ANTI-MONEY LAUNDERING/COUNTERING FINANCING OF TERRORISM (AML/CFT); GUIDANCE NOTE FOR NON-GOVERNMENT ORGANISTIONS (NGOs)

1. INTRODUCTION

The Anti- Money Laundering Act, 2013 (the "**AMLA**") lists Non-Government Organisations (**NGOs**)[1] as accountable persons and therefore are subject to the requirements under the AML/CFT legislation and regulations. This guidance is issued by the Financial Intelligence Authority (**FIA**) pursuant to S. 20(d) of the *Anti-Money Laundering Act, 2013.*

The purpose of this Guidance is to provide industry specific guidance for NGO'S on their legal obligations on measures to deter and detect money laundering and the financing of terrorism activities. It provides clarity and interpretation of the issues arising out of the AMLA and the AML regulations. This guidance explains the most common situations under the specific laws and related regulations which impose AML/CFT requirements. It is provided as general information for

[1] For the sake of convenience, the abbreviations NGOs and NPO will be used throughout the text of this Guidance to indicate the terms "non-government organisations" and "non-profit organisations", respectively.

guidance. It is not legal advice, and is not intended to replace the Acts and Regulations.

NPOs by their nature are vulnerable to crimes. An NPO may be set up as a sham business to bring illegally obtained funds into the financial system. Legitimately obtained funds can be channeled through NPOs and misused by terrorists to finance terrorist activities. For example, an 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 end up being transferred to a terrorist group.

In light of the vulnerability of NPOs to ML/FT, Recommendation 8 of the FATF 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;

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 Uganda enacted the Non-Government Organisation Act, 2016. It was made to provide for the registration of NGOs, the establishment and maintenance of a register of NGOs, the obligations of NGOs and for other related matters.

2. PURPOSE/OBJECTIVE OF THESE GUIDANCE NOTES.

The purpose of this document is to provide industry specific guidance for NGOs in Uganda on their legal obligations to detect and deter Money Laundering (ML) and Financing of Terrorism (FT) activities using a risk based approach.

3. WHEN DO THE AML/CFT OBLIGATIONS APPLY TO NGOS

Section 8 of the AMLA, 2013 as amended subjects its requirements to NGOs when engaged in any cash transactions either domestic or foreign exceeding one thousand currency points equivalent of UGX. 20,000,000/= (UGX. Twenty Million Only).

4. SUMMARY OF AML/CFT OBLIGATIONS FOR NPOS

All NGOs are required by the AMLA and the AML Regulations to fulfill certain obligations. These obligations include:

(1) Registration with the Financial Intelligence Authority (FIA)
(2) Obtain Due Diligence Information (CDD)
(3) Reporting suspicious transactions and certain cash transactions
(4) Ensure that there are internal controls to prevent money laundering and financing of terrorism.
(5) Appoint a Money Laundering Control Officer,
(6) Conduct Risk Assessment and give a report to the Financial Intelligence Authority (FIA) of the Risk Assessment
(7) Not to enter into or continue a business transaction or business relationship with a designated entity.
(8) Reporting Terrorist Funds/Property
(9) Reporting Large Cash Transactions
(10) Record Keeping
(11) No Tipping Off
(12) Develop A Written Compliance Programme
(13) Implement And Test Your Compliance Programme

4.1 REGISTRATION WITH FIA

Regulation 4 of the AMLA Regulations, 2015, requires all NGOs to register with the FIA for the purpose of establishing the identity of an entity to be able to be supervised by the FIA. The entity must also notify the FIA of a change of address of its registered office or principal place of business.

How to Register

On-line registration can be done through the FIA's website; www.fia.go.ug. Alternatively, you may download the form from the website, have it filled and physically delivered to FIA office on; Plot 6 Nakasero Road, 4th Floor Rwenzori Towers (Wing B).

4.2 OBTAIN KYC AND DUE DILIGENCE INFORMATION (CDD)

NGOs as accountable persons must comply with Section 6 the AMLA, as amended to conduct customer due diligence where it engages in a financial transaction. The NPO must obtain relevant identification documentation which can include a valid passport, national identification card or driver's license to identify the donor or beneficiary. The identity so established should then be verified through reliable and independent sources.

In order to apply a Risk Based Approach, NPOs need to be 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. These are 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. NPOs that are assessed as high risk are subject to AML/CFT compliance examinations by the FIA. The FIA is empowered under section 21 of the AMLA, 2013 as amended to monitor and supervise, including conducting onsite AML/CFT examinations of NPOs.

NPOs that are selected for compliance examinations, which is done on a risk based assessment will be notified in advance of the examination and provided with a list of items that the FIA officers will be seeking to verify. The main purpose of the compliance examination is to test the effectiveness of AML/CTF 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:

a) 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 nature of the NPO.
b) 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 organization.
c) Give careful consideration to due diligence, monitoring and verification of use of funds they need to meet their legal duties
d) Take reasonable and appropriate steps to know who their beneficiaries are, at least in broad terms, carry out appropriate checks, especially where the risks are high and have clear beneficiary selection criteria which are consistently applied. Know Your Donors:
e) Know your donors. Before receiving funds from a donor, NPOs must establish that the donor is not a sanctioned entity, either under the UN or other authority.
f) 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.

g) NPOs shall conduct, on a risk-based approach, a 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 or are under sanctions for being involved in activities relating to terrorism, including terrorist financing.

Know Your Beneficiaries and Partners:

a) NGO must ascertain correct and complete identification particulars of each of its beneficiary (person, group of persons or organisation) who receives cash or services or in-kind contributions.
b) In case the beneficiary is an organization/ group of persons, the donor NPO must have knowledge of detailed profile and particulars of such organisation. NGO shall ensure that it's beneficiaries are not linked to any suspected terrorism activity or th terrorist support networks.
c) 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.
d) 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: NGO must maintain records of particulars of its employees (both Ugandan nationals or foreign nationals), including but not limited to permanent address, present address, copy of national ID card, passport number, nationality, personal email, employment ID, and phone/ mobile number.

4.3 REPORTING SUSPICIOUS TRANSACTIONS AND CERTAIN CASH TRANSACTIONS

NPOs are under obligation to report suspicious transactions, not later than two (2) working days from the date the suspicion was formed. The obligation to report is provided for under Section 9 of the AMLA, 2017 (as amended).

a) Defining Knowledge and Suspicion

i. Before an NPO files a report, it must know or have reasonable grounds for suspecting, that the person to be reported is engaged in ML or FT.

ii. NPOs are also required to report if they have 'reasonable grounds' to suspect that someone is engaged in money laundering or financing of terrorism. The requirement to report will apply based on the facts of the particular scenario and the conclusion that those facts should have led to a suspicion of money laundering or financing of terrorism.

b) Attempted Transactions

NPOs have to pay attention to suspicious attempted transactions. If a donor attempts to conduct a transaction, but for whatever reason that transaction is not completed, and the NPO believes that the attempted transaction is suspicious, it must report it to the FIA. Example of suspicious attempted transaction: a donor wants the NPO to send funds to another charity in a conflict zone for him. He could be vague on the proposed beneficiary's business activities.. The NPO asks him for identities of the beneficiaries and he delays in providing it but keeps pressing for the funds to be sent and he subsequently terminates the transaction. If the NPO believes that this transaction is related to some crime, then it has to report that attempted transaction to the FIA. 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 the NPO knows or reasonably suspects that the funds are criminal proceeds or related to money laundering that it has to report: It does not have to know what the underlying criminal activity is or whether illegal activities actually occurred in order to report suspicious transactions/activities.

c) How to Identify a Suspicious Transaction/Activity

The NPO should be able to determine whether a transaction or activity is suspicious based on its knowledge of the NPO. Its 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. It will need to consider factors such as;

i. 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.

ii. Industry specific indicators would also help you're the NPO and its employees to better identify suspicious transactions whether completed or attempted.

4.4 ENSURE THAT THERE ARE INTERNAL CONTROLS TO PREVENT MONEY LAUNDERING AND FINANCING OF TERRORISM.

These include among others; auditing, carrying out compliance checks, file annual compliance reports, monitoring customers and transactions, training of staff in AML/CFT, putting in place AML/CFT policies and procedures.

The degree and nature of monitoring by an NGO will depend on;

i. The size of the NGO

ii. The AML/CFT risks that it has

iii. The monitoring method being utilised (manual, automated or some combination), and

iv. The type of activity under scrutiny.

4.5 APPOINT A MONEY LAUNDERING CONTROL OFFICER,

The Money Laundering Control Officer (MLCO) appointed must be a senior officer or other competent professional whose details have to be registered with the Financial Intelligence Authority (FIA). Any changes that may arise in the registered details must also be reported. This requirement is provided for under Regulation 6 of the AMLA, 2015. The duty of the MLCO is to implement the compliance of the NPO with AML/CFT requirements. They include;

i. Monitoring transactions, (e.g. routine or spot checking).

ii. Making suspicious transaction reports to the FIA.

iii. Regular reporting to senior management about AML/CFT performance.

If the NPO does not have employees, then the owner can appoint himself/herself as MLCO to implement a compliance regime. Further, as a good governance practice, the appointed officer in an NPO should preferably not be directly involved in the receipt, transfer or payment of funds.

The MLCO's responsibilities include:

i. Having full responsibility for overseeing, developing, directing, updating and enforcing the AML/CFT Programme;

ii. Being competent and knowledgeable regarding ML/TF issues and risks and the AML/CTF legal framework;
iii. Submitting STRs to the FIU and keeping relevant records;
iv. Acting as Liaison officer between your NPO and the FIA;
v. Ensuring the training of employees, volunteers and directors on AML/CFT obligations; and
vi. Ensuring independent audits of the Compliance Programme are conducted.
vii. Monitoring transactions, (e.g. routine or spot checking).
viii. Making suspicious transaction reports to the FIA.
ix. Regular reporting to senior management about AML/CFT performance.

Section 9A of AMLA, 2013 as amended; states that the identities of the MLCO must be treated with the strictest confidence by the NPO and its employees. For consistency and on-going attention to the compliance regime, the appointed MLCO may choose to delegate certain duties to other employees. For example, the MLCO 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 officer retains full responsibility for the implementation of the compliance regime.

4.6 CONDUCT RISK ASSESSMENT AND GIVE A REPORT TO THE FINANCIAL INTELLIGENCE AUTHORITY (FIA). This requirement is provided for under Section 6A (1) to (3) of the AMLA, 2017 (as amended). NGOs should conduct risk assessments of their business taking into account the following factors:

i. The size of their NGO, e.g. the financial value of the transactions facilitated.

ii. Nature of business of the donor, overseas and/or domestic.

iii. How funds are obtained, e.g. through advertising, or through referrals

4.7 NOT TO ENTER INTO OR CONTINUE A BUSINESS TRANSACTION OR BUSINESS RELATIONSHIP WITH A DESIGNATED/SANCTIONED ENTITY. A designated entity means any individual or entity and their associates designated as terrorist entities by the United Nations Security Council (UNSC) Resolutions1267,

i. United Nations Resolutions 1267/1989 (Al-Qaida) adopted unanimously on 15 October 1999, designating Osama bin Laden and associates as terrorists and establishing a sanctions regime to cover individuals and entities associated with AlQaida, Osama bin Laden and the Taliban, wherever located;

ii. United Nations Resolutions 1267/1988 (Taliban) adopted unanimously on June 17, 2011, on terrorism and the threat to Afghanistan, and imposing sanctions regimes on Al-Qaeda and the Taliban and:

iii. 1373 where United Nations Resolutions 1373 adopted unanimously on 28 September 2001, as a counter-terrorism measure following the 11 September terrorist attacks on the United States; and their successive Resolutions.

4.8 REPORTING TERRORIST FUNDS/PROPERTY

i. Section 9 of the AMLA, 2013 as amended provides that the NPO must report immediately to the FIA the existence of funds that it has received where it knows or has 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. The NPO must report immediately to the FIA where it knows or have reasonable grounds to believe that a person or entity named on the UNSC list has funds in Uganda.

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

4.9 REPORTING LARGE CASH TRANSACTIONS

Section 8 of the AMLA, 2013 as amended requires all NPOs to report all cash and monetary transactions equivalent to or exceeding one thousand currency points equivalent of UGX. 20,000,000/= (UGX. Twenty Million Only).USD 10,000.

4.10 RECORD KEEPING

Section 7 of the AMLA, 2013 as amended, provides that NGOs must keep a record of each and every transaction for a minimum period of 10 (ten) years .Record keeping is important for anti-money laundering investigation and analysis because it 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.

NGOs must keep the following records in electronic or written form for a period of ten (10) years or such longer period as the FIA may direct. The records must be kept for ten (10) years after the end of the business relationship or completion of a one-off transaction.

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

4.11 DEVELOP A WRITTEN COMPLIANCE PROGRAMME/POLICY

NPOs that have registered with the FIA must develop a written Compliance Programme ("CP"). The CP has to be approved by senior management. The CP is a written document which include a risk assessment of the NGO and sets out the system of internal procedures, systems and controls which are intended to mitigate the vulnerabilities and inherent risks identified during the assessment and which can be exploited by money launderers and terrorism financiers. The CP will contain measures that ensure compliance with reporting, record keeping, customer due diligence, employee training, and other AML/CFT obligations. These policies, procedures and controls, must be communicated to

all your members, and when fully implemented, will help reduce the risk of the NGO from being used for ML/FT. The CP must be reviewed periodically. A well-designed, applied and monitored CP will provide a solid foundation for compliance with the AML/CFT laws. As not all individuals and entities operate under the same circumstances, compliance procedures will have to be tailored to fit the NPO's specific needs. It should reflect the nature, size and complexity of your operations as well as the vulnerability of your business to ML/FT activities. The following five (5) elements must be included in your compliance regime:

a) The appointment of a staff member as MLCO and his/her responsibilities;
b) Internal compliance policies and procedures such as reporting suspicious transactions/activities to the MLCO; the implementation of CDD and record keeping;
c) Your assessment of your risks to ML/FT, 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.

4.12 IMPLEMENT AND TEST YOUR COMPLIANCE PROGRAMME/POLICY

The obligations for an NPO include implementing a written CP. The FIA 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 risks. Internal testing must be undertaken to evaluate compliance by staff with the 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 MLCO, to avoid potential conflict since the MLCO 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 the Compliance Officer is also the most senior employee, an external independent review will satisfy compliance with the obligation to test implementation of AML/CFT obligations.

5. CONSIDER THE FOLLOWING RED FLAGS FOR NGOs

DONATIONS

i. Unusual or substantial one-time donations are received form unidentifiable or suspicious sources.
ii. If a series of small donations are received from sources that cannot be identified or checked
iii. Where donations are made in a foreign currency or foreign sources where financial regulation or AML/CFT legal framework is not as rigorous.
iv. Where payments received from a known donor but through an unknown party.
v. Where donations are received from unknown or anonymous bodies
vi. Where payments received from an unusual payment mechanism where this would not be a typical method of payment.
vii. Where donations are conditional to be used in partnership with particular individuals or organisations where the NPO has concerns about those individuals or organisations.
viii. If conditions attached to a donation are such that the NPO would merely be a vehicle for transferring funds from one individual or organisation to another individual or organization

ix. Where an NPO is asked to provide services or benefits on favorable terms to the donor or a person(s) nominated by the donor as beneficiaries

BENEFICIARIES

i. Where an NPO provides assistance, services or support on the basis of certain sum of money per beneficiary and the numbers are relatively high.
ii. Where an NPO provides services to larger numbers or beneficiaries, where it may be easier to disguise additional beneficiaries
iii. Where there may appear signs that people may have been placed on distribution and aid lists by providing kickbacks and bribes to officials
iv. Lists of beneficiaries contain multiple manual corrections, multiple names may appear, may contain more family members
v. Evidence that third parties or intermediaries have demanded payment for recommending or nominating beneficiaries
vi. Fake or suspicious identity documents.
vii. Beneficiaries with identical characteristics and addresses or multiple identical or similar names and signatures of employees

EMPLOYEES

i. Indications that staff may be living beyond their means or appearing at unusual times.
ii. Staff carrying out tasks or jobs they should not be, or other unusual staff behavior or conduct
iii. Sudden or increased staffing costs for the projects

PROJECTS

i. Invoices and paperwork have been tampered with, altered in crucial aspects with handwritten amendments.
ii. Inventory shortages
iii. The project is vague or lacks adequate financial or technical details.

iv. Missing key documents or only copies can be reproduced.
v. Lack of evidence to show fair and transparent tendering or procurement procedures
vi. Invoices and papers recording a higher cost for goods or services than expected or agreed.
vii. Signatures confirming receipt or payment are missing or the invoice unsigned or undated.
viii. Receipts have been signed and dated a long time after the goods or services should have been delivered.
ix. Repeated excuses of system crashing, losing records or paperwork.
x. Discrepancies between budgeted needs and payments requested.
xi. Requests for payments in cash to be made to an unknown third party or other organization.
xii. Funds are not being banked or accounted for.
xiii. 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.
xiv. Inconsistencies between narrative reports and financial claims and reports Partners.

PARTNERS

i. The structure or nature of the proposed project makes it difficult to identify the partner and verify their identity and details.
ii. The proposal includes delegating work to other unknown partners or newly formed organisations.
iii. Partners request unnecessary or unusual levels of privacy and secrecy.
iv. Requests by partners to use a particular auditor or accountant.
v. 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 that may be suspicious. ML includes the layering and

integrating stages where there is no new cash, but funds that are moved around while trying to confuse the money trail.

6. OFFENCES AND PENALTIES FOR NON-COMPLIANCE

Failure to comply with the obligations under the AMLA and the AML regulations may result in criminal and/or administrative sanctions.

Penalties may include fines and terms of imprisonment. Sanctions include possible revocation of licenses, issuance of directives and court orders.

The offences under the AMLA include;

a. Money Laundering (section 3 and 116);
b. Tipping Off (section 117);
c. Falsification, Concealment of documents (section 118);
d. Failure to identify persons (section 119);
e. Failure to keep records (section 120);
f. Facilitating money laundering (section 121);
g. Destroying or tampering with records (section 122);
h. Refusal, omission, neglect or failure to give assistance (section 123);
i. Failure to report cash transactions (section 124);
j. Failure to report suspicious or unusual transactions (section 125);
k. Failure to report conveyance of cash into or out of Uganda (section 126);
l. Failure to send a report to the Authority (section 127);
m. Failure to comply with orders made under the Act (section 128);
n. Contravening a restraining order (section 129);
o. Misuse of information (section 130);
p. Obstructing an official in performance of functions (section 131);
q. Influencing testimony (section 132);
r. General non-compliance with requirements of this Act and conducting transactions to avoid reporting duties (section 133);
s. Unauthorised access to computer system or application or data (section 134);

t. Unauthorised modification of contents of computer system (section 135).

Penalties

According to section 136 of the AMLA, a person who commits money laundering is liable on conviction to:-

a. in the case of a natural person, imprisonment for a period not exceeding fifteen years or a fine not exceeding one hundred thousand currency points or both;
b. in the case of a legal person by a fine not exceeding two hundred thousand currency points.

According to section 136(2) of the AMLA, a person who commits any other offence under the Act is punishable-

a. if committed by a natural person, by imprisonment for a period not exceeding five years or a fine not exceeding thirty-three thousand currency points, or both;
b. if committed by a legal person such as a corporation, by a fine not exceeding seventy thousand currency points;
c. if a continuing offence, by a fine not exceeding five thousand currency points for each day on which the offence continues; or
d. if no specific penalty is provided, by a fine not exceeding nine thousand currency points and in case of a continuing offence, to an additional fine not exceeding five thousand currency points for each day on which the offence continues

7. REVIEW OF THE GUIDELINES

NGOs are encouraged to compile and record any comments, which arise in relation to these guidelines, and forward them to the Financial Intelligence Authority for its appropriate action