Profit Companies incorporated under the Companies Act Cap 308, except those exempted by the Registrar.

3.0 FINANCING OF TERRORISM AND PROLIFERATION

3.1 Financing of Terrorism

7. Terrorism is the act of seeking for political, religious or ideological reasons to intimidate or compel others to act in a specified manner. A successful terrorist group, much like a criminal organization, is generally able to obtain sources of funding and develop means of

obscuring the links between those sources and the uses of the funds. While the sums needed are not always large and the associated transactions are not necessarily complex, terrorists need to ensure that funds are available to purchase the goods or services needed to commit terrorist acts. In some cases, persons accused of terrorism may commit crimes to finance their activities and hence transactions related to terrorist financing may resemble money laundering.

8. It is worth emphasizing that while money laundering is concerned with funds generated from unlawful sources, funds used for terrorist activities are often legitimate in nature. The source of funds is, therefore, not the sole consideration for agents. The conversion of assets into money and the subsequent direction of that money must be observed.

9. As information changes, the United Nations publish lists of terrorist or terrorist organizations. Financial institutions and designated non-financial businesses and professionals are required to remain abreast of this information and check their databases against these lists. Should any person or entity on the lists be clients, that information should be immediately communicated to the FIU and the Commissioner of Police.

10. The FATF Recommendations place obligations on countries as they relate to terrorist financing in the context of national cooperation and coordination, confiscation and provisional measures and targeted financial sanctions related to terrorism and terrorist financing. The latter is applicable to all United Nations Security Council resolutions (UNSCRs) applying targeted financial sanctions relating to the financing of terrorism. The AMLA's role is to safeguard against access to financing by individuals and entities who may be involved in or supporting terrorism.

3.2 Financing of Proliferation

11. The FATF defines proliferation financing as "*the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, 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 goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.*[1]". Proliferation of weapons of mass destruction can take many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long range missiles).The AMLA's role is to safeguard against access to financing by individuals and entities who may be involved in or supporting such proliferation.

[1] http://www.fatfgafi.org/topics/methodsandtrends/documents/typologiesreportonproliferationfinancing.html

4.0 INTERNATIONAL INITIATIVES

12. The **FATF Forty Recommendations** were revised in February 2012, and renamed the **International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations**. The Recommendations were since updated in February 2013 (Mutual Legal Assistance and other forms of International Cooperation); October 2015 (Interpretative Note on Foreign Terrorist Fighters); June 2016 (Note on Non-profit Organizations); October 2016 (Interpretative Note on Terrorist Financing Offence); June 2017 (Interpretive Note on Targeted Financial Sanctions related to proliferation); November 2017 (on Tipping-off and Confidentiality and Interpretive Note on internal controls and foreign branches and subsidiaries); February 2018 (on National Cooperation and Coordination); and October 2018 (on New Technologies). The FATF normally issues Guidance and Best Practices Papers to assist countries in implementing the Recommendations. Registered charities and NPOs should keep abreast of developments in the international standards and refine their programmes accordingly.

5.0 LEGISLATIVE AND REGULATORY FRAMEWORK

13. The Government of Barbados has enacted several pieces of legislation aimed at preventing and detecting drug trafficking, money laundering, terrorist financing and other serious crimes. The Acts which are most relevant for the purpose of this guideline are as follows:

    (i) Drug Abuse (Prevention and Control) Act, Cap. 131;
    (ii) Proceeds and Instrumentalities of Crime Act, 2019;
    (iii) Mutual Assistance in Criminal Matters Act, Cap. 140A;
    (iv) Anti-Terrorism Act, 2002-6;
    (v) Anti-Terrorism (Amendment) Act, 2015;
    (vi) Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23;
    (vii) Money Laundering and Financing of Terrorism (Prevention and Control) (Amendment) Act, 2019;
    (viii) Transnational Organised Crime (Prevention and control) Act, 201-3; and
    (ix) Criminal Assets Recovery Fund Act, 2016.

14. The MLFTA confers responsibility for its supervisory functions to the Anti-Money Laundering Authority (AMLA), which was established in August 2000. The office of the AMLA comprises a Compliance Unit (CU) which is responsible for carrying out AMLA's supervisory functions, including compliance and inspection.

15. The office of AMLA also comprises the Financial Intelligence Unit whose responsibilities, inter alia, include:
    (i) Receiving reports from supervised entities including large transaction reports and suspicious or unusual transactions reports;

(ii) Conducting inspections of regulated entities for AML/CFT compliance
(iii)Investigating suspicious or unusual transactions reports; and
(iv)Providing training in respect of record keeping obligations and reporting obligations under the MLFTA.

16. Where a charity or NPO is uncertain about how to treat an unusual or suspicious transaction or any other requirement of the MLTFA, its representatives are strongly urged to speak directly to the AMLA for guidance.

6.0 RISK-BASED APPROACH

17. Most charities and NPOs have good relations with their donors, partner organizations and beneficiaries who give to or work with the organization in good faith. However, practical risks do exist and such entities can be abused for terrorist financing purposes. The nature of the risk in the particular circumstances, the activities that the charity or NPO carry out, and how and where the activities are undertaken, are all reasons why it is important for charities and NPOs to understand the risks they face and take appropriate measures to mitigate these risks.

18. The MLFTA provides for the application of a risk-based approach to combating money laundering and the financing of terrorism and proliferation. The RBA to AML/CFT means that countries, competent authorities and supervised entities, including registered charities and NPOs, should identify, assess and understand the ML/TF risks to which they are exposed and take the required AML/CFT measures effectively and efficiently, to mitigate and manage the risks.

19. Key elements of a RBA can be summarised as follows:

(i) **Risk Identification and Assessment** - *identifying ML/TF risks facing a firm, given its customers, services, countries of operation, also having regard to publicly available information regarding ML/TF risks and typologies*

(ii) **Risk Management and Mitigation** - *identifying and applying measures to effectively and efficiently mitigate and manage ML/TF risks*

(iii) **Ongoing Monitoring** -*putting in place policies, procedures and information systems to monitor changes to ML/TF risks*

(iv) **Documentation** - *documenting risk assessments, strategies, policies and procedures to monitor, manage and mitigate ML/TF risks*

20. The general principle of a RBA is that, where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive measures and controls conducted should be stronger in higher risk scenarios. However, where the ML/TF risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter.

21. Charities and NPOs should also observe higher/lower risks identified in risk assessments undertaken by the Competent Authority and the National Risk Assessment and take appropriate enhanced or simplified measures.

6.1 Risk Criteria

22. Criteria used for assessing charities' and NPOs' and determining their risk profiles include:

- **Size** – whether the entity's asset size or income level represents a significant proportion of the total for the charitable or NPO sector

- **International activities**–
  - Whether the charity or NPO has foreign sources of funding
  - Whether the charity or NPO has foreign beneficiaries
  - Whether the charity or NPO has an overseas branch or is itself a branch of an overseas organization

- **Geographical and other exposures**–
  - Whether the charity or NPO operates in, or has links to, areas known to have terrorist activity
  - Whether the charity or NPO has potential exposure to abuse by extremist groups

6.2 Mitigating Risk

23. The best approach for charities and NPOs to ensure that they are not abused for terrorist purposes is to put in place good governance and strong financial management, including having robust internal and financial controls and risk management procedures. In addition, carrying out proper due diligence on those individuals and organizations that give money to, receive money from or work closely with the charity or NPO, is also important. Proper due diligence is dependent upon the circumstances and context of each organization and the environment in which it operates.

24. Charities and NPOs should implement appropriate measures and controls to mitigate the potential ML/TF risks especially those determined to be of higher risk. These measures should be tailored to the identified risks, to ensure that the risks are adequately addressed and to assist in the appropriate allocation of the resources of the entity.

25. For those charities and NPOs deemed at higher risk of TF abuse, the risk mitigation measures that each individual entity should implement depend on a range of factors, including various aspects of its work and the associated risks, existing due diligence and risk mitigation measures, whether the entity works with partners and whether those partners operate in a close proximity to an active terrorist threat.

26. At a minimum charities and NPOs should have –
    - Adequate records of the receipt and use of funds and of the decisions made regarding the operations of the charity or NPO.
    - Adequate financial and internal controls to ensure that funds are properly accounted for and are spent in a manner that is consistent with the objects of the charity or NPO.
    - Adequate due diligence, monitoring and use of funds procedures in place for undertaking their legal responsibilities
    - Taken reasonable and appropriate steps and carried out the necessary steps to identify who are the beneficiaries, especially where the risk is considered high.

7.0 DUE DILIGENCE REQUIREMENTS - "KNOW YOUR"PRINCIPLES

27. Due diligence is the range of practical steps that need to be taken by charities and NPOs so that they are reasonably assured of the provenance of the funds given to the NPO; confident that they know the people and organizations the charity or NPO works with; and able to identify and manage associated risks. Entities may also undertake their own internal risk analysis to help better understand the risks they face in their operations and design appropriate risk mitigation and due diligence measures.

28. In order to ensure that they are fulfilling their duty to manage the funds of a charity or NPO properly, trustees or managers need to know where the funds originated, whether they are to be applied in accordance with the entity's objects and who will be involved in delivering the charitable services.

29. The voluntary nature of charities and NPOs and their areas of work can make them vulnerable to people who want to misuse the entities for their own gain. They are highly valued in society and their very nature can make them attractive targets for criminal abuse such as fraud, theft and money laundering. People also abuse charities and NPOs for private advantage, for example by ensuring the entity uses a particular organization or individual to provide services which are not necessarily charged on the best terms available.

30. To satisfy the core elements of due diligence, trustees and managers must take reasonable steps to ensure they:

    a) **Identify** –know who you are dealing with

    b) **Verify** – where reasonable, and the risks are high, verify identities

    c) **Know what the organisation's or individual's business is** and can be assured this is appropriate for the charity to be involved with

    d) **Know what their specific business is with your charity** and have confidence they will deliver what you want them to and

31. The "Know Your" principles are key to the legal duties and responsibilities of trustees and managers of charities and NPOs. These requirements are not new. Similar duties and principles exist in other sectors. In the financial sector, for example, banks and other institutions have to take reasonable steps to ensure that they know their customers. For charities and NPOs, the requirements can be summed up in the following three 'know your' principles:

    - Know Your Donor
    - Know Your Beneficiaries
    - Know Your Partner

7.1 Know Your Donor

32. Most charities and NPOs should know, at least in broad terms, the source of the money they are being given (e.g. grants, cash donations etc.).Trustees and managers should take reasonable and appropriate steps to know who the donors are, particularly where significant sums are being donated or the circumstances of the donation give rise to notable risk. Good due diligence will help to:
    a) assess any risks to the charity or NPO that may arise from accepting a donation or certain types of donations
    b) ensure that it is appropriate for the charity or NPO to accept money from the particular donor, whether that is an individual or organization
    c) give trustees and managers reasonable assurance that the donation is not from any illegal or inappropriate source
    d) ensure that any conditions that may be attached are appropriate and can be accepted.

33. Trustees and managers need to implement effective processes to identify and verify donors, particularly substantial donors. They should also have assurance on the source of donor funds and any conditions attached to them (**i.e. know what the donor's specific business is with your charity).** This does not mean charities and NPOs have to question every donation nor must they know lots of personal and other details about every donor.

7.2 Know Your Beneficiaries

34. The identification and selection of beneficiaries are important decisions. Sometimes this is specified in the entity's governing document, making it a legal requirement. In other cases trustees and managers may have more discretion about selection criteria. They may have decided on a policy to guide their decision making.

35. Charities and NPOs use a variety of ways to reach those they aim to assist through their own charitable activities, providing funding for others, and coordinating efforts to provide assistance. They may use their own staff and resources, or may work in collaboration and partnership with other organizations, including governments. Because of their contact with, knowledge of, and reach into local communities, charities and NPOs are often uniquely placed to accurately identify the targeted beneficiaries of aid, assistance or other

services.

36. Some charities and NPO activities are available to and open to everyone, and the "Know Your Beneficiaries" principle will not have specific application. For example, a charity or NPO may provide a recreation ground. The charity or NPO does not choose its beneficiaries as such and clearly, there is no need to check and verify the identity of members of the public who walk across or use the ground. Some charities or NPOs will not have individually identifiable beneficiaries, for example, an entity carrying out environmental work for the benefit of the public in a particular. So again, the "Know Your Beneficiaries" principle will not have specific application.

37. Therefore as charities and NPOs carry out their activities and delivery of services in pursuit of their charitable purposes, a common sense approach needs to be exercised, when applying the "Know Your Beneficiaries" principle.

38. A charity and NPO should be wary of doing business with persons from countries where, for example, it is believed that there is a high level of drug trafficking or corruption and greater care may be needed in establishing and maintaining the relationship or accepting documentation from such countries. The charity or NPO should observe the "Improving Global AML/CFT Compliance: Ongoing Process Statements" and "Public Statements" issued by the FATF and CFATF as it relates to business relationships and transactions with natural and legal persons, and financial institutions from listed countries. Refer to the FATF: High Risk & Other Monitored Jurisdictions and any lists of high-risk jurisdictions provided by the Competent Authority from time to time.

In addition to the above, the Competent Authority may require countermeasures, which are effective and proportionate, to the risks identified from listed countries, either when called up onto do so by the FATF and CFATF or independently of any call to do so.

7.3 Know Your Partner

39. Due diligence of partners is important, as the responsibility of trustees' and managers is not only to ensure that funds actually reach the place, people and purpose intended. Their responsibilities also include determining whether a partner is appropriate and suitable for their organization to work with. For example, a charity or NPO should not accept funding from or provide support to a partner organization that exposes beneficiaries to activities which directly, or indirectly, promote money laundering or terrorism. This is so even if the charity's funding or support were used for legitimate humanitarian aid or other charitable activities.

40. To prevent the abuse of funds by partners, charities and NPOs should therefore carry out appropriate due diligence on those individuals and organisations that the charity or NPO receives donations from, gives money to or works with closely, before entering into relationships or agreements. Charities and NPOs should verify partner reputations through the use of selection criteria and searches of publicly available information, including domestic and UN sanctions lists.

41. The more significant or substantial the charitable activity or partnership, the greater the need for enhanced due diligence by trustees and managers. Steps should be taken to verify the identity of the partner and to further assess the risks. This may involve checking the legal status of the partner – is it registered as a company and who owns it, for example, and is it appropriately registered with another charity regulator. Due diligence is also an opportunity for the charity or NPO to check that the partner has the operational capacity and capability to do what is required and that the partner fully understands the aims and parameters of the activity. Due diligence will usually involve judging the quality and completeness of the initial information obtained and then deciding whether further checks or enquiries are necessary.

42. Charities and NPOs should have written agreements with their partner organizations. A written agreement or understanding should be drafted and signed by the participants. This should include the funding organization and the end user, whether it is an individual or an organization. Such an agreement should outline what the funds are to be used for and how the user will report back for accountability purposes. The agreement should also include requirements regarding the management of local employees according to defined ethical standards.

43. Trustees and managers should also ensure that they are able to act independently from their partners and to be able to hold partners accountable for how funds are spent and how projects are managed. If a partner is able to exert considerable influence over the charity or NPO, such as when organizations share key directors or officers, this may create conflicts of interest and prevent the entity from complying with anti-money laundering and anti-terrorist financing requirements.

7.5 Assessing how many Due Diligence enquiries need to be carried out

44. The nature and extent of due diligence checks should be proportionate to the risks involved or when entering into any new relationship. These include the scale of the funding involved and any identified risks in the area where the donor or beneficiary is operating. Where the risks are higher, more in-depth checks will be appropriate. If the partner is from a jurisdiction about which concerns have been raised, the trustees and managers should take more steps to ensure that working with the partner is appropriate.

45. Effective due diligence will help trustees and managers identify potential risks so that they can put in place appropriate and proportionate safeguards. The effectiveness of the safeguards can then be monitored and any necessary adjustments made. Risk of abuse may be greater where:
    a) the project proposal is vague or lacks adequate financial or technical details

    b) the structure or nature of the proposed project makes it difficult to identify the donor or beneficiary and verify their identity and details

c) the proposals include delegating work to other unknown persons or newly formed organisations

d) it is difficult to contact the donor or beneficiary at their main address, or their telephone numbers are not working, or the person always insists upon contacting the charity or NPO and not the other way round

e) the project involves unusual payment mechanisms, or requests for cash, or for money to be paid into an account not held in the name of the partner, or in a country in which the partner is not based and not where the project is being carried out

f) the partner may be, or may have involvement with, politically exposed persons (PEPs)

g) partners request unnecessary or unusual levels of privacy and secrecy

h) the partner cannot demonstrate much previous project delivery and it is difficult to get independent references to vouch for it

46. Trustees and managers may also want to consider publicizing or making clear that due diligence checks will be carried out on donors, beneficiaries and other partners. This may act as a deterrent against those who may wish to abuse charities and NPOs. Some entities may wish to consider going as far as making it clear that information may be shared with the police and other competent authorities for the purpose of detecting and preventing abuse and criminal activity.

47. Trustees and managers should keep written records of due diligence processes and the results which informed their decision making. This should include the checks carried out and the results and conclusions of their assessment of donors, beneficiaries and partners. Trustees and managers should document the risks identified from their assessments together with the actions they consider necessary to properly manage the risks arising from entering into any arrangement.

48. Annex 2 of the *FATF Best Practices Paper on Combatting the Abuse of Non-Profit Organizations*[2] gives examples of measures that have been implemented by some NPOs and which may, depending on the circumstances, help to mitigate TF risk. In practice, the unique circumstances and context of each case will determine whether a particular measure is a good practice that is partially or fully mitigating the specific risk involved. The types of circumstances and context which are relevant to such a determination include: the level and type of TF risk, the type of charitable funds or assets being distributed, the geographical context, and other controls and due diligence measures in place.

[2] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-combating-abuse-npo.html

7.6 Politically Exposed Persons (PEPs)

49. Concerns about the abuse of power by public officials for their own enrichment and the associated reputation and legal risks which charities and NPOs who deal with them may face have led to calls for enhanced due diligence on such persons. The FATF categorizes PEPs as foreign, domestic, or a person who is or has been entrusted with the prominent function by an international organization. These categories of PEPS are defined as follows:

    - Foreign PEPs: individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

    - Domestic PEPs: individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

    - International organization PEPs: persons who are or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions.

    - Family members are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.

    - Close associates are individuals who are closely connected to a PEP, either socially or professionally.

8.0 RECORD-KEEPING

50. Charities and NPOs should establish internal controls and monitoring systems to ensure that funds and services are being used as intended. For example, charities and NPOs should clearly define and document the purpose and scope of their activities, identify beneficiary groups, and consider the risks of terrorist financing and risk mitigation measures before undertaking projects. They should maintain detailed budgets for each project and generate regular reports on related purchases and expenses. Charities and NPOs should establish procedures to trace funds, services, and equipment, and carry out transactions through the financial system when possible, to maintain transparency of funds and mitigate the risk of terrorist financing. Project performance should be monitored on a regular basis by verifying the existence of beneficiaries and ensuring the receipt of funds. Charities and NPOs should take appropriate measures, based on the risks, to account for funds and services delivered.

51. To demonstrate compliance with the MLFTA and to allow for timely access to records by the FIU, charities and NPOs should establish a document retention policy that provides for the maintenance of a broad spectrum of records, including donor and beneficiary identification data, business transaction records, internal and external reporting and training records, as well as any analysis done. Business transaction records should be maintained for a minimum of five years in accordance with section 18 of the MLFTA. However, it may be necessary to retain records, until such time as advised by the FIU or High Court, for a period exceeding the date of termination of the last business transaction where:

    a) There has been a report of a suspicious activity; or
    b) There is an on-going investigation relating to a donor or beneficiary.

52. The nature of records that should be retained is set out at Section 2 of the MLFTA, which defines a business arrangement, business transaction and business transaction record.

8.1 Internal and External Records

53. Charities and NPOs should maintain records related to unusual and suspicious business transactions for no less than 5 years. These should include:

    i) The internal written findings of transactions investigated. This applies irrespective of whether a suspicious report was made and includes all reports made by staff to the Compliance Officer;
    ii) Consideration of those reports and of any action taken;
    iii) Reports by the Compliance officer to the trustees and management;
    iv) Reports to the Authority on positive screening results in relation to terrorist financing and the financing of proliferation; and
    v) Reports to the Authority on the total amount of frozen assets in relation to terrorist financing and the financing of proliferation.

8.2 Training Records

54. In order to provide evidence of compliance with Section 21 of the MLFTA at a minimum, the following information must be maintained:
    (i) Details and contents of the training programme attended by or provided to persons associated with the charity or NPO;
    (ii) Names of persons receiving the training;
    (iii) Dates that training sessions were attended or held; and
    (iv) An on-going training plan.

9.0 COMPLIANCE FUNCTION

55. Charities and NPOs must establish procedures for ensuring compliance with legal requirements as set out in relevant legislation and this Guideline to demonstrate that they are able to identify suspicious activity.

56. Trustees and managers have the responsibility of personally carrying out all required due diligence activities, unless this function is contracted out. However, the trustee or manager remains responsible for the compliance function.

57. Each registered charity or NPO must appoint a compliance officer at a senior level who must have access to all relevant internal information without having to seek clearance in each case. Where the compliance function is contracted out, the trustee or manager remains responsible for the function.

9.1 Internal Reporting Procedure

58. To facilitate the detection of suspicious transactions, a charity or NPO should:

(i) Require donors to declare the source of funds where a transaction seems unusual or in excess of threshold limits, or such lower amount as may be determined to reasonably ascertain that funds are not the proceeds of criminal activity **Appendix 2** indicates a specimen of a Declaration of Source of Funds form.

(ii) Develop written policies, procedures and processes to provide guidance on the procedures to be followed when identifying and researching unusual transactions and reporting suspicious activities;

(iii) Identify a suitably qualified and experienced person to whom unusual and suspicious reports are channeled. The person should have direct access to the appropriate records to determine the basis for reporting the matter to the Authority

(iv) Require staff to document in writing their suspicion about a transaction; and

(v) Require documentation of internal enquiries.

9.2 External Reporting - Reporting Suspicious Activity

59. Persons are required by law to report promptly to the FIU where the identity of the person involved, the transaction or any other circumstance concerning that transaction lead the charity or NPO to have reasonable grounds to suspect that a transaction:

(i) Involves proceeds of crime to which the MLFTA applies;

(ii) Involves the financing of terrorism;

(iii) Is of a suspicious or unusual nature; or

(iv) Is conducted by, or relates to, a person against whom a terrorist designation order is in force or relates to the property of such a person.

60. Charities and NPOs are advised to monitor suspicious activity, but there is an obligation to report activity that satisfies the threshold for inconsistency with normal behaviour. After a reasonable time, a transaction, or series of transactions, should be cleared of suspicion, and if this cannot be done with a clear conscience, a report should be made to the FIU.

61. A Suspicious Transaction Report (**Appendix 3**) should be completed and submitted to the FIU for analysis. Once reported, nothing should be done to indicate to any person that such a report was made. There are legal consequences for tipping off a person that an investigation is about to commence or has commenced or that a report was made to the FIU.

Bear in mind that tipping off may be inadvertent and could take place through the loose handling of information.

62. Where a suspicious report has been filed with the Authority, and further unusual or suspicious activity pertaining to the same customer or account arises, licensees should file additional reports with the Authority.

63. In addition, pursuant to the United Nations Security Council Resolutions on terrorist financing and the financing of proliferation, all natural and legal persons, including charities and NPOs are required to freeze any funds or other assets held for individuals or entities so designated by a terrorist designation order or counter-proliferation order in respect to listed persons. Orders will be communicated electronically or in the Official Gazette and local newspapers. Charities and NPOs are required to submit a report to the identified Competent Authority, which should include the total sum of frozen assets. Freezing obligations are extended to all funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, of designated persons or entities, as well as funds or assets of persons and entities on behalf of, or at the direction of, designated persons or entities. Where a terrorist designation order or counter-proliferation order has been lifted, charities and NPOs should have a mechanism in place to release the assets previously frozen.

9.3 Unusual or Suspicious Transactions

1. Suspicious transactions are financial transactions that give rise to reasonable grounds to suspect that they are related to the commission of a money laundering or terrorism offence. These transactions may be complex, unusual or large or may represent an unusual pattern. This includes significant transactions relative to the relationship, transactions that exceed prescribed limits or activity that is inconsistent with the expected pattern of transactions. In some instances, the origin of the transaction may give rise to suspicion. For examples of "Red Flags" see **Appendix 4**.

APPENDICES

APPENDIX 1

Summary of Money Laundering and Terrorism Sanctions and Offences

Area	Description of Offence / Breach	Description of Fine/Sanction	Section of Legislation
Reporting Obligations	Failure of a financial institution or non-financial business entity or professional to make a report on a transaction involving proceeds of crime, the financing of terrorism or is of a suspicious or unusual nature to the FIU Director.	$100,000 on conviction on indictment	Section 23 (2) MLFTA
	Failure of a licensee to maintain business transactions records.	$100,000 on conviction on indictment	Section 18(4) MLFTA
	Failure of a person to report transfers out of Barbados or transfers Barbadian currency or foreign currency into Barbados, of more than BDS$10,000 without Exchange Control permission.	Summary conviction - $10,000 or 2 years imprisonment Conviction on indictment - $200,000 or 5 years imprisonment	Section 24(6) MLFTA
	Failure by a person to report receiving more than BDS$10,000 in Barbadian currency (or foreign equivalent) without the Exchange Control permission.	Summary conviction - $10,000 or 2 years imprisonment Conviction on indictment - $200,000 or 5 years imprisonment	Section 24 (6) MLFTA
Internal Policies, procedures, controls; Internal reporting procedures; Internal employee training and awareness pro-	Failure by a financial institution to develop policies and procedures; audit functions; and procedures to audit compliance.	Imposition of a pecuniary penalty (up to $5,000 for any of the circumstances referred to at section 34(1) of the MLFTA; $500 daily for failure to take a measure or action or cease a iour or practice) in accor-	Section 19(2) of the MLFTA

Area	Description of Offence / Breach	Description of Fine/Sanction	Section of Legislation
grams		dance with section 36.	
Information Gathering & Investigations	Failure by a financial institution to comply with any instruction issued or request made by the FIU Director.	The licence of the financial institution may be suspended.	Section 30(5) of the MLFTA.
Onsite Inspections	Failure to comply with an instruction or request made by an authorised officer or Regulatory Authority.	The licence of the financial institution may be suspended.	Section 31(4) of the MLFTA
Interference in the Line of Duty	The obstruction, hindrance, molestation or assault to any member of the Authority, constable or other person in performing duties under the Act.	$50,000 or imprisonment of 2 years or both.	Section 42 MLFTA
Directives	Contravention of the Act but circumstances do not justify taking action under sections 34, 35 or 36 of the MLFTA.	Issuance of directives by the Anti-Money Laundering Authority or Regulatory Authority to cease and desist.	Section 33 of the MLFTA.
Money Laundering Offences	Engagement in money laundering.	Summary conviction - $200,000 or 5 years imprisonment or both. Conviction on indictment - $2,000,000 or 25 years imprisonment or both. Forfeiture of licence for financial institution.	Section 6 (1) MLFTA Sections 35 & 46(1)
	Providing assistance to engage in money laundering.	Summary conviction - $150,000 or 4 years imprisonment or both. Conviction on indictment - $1,500,000 or 15 years imprisonment or both	Section 6(2) MLFTA

Area	Description of Offence / Breach	Description of Fine/Sanction	Section of Legislation
	A body of persons (corporate or unincorporated) whether as a director, manager, secretary or other similar officer engaging in a money laundering offence.	Subject to trial and punishment accordingly.	Section 44 MLFTA
Disclosure of Information	Disclosure of information on a pending money laundering investigation. Falsifying, concealing, destruction or disposal of information material to investigation or order.	$50,000 or 2 years imprisonment or both	Section 43(b) MLFTA
	Disclosure or publication of the contents of any document, communication or information in the course of duties under this Act.	$50,000 or 5 years imprisonment or both.	Section 48(3) MLFTA.
Terrorism Offences	Provision or collection funds or financial services to persons to be used to carry out an offence as defined in the listed treaties[3] or any other act.	Conviction on indictment to 25 years imprisonment.	Section 4(1) Anti-Terrorism Act
	Provision of assistance or involve in the conspiracy to commit a terrorist offence.	Conviction on indictment and principal offender punished accordingly.	Section 3 of ATA
	A terrorist offence committed by a person responsible for the management or control of an entity located or registered in Barbados, or otherwise organised under the laws of Barbados.	$2,000,000 notwithstanding that any criminal liability has been incurred by an individual directly involved in the commission of the offence or any civil or administrative sanction as imposed by law.	Section 5 of ATA

[3]Treaties respecting Terrorism: Convention for the Suppression of Unlawful Seizure of Aircraft, Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons including Diplomatic Agents, International Convention against the taking of Hostages, Convention on the Physical Protection of Nuclear Material, Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention for the suppression of Unlawful Acts against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf and the International Convention for the Suppression of Terrorists Bombings.

APPENDIX 2

Declaration Of Source Of Funds/Wealth

Customer Name Or Business:.....

Current Address:.....

Account Number:.....

Identification:.....

Amount Of Transaction & Currency:

Description/Nature Of Business Transaction:

☐ Deposit ☐ Monetary Instrument ☐ Currency Exchange ☐ Wire Transfer ☐ Credit/Debit Card

☐ ATM ☐ Loan ☐ Investment ☐ Trust Settlement / Distribution Other ☐ (Specify)

Source of Funds / Wealth:

.....

.....

.....

Supporting Evidence:.....

Customer Signature:.....

Date:.....

Transaction Approved? Yes ☐ No ☐

If No, state reason:.....

.....

.....

OFFICER COMPLETING TRANSACTION
(Signature & Title)

.....

AUTHORISING OFFICER
(Signature & Title)

APPENDIX 3

[Insert updated form available on FIU's website]

CONFIDENTIAL

SUSPICIOUS/UNUSUAL TRANSACTION REPORT

PLEASE TYPE INFORMATION OR WRITE IN BLOCK LETTERS

IMPORTANT: Complete using information obtained during normal course of the transaction. The report should be completed as soon as practicable AFTER the dealing, and a copy forwarded to:

THE DIRECTOR, FINANCIAL INTELLIGENCE UNIT
ANTI-MONEY LAUNDERING AUTHORITY
P.O. BOX 1372 Bridgetown, Barbados
FACSIMILE NO. (246) 436-4756
Email: **adminfiu@barbados.gov.bb**
For urgent reporting – Tel. (246) 436-4734/5

FOR OFFICIAL USE ONLY **FIU Reference No.: .....**

PART A – Initial Information

1. ☐ Completed Transaction ☐ Attempted/Aborted Transaction
☐ Terrorist Designation ☐ Counter-Proliferation Designation

2. Is this report a correction or follow-up to a Report previously submitted?

☐NO
(Skip to No.4)

☐ YES
☐Correction
☐ Follow-up

3. If yes, original Report's date |__|__|__|
D M Y

4. Reporting date |__|__|__|
D M Y

5. Which one of the following reporting entities best describes you:-

- ☐ Accountant
- ☐ Attorney-at-Law
- ☐ Commercial Bank
- ☐ Cooperative Society
- ☐ Credit Union
- ☐ Corporate &/or Trust Service Provider
- ☐ Dealer in Precious Metals &/ or Stones
- ☐ Finance Company
- ☐ Gaming Institution
- ☐ Life Insurance Broker/Agent
- ☐ Life Insurance Company
- ☐ Merchant Bank
- ☐ Money Service Business/Money or Value Transmission Services
- ☐ Mutual Fund Administrator/Manager
- ☐ Real Estate Agent/Entity
- ☐ Regulator
- ☐ Securities Dealer

Part B – Identity of Customer/Client 1

1.Click or tap here to enter text. 2.Click or tap here to enter text.3. Click or tap here to enter text.

Surname Given Name Middle Name(s)

4. Click or tap here to enter text.
Alternative Names/Spelling

5. Click or tap here to enter text.
Address(es)

6. Click or tap here to enter text.
Nationality/(ies)

7. Click or tap here to enter text.
Date of Birth (D/M/Y)

8. Identifier #1 ☐ ID Card
☐ Passport
☐ Driver's License
☐ Other.....

9. Click or tap here to enter text.
ID No.(1)

10. Click or tap here to enter text.
Place of Issue

11. Identifier #2☐ID Card
☐Passport
☐ Driver's License
☐ Other Place of Issue

12. Click or tap here to enter text.
ID No.(2)

13. Click or tap here to enter text.

14. Click or tap here to enter text.
Occupation

15. Click or tap here to enter text.
Employer

16. Click or tap here to enter text.
Telephone # (Include area Code) (H)

Click or tap here to enter text.
Telephone # (Include area code) (W)

Click or tap here to enter text.
Telephone # (Include area Code) (C)

17. Click or tap here to enter text.
Email Address(es)

Click or tap here to enter text.
Email address(es)

18.Click or tap here to enter text.
Account Number(s)

☐ Personal
☐ Corporate
☐ Trust
☐ Other Click or tap here to enter text.

19. Click or tap here to enter text.
State if account is joint, other signatories, etc

20. Click or tap here to enter text.

Provide other account(s) customer may have at institution, include account type, whether joint, other signatories, etc.

CUSTOMER/CLIENT 2

1.Click or tap here to enter text. 2.Click or tap here to enter text.3. Click or tap here to enter text.

Surname Given Name Middle Name(s)

4. Click or tap here to enter text.
Alternative names/Spelling

5. Click or tap here to enter text.

Click or tap here to enter text.
Address(es)

6. Click or tap here to enter text.
Date of Birth (D/M/Y)

7.Click or tap here to enter text.

8. Identifier #1 ☐ ID Card
☐ Passport
☐ Driver's License
☐ Other Place of Issue

9. Click or tap here to enter text.
ID No.(1)

10. Click or tap here to enter text.

11. Identifier #2☐ ID Card
☐ Passport
☐Driver's License
☐ Other .....

12. Click or tap here to enter text.
ID No.(2)

13. Click or tap here to enter text.
Place of Issue

14. Click or tap here to enter text..
Occupation

15. Click or tap here to enter text.
Employer

16. Click or tap here to enter text.
Telephone # (Include area Code) (H)
Click or tap here to enter text.
Telephone # (Include area Code) (C)

Click or tap here to enter text.
Telephone # (Include area code) (W)

17. Click or tap here to enter text.
Email Address(es)

Click or tap here to enter text.
Email address(es)

18.Click or tap here to enter text.
Account Number(s)

☐ Personal
☐Corporate
☐ Trust

☐Other Click or tap here to enter text.

19.Click or tap here to enter text.
State if account is joint, other signatories, etc

20. Provide other account(s) customer may have at institution, include account type, whether joint, other signatories, etc.
Click or tap here to enter text.

Customer 2 applies where there is a transfer between customers.

CUSTOMER/CLIENT– Company

Name:
Please enter the name of the company.

Date of Incorporation:
Click or tap to enter a date.

Share Capital
Click or tap here to enter text.

Country of Incorporation
Click or tap here to enter text.

Number
Click or tap here to enter text.

Type Choose an item.

Business Activity
Click or tap here to enter text.

Website
Click or tap here to enter text.

Relationship to Company:
Please enter the relationship

Items in Relationship to Company Drop-Down Box	
Legal Officer Chief Executive Officer Chief Financial Officer	Nominee Director Shareholder Director
Items in 'Type': Drop-Down Box	
Accountant	Attorney-at-Law
Commercial Bank	

1. Click or tap here to enter text. 2.Click or tap here to enter text. 3. Click or tap here to enter text.

Surname Given Name Middle Name(s)

4. Click or tap here to enter text.
Alternative names/Spelling

5. Click or tap here to enter text.

Click or tap here to enter text.

Address(es)

6. Click or tap here to enter text.
Date of Birth (D/M/Y)

7. Click or tap here to enter text.

8. Identifier #1 ☐ ID Card
☐ Passport
☐ Driver's License
☐ Other

9. Click or tap here to enter text.
ID No.(1)

10. Click or tap here to enter text.
Place of Issue

11. Identifier #2 ☐ ID Card
☐ Passport
☐ Driver's License
☐ Other .....

12. Click or tap here to enter text.
ID No.(2)

13. Click or tap here to enter text.
Place of Issue

14. Click or tap here to enter text..
Occupation

15. Click or tap here to enter text.
Employer

16. Click or tap here to enter text.
Telephone # (Include area Code) (H)
Click or tap here to enter text.
Telephone # (Include area Code) (C)

Click or tap here to enter text.
Telephone # (Include area code) (W)

17. Click or tap here to enter text.
Email Address(es)

Click or tap here to enter text.
Email address(es)

18.Click or tap here to enter text.
Account Number(s)

☐ Personal
☐ Corporate
☐ Trust
☐ Other .....

19. Click or tap here to enter text.
State if account is joint, other signatories, etc

20. Click or tap here to enter text.
Provide other account(s) customer may have at institution, include account type, whether joint, other signatories, etc.

Customer/Client 2 applies where there is a transfer between customers.

PART C – To be completed only if the transaction was conducted on behalf of another person/entity other than those mentioned in Part B.

1. Click or tap here to enter text. Surname

2.Click or tap here to enter text. Given Name

3. Click or tap here to enter text. Middle Name(s)

4. Click or tap here to enter text. Alternative names/Spelling

5. Click or tap here to enter text. Address(es)

6. Click or tap here to enter text. Date of Birth (D/M/Y)

7. Click or tap here to enter text.

8. Identifier #1 ☐ ID Card ☐ Passport ☐ Driver's License ☐ OtherClick or tap here to enter text.

☐ Certificate of Incorporation ☐ Registration for Business Name

9.Click or tap here to enter text. ID No.(1)

10.Click or tap here to enter text. Place of Issue

11.Click or tap here to enter text. Occupation/Type of Business

12. Click or tap here to enter text. Employer	13. Click or tap here to enter text. Telephone (#1)- area code (H)
Click or tap here to enter text. Telephone (#2) - area code (W)	Click or tap here to enter text. Telephone (#3)- area code (C)

14. Click or tap here to enter text. Email Address #1

Click or tap here to enter text. Email Address #2

15. Click or tap here to enter text. Account Number(s)

16. Click or tap here to enter text. State if a/c joint, other signatories, etc

PART D – Transaction Details

1. Type of Transaction

- ☐ Cash Out
- ☐ Deposit to an account Cash/Cheque
- ☐ Life Insurance Policy purchased/deposit
- ☐ Purchase of bank draft
- ☐ Purchase of Jewelry
- ☐ Purchase of precious metals/stones
- ☐ Securities
- ☐ Real Estate Purchase
- ☐ Other .....
- ☐ Conducted Currency Exchange
  - ☐ Inter-account transfer
- ☐ Outgoing electronic funds transfer
- ☐ Purchase of diamonds
  - ☐ Purchase of money order
  - ☐ Purchase of traveller's cheques
- ☐ Purchase of Gold

2. Date(s) of transaction(s) ☐☐ ☐☐ ☐☐☐☐
D M Y

3. Click or tap here to enter text.
Amount & Currency

4. Click or tap here to enter text.
BBD $ Equivalent

5. Click or tap here to enter text.
Name of drawer/Ordering Customer

6. Click or tap here to enter text.
Name of Payee/beneficiary

7. Click or tap here to enter text.
Other bank involved, other Country

Please provide copies of relevant documents (e.g. bank statements, real estate documents, etc.) for suspicious or unusual activity and identification and verification information.

PART E – Grounds for Suspicion

(Please describe clearly and completely the factors or unusual circumstances that led you to suspect that the transaction(s) involve(s) the proceeds of crime, involve(s) the financing of terrorism, is of a suspicious or unusual nature.)

If the report relates to attempted transaction(s), describe why each one was not completed.

Click or tap here to enter text.

PART E2

If additional information is attached, please tick box ☐

PART E3

If identity of the customer has not been established in PART B and they are not known to the officer, give a description (e.g., sex, approximate age, height, built, ethnicity, complexion, etc.)

Click or tap here to enter text.

PART F - Suspected Offences

- ☐ Participation in an organised criminal group and racketeering
- ☐ Terrorism, including terrorist financing;
- ☐ Trafficking in human beings and migrant smuggling
- ☐ Sexual exploitation, including sexual exploitation of children
- ☐ Illicit trafficking in narcotic drugs and psychotropic substances
- ☐ Illicit arms trafficking; and illicit trafficking in stolen and other goods
- ☐ Corruption and bribery
- ☐ Fraud
- ☐ Counterfeiting currency
- ☐ Counterfeiting and piracy of products
- ☐ Environmental crime
- ☐ Murder, grievous bodily injury
- ☐ Kidnapping, illegal restraint and hostage-taking
- ☐ Robbery or theft
- ☐ Smuggling; (including in relation to customs and excise duties and taxes)
- ☐ Tax crimes (related to direct taxes and indirect taxes)
- ☐ Extortion
- ☐ Piracy Forgery
- ☐ Insider trading and market manipulation
- ☐ Proliferation Financing
- ☐ Unknown

PART G - Details of financial institution/place of transaction

1. Click or tap here to enter text.
Organisation

2. Click or tap here to enter text.
Branch where transaction occurred ifapplicable

3. Click or tap here to enter text.
Name and Title of Reporting Officer

4. Click or tap here to enter text.
Signature of Reporting Officer

5. Click or tap here to enter text.
Dealers internal reference number

6. Click or tap here to enter text.
Reporting Officer's direct telephone number

APPENDIX 4

RED FLAGS/HIGH RISK INDICATORS FOR CHARITIES/NPOs

Donations:

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

Beneficiaries:

- A charity or NPO provides financial assistance, services or support on the basis of a certain sum of money per beneficiary and the numbers are relatively high
- A charity or NPO provides services to large numbers of beneficiaries, where it may be easier to disguise additional beneficiaries
- Signs that persons 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, or 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

Partners:

- The project proposal is vague or lacks adequate financial or technical details
- The structure or nature of the proposed project makes it difficult to identify the partner and verify their identity and details
- The proposals include delegating work to other unknown partners or newly formed organizations
- It is difficult to contact the partner at their main address, or their telephone numbers are not working
- The project involves unusual payment mechanisms, or requests for cash, or for money to be paid into an account not held in the name of the partner, or in a country in which the partner is not based and not where the project is being carried out
- Partners request unnecessary or unusual levels of privacy and secrecy
- Requests by partners to use a particular auditor or accountant

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

Monitoring of Projects:

- Invoices and paperwork have been tampered with, altered in crucial aspects with hand-written amendments
- Inventory shortages
- A 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
- Missing key documents or only copies can be produced, which raise suspicions perhaps because they are poor copies or because key details are illegible or have been altered
- Signatures confirming receipt or payment are missing or the invoice is unsigned or un-dated
- Receipts have been signed and dated a long time after the goods or services should have been delivered
- Particularly late or early invoicing
- Repeated excuses of system crashing; losing records or paperwork
- Relief, goods or items provided by the charity or NPO in connection with the project have been tampered with
- Documents accompanying goods and items are missing
- The local community is receiving aid or assistance by other unexplained or unexpected means
- Unexpected transactions, where commission is not charged or no receipts are available
- Figures in documents or records that look familiar or may be repeated
- Discrepancies between budgeted needs and payments requested
- Requests for payment in cash to be made to an unknown third party or other organization
- Payment of administration costs not appearing to relate to the project or which appear unusually high taking into account the nature of the project
- Cash advances and payments that are unusually frequent and/or have not been recorded or approved
- Funds are not being banked or accounted for
- Infrequent and/or poor reconciliation of local banking and accounting records / bank reconciliations not done in a timely manner
- Payments to suppliers via cash payments to employees

- Offers for monitoring to be carried out by friends or known associates of the local partner without the need for the charity or NPO to carry out an inspection or checks on the partner themselves

- Requests to use particular officials in the locality for monitoring purposes

- 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