SECURITIES AND EXCHANGE COMMISSION (SEC)
AND
FINANCIAL INTELLIGENCE CENTRE (FIC)

"Ensuring Investor Protection"

ANTI-MONEY LAUNDERING/COMBATING THE FINANCING OF TERRORISM & THE PROLIFERATION FINANCING OF WEAPONS OF MASS DESTRUCTION (AML/CFT / CPF) GUIDELINES

SEC/GUI/001/08/2021

NOVEMBER 1, 2021

Table of Contents

LIST OF ACRONYMS & ABBREVIATION

ACAMRO	-	Association of Capital Market Anti-Money Laundering Reporting Officers.
AML/CFT & PF	-	Anti-Money Laundering/ Combating the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction
AMLRO	-	Anti-Money Laundering Reporting Officer
ATM	-	Automatic Teller Machine
CDD	-	Customer Due Diligence
CFT	-	Combating of the Financing of Terrorism
CTR	-	Currency Transaction Report
DNFBPs	-	Designated Non-Financial Businesses and Professions
ETR	-	Electronic Transaction Report
FATF	-	Financial Action Task Force
FIC	-	Financial Intelligence Centre
GIABA	-	Inter-Governmental Action Group against Money Laundering in West Africa
IOSCO	-	International Organization of Securities Commissions
KYC	-	Know Your Customer
LEA	-	Law Enforcement Agency
MDAs	-	Ministries, Departments and Agencies
ML	-	Money Laundering
MO	-	Market Operator
NGO	-	Non-Governmental Organization
NIC	-	National Insurance Commission
PEP	-	Politically Exposed Person
PF	-	Proliferation Financing
RO	-	Religious Organization
SEC	-	Securities and Exchange Commission
SIA	-	Securities Industry Act

STR	-	Suspicious Transaction Report
TF	-	Terrorist Financing

FOREWORD

Misuse of Ghana's financial market for financial crime purposes can result in significant economic, political and security consequences at both national and international levels. In spite of Anti-Money Laundering, Countering the Financing of Terrorism and Proliferation Financing of weapons of mass destruction (AML/CFT&PF) efforts in Ghana, policy makers still face challenges in their ability to combat this menace.

Full and effective implementation of the new AML Act and the FATF Revised 40 Recommendations by MOs is critical to the safety and integrity of the Ghanaian financial market. In view of this, the SEC/FIC AML/CFT&PF Guidelines have been revised to provide effective procedures for Market Operators (MOs) to implement risk-based approach to prevent, deter, detect and mitigate the emerging financial crime risks related to money laundering, terrorist financing and proliferation financing of weapons of mass destruction.

These Guidelines have been revised in accordance with the update made to the following documents:

a. New AML Act, 2020 (Act 1044)
b. Revised FATF 40 Recommendations
c. Lessons drawn from working with the previous SEC/FIC/ AML/CFT&PF Guidelines for MOs in Ghana.
d. Lessons learnt from Ghana's 2018 National Risk Assessment's report updated in 2018
e. Lessons learnt from Ghana's 2016 Mutual Evaluation Report

The Guidelines which have been duly validated by the Financial Intelligence Centre (FIC) and Market Operators (MOs) must be strictly complied by all market operators in the performance of their AML/CFT&PF obligations.

INTRODUCTION

The Securities and Exchange Commission (SEC) is empowered to ensure that all its regulated entities operate in compliance with the provisions of:

a. Section 138 of Securities Industry Act, 2016 Act (929)
b. Section 52 of the Anti-Money Laundering Act, 2020 Act (1044)
c. Anti-Terrorism Act, 2008 (Act 762) as amended by Anti-Terrorism (Amendment) Act, 2014 (Act 875); and
d. The Revised 40 Financial Action Task Force (FATF) Recommendations

to fight Money Laundering (ML), Terrorist Financing TF, the Proliferation Financing of Weapons of Mass Destruction (PF) and other financial crimes.

Given the prominence that financial crimes especially Money Laundering (ML), Terrorist Financing (TF), the Financing of the Proliferation of Weapons of Mass Destruction (PF) and transnational organized crimes have assumed and the risks they pose to the financial markets globally and to Ghana in particular, the need for a comprehensive effort to fight this menace has been realized. It is against this background that SEC and the Financial Intelligence Centre (FIC) in accordance with Section 52 of AML Act 1044 have developed these Guidelines for Market Operators (MOs) to enhance their operations, monitoring and surveillance systems with a view to preventing, detecting and responding appropriately to ML, TF, PF and similar risks in the financial market. SEC also collaborates with appropriate Law Enforcement Agencies (LEAs) and other stakeholders in its work.

These Guidelines are issued pursuant to section 209 of Securities Industry Act, 2016 Act (929) and is structured in two parts, namely Part A and Part B.

Part A covers among others the following areas:

i. Institutional Policy Framework;
ii. Risk Assessment;
iii. Reporting Officer designation and duties;
iv. The need to co-operate with the supervisory authorities;

v. Customer Due Diligence;

vi. Monitoring and responding to suspicious transactions reporting requirements;

vii. Record keeping; and

viii. AML/CFT & PF employee training program.

Part B covers areas such as:

i. Know Your Customer (KYC) procedures;

ii. Identification procedures; and

iii. Financial inclusion and sanctions.

DIRECTOR-GENERAL
SECURITIES AND EXCHANGE COMMISSION

CHIEF EXECUTIVE OFFICER
FINANCIAL INTELLIGENCECENTRE

1.0. PART A

1.1. AML/CFT & PF INSTITUTIONAL POLICY FRAMEWORK

Persons, who hold ownership (including beneficial ownership), control and/ or key management roles in an MO, shall ensure that:

a. The MO designates an officer appropriately as the AMLRO to; inter alia supervise the monitoring and reporting of suspicious transactions and shall put in place a structure that ensures the operational independence of the AMLRO.

b. The MO develops a written policy framework that would guide and enable its staff to monitor, recognize and respond appropriately to suspicious transactions in dealing with financial crimes. A list of ML/TF&PF "Red Flags" is provided in Appendix C to these Guidelines**.**

c. The MO becomes alert to the various patterns of conduct that have been known to be suggestive of ML/TF & PF and maintain a checklist of such transactions which shall be disseminated to the relevant staff.

d. A staff of an MO, who detects any "red flag" or suspicious activity shall promptly report to the AMLRO. Every action taken by the AMLRO (including any preliminary investigations and any suspicious transaction report filed with the FIC) shall be documented and treated with confidentiality.

e. Where the MO suspects or has reason to suspect that a client's funds are the proceeds of unlawful activity related to ML/TF&PF, it shall report promptly to the FIC. Any suspicious transactions, including attempted transactions shall be reported regardless of the amount involved. This requirement to report suspicious transactions shall apply regardless of whether they are thought, among other things, to involve tax matters.

f. The directors and employees (permanent and temporary) of MOs are prohibited from disclosing to anybody, the fact that a report is required to be filed or has been filed with the competent authorities.

g. The MO adopts policies indicating its commitment to comply with AML/CFT & PF obligations under the relevant Acts and Regulations to prevent any transaction that facilitates these activities.

h. The MO formulates and implements internal rules, procedures and other controls that will deter criminals from using its facilities for ML/TF&PF and to ensure that its obligations under the relevant laws and regulations are always met.

i. The MO puts in place the following AML/CFT & PF preventive measures:

- **i.** appointment of AMLRO;
- **ii.** risk assessment;
- **iii.** design and implementation of internal policies, controls and procedures (see Section 49 of Act 1044 and Appendix H of these Guidelines);
- **iv.** conduct of continuous employee education and training; and
- **v.** independent audit testing of its compliance programme.

j. The MO establishes and maintains internal policies, procedures, processes and controls to prevent ML/TF&PF and to communicate these to its employees.

1.2 CO-OPERATION WITH COMPETENT AUTHORITIES

a. An MO shall declare its commitment to comply promptly with all requests made pursuant to the law and regulations and provide information to the SEC, FIC and other relevant competent authorities.

b. An MO's procedures for responding to authorized requests for information on ML,TF& PF shall include the following:

- **i.** search immediately through the institution's records to determine whether it maintains or has maintained any account for or has engaged in any transaction with each individual, entity, or organization named in the request(s);
- **ii.** report promptly to the competent authority the outcome of the search (refer to Section 36 of Act 1044) and
- **iii.** protect the security and confidentiality of such requests.

1.3 ASSESSING ML/TF&PF RISK AND APPLYING A RISK–BASED APPROACH **(refer to Recommendation 1 of FATF 40 recommendations)**

- **a.** An MO's AML/CFT & PF risk management function shall be aligned and integrated with its overall risk management control function.
- **b.** An MO shall take appropriate steps to identify, assess and understand its ML/TF & PF risks in relation to its customers, geographical areas, products and services, transactions or delivery channels in the form of a framework to guide staff in the organization.

c. An MO shall use the results of its risk assessment to design its AML/CFT & PF Compliance Programme in accordance with Section 49 of Act 1044 and its regulations.

d. An MO, in assessing ML/TF & PF risks, shall:

i. document its risk assessments methodology and submit a copy to the SEC upon request;

ii. document its risk assessment findings in the form of a risk assessment report and submit a copy to the SEC and FIC upon request;

iii. consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

iv. keep the assessment up-to-date through a periodic review; and

v. provide periodic risk assessment information to SEC anytime there is a review and or upon a request.

e. An MO shall:

i. conduct additional risk assessment when required by the SEC;

ii. be guided by the findings of National Risk Assessment Reports in conducting its risk assessments;

iii. be guided by the findings of Mutual Evaluation Reports in conducting its risk assessments;

iv. provide timely reporting of its;

a. AML/CFT & PF risk assessment;

b. ML/TF & PF risk profile (risk categorization) and

c. the effectiveness of risk control and mitigation measures

to its Board of Directors.

The frequency of the reporting shall be determined by the Board.

Further Guidance on MOs Risk Assessment and Business/Customer Risk Profiling is provided in Appendix D.

1.4 RISK ASSESSMENT FOR NEW PRODUCTS

a. An MO shall review, identify and record areas of potential ML/TF&PF risks for new products that are not covered by these Guidelines and submit a report for SEC's approval before they are launched.

b. An MO shall review its AML/CFT & PF framework from time to time with a view to determining their adequacy and identification of other areas of potential risks when introducing new products.

1.5 APPOINTMENT AND DUTIES OF ANTI–MONEY LAUNDERING REPORTING OFFICER

a. An MO shall appoint a person to act as an Anti-Money Laundering Reporting Officer (AMLRO) who shall be a key management personnel of the MO and will operationally report to its Board in accordance with section 50(b) of the Act 1044 and AML Regulations, 5(1) of L.I. 1987.

b. The AMLRO shall have relevant AML/CFT & PF qualification(s) and experience as may be approved by the Commission from time to time.

c. The AMLRO shall:

- **i.** develop and implement an AML/CFT & PF Compliance Programme;
- **ii.** receive reports from staff and conduct preliminary investigations of suspicious transactions;
- **iii.** file suspicious transaction report, cash transaction report and electronic transaction report with the FIC;
- **iv.** coordinate the training of staff in AML/CFT & PF awareness, detection methods and reporting requirements;
- **v.** serve as a liaison officer to the SEC and the FIC, and a point-of-contact for all employees on issues relating to ML, TF and PF; and
- **vi.** undertake other duties relevant to AMLRO's function.

d. An MO shall ensure that its AMLRO has access to any information that may be of assistance to him/her in consideration of a suspicious transaction. The MO shall also ensure that its AMLRO cooperates with the Law Enforcement Agencies to facilitate the exchange of information relating to ML/ TF&PF.

1.6 CUSTOMER DUE DILIGENCE (Refer to Section 30 of Act 1044)

1.6.1An MO shall undertake CDD where:

- **a.** Business relationships are established;

b. Carrying out occasional transactions relating to the applicable designated threshold of GHS50, 000.00 (or its equivalent in foreign currency) or as may be determined by the FIC from time to time. This may include transactions carried out in a single operation or several operations that appear to be linked. It may also involve carrying out occasional transactions such as money transfers, including those applicable to cross border and domestic transfers between MOs by means of credit or debit cards and other financial technologies to effect the transaction. The following transactions are however, exempted:

i. Any transfer flowing from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanying such transfers does flow from the transactions such as withdrawals from a bank account through an ATM, cash advances from a credit card or payment for goods.

ii. MO-to-MO transfers and settlements where both the originator person and the beneficial person are MOs acting on their own behalf.

c. There is a suspicion of ML/TF&PF, regardless of any exemptions or any other thresholds referred to in the Guidelines or

d. There are doubts about the veracity or adequacy of previously obtained customer identification data.

1.6.2 The MOs are not permitted to operate numbered accounts, anonymous accounts or accounts in fictitious names.

1.7 CDD PROCEDURES

a. An MO shall identify their customers (whether permanent or occasional; natural or legal persons; or legal arrangements) and verify the customers' identities using reliable, independently sourced documents, data or information. All MOs are required to carry out the full range of the CDD procedures in these Guidelines. However, in reasonable circumstances, MOs can apply the CDD procedures on a risk-based approach.

b. Types of customer information to be obtained and identification data to be used to verify the information are provided in **Appendix A**.

In respect of customers that are legal persons or legal arrangements, MOs shall:

i. Verify the identity of the person purporting to have been authorized to act on behalf of such a customer and

ii. Verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from the Registrar General's Department or similar evidence of establishment or existence and any other relevant information.

c. An MO shall identify a beneficial owner and take reasonable measures to verify his/her identity using relevant information or data obtained from a reliable source to satisfy themselves that they know who the beneficial owner is.

d. An MO shall in respect of all customers determine whether or not a customer is acting on behalf of another person. Where the customer is acting on behalf of another person, the MO shall take reasonable steps to obtain sufficient identification data and to verify the identity of that other person.

e. An MO shall take reasonable measures in respect of customers that are legal persons or legal arrangements to:

i. Understand the ownership and control structure of such a customer and

ii. Determine the natural persons that ultimately own or control the customer.

Where the customer or the owner of the controlling interest is a public company listed on a recognized securities exchange, it is not necessary to identify and verify the identity of the shareholders of such a public company.

f. An MO shall obtain information on the purpose and intended nature of the business relationship of their potential customers.

g. MOs shall conduct ongoing due diligence on the business relationship as stated in **(f).**

h. The ongoing due diligence in **(g)** above includes scrutinizing the transactions undertaken by the customer throughout the course of the MO/customer relationship to ensure that the transactions being conducted are consistent with the MO's knowledge of the customer, its business and risk profiles, and the source of funds. In keeping with this requirement, MOs may develop or acquire an automated monitoring tool to monitor all transactions aimed at detecting suspicious transactions by their customers.

i. MOs shall ensure that documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly the records in respect of high-risk business relationships or customer categories.

j. MOs shall screen all customers (both existing and new) against all domestic and international sanctions lists.

1.8 HIGH-RISK CATEGORIES OF CUSTOMERS

An MO shall perform enhanced due diligence for high-risk categories of customers and business relationships or transactions. These measures include making enquiries on:

i. the purpose for opening the account;
ii. the level and nature of trading activities intended;
iii. the ultimate beneficial owners of the account;
iv. the source of funds; and
v. the source of wealth.

An MO shall continue to undertake enhanced monitoring of the business relationship. Refer to Appendices C and D.

1.9 LOW RISK CUSTOMERS, TRANSACTIONS OR PRODUCTS

a. Where there are low risks, MOs shall apply reduced or simplified measures.

- **i.** MOs that apply simplified or reduced CDD procedures on customers' resident abroad are required to limit such to customers in countries that have effectively implemented the FATF Recommendations.
- **ii.** Simplified CDD procedures are not acceptable and therefore cannot apply to a customer whenever there is suspicion of ML/TF&PF or specific high-risk scenarios. In such a circumstance, enhanced due diligence is mandatory.

b. MOs shall prepare an internal risk assessment framework to identify, assess and take effective action to mitigate its ML/TF&PF risks.

1.10 TIMING OF VERIFICATION

a. An MO shall verify the identity of the customer, beneficial owner and occasional customers before or during the course of establishing a business relationship or conducting transactions for them except where:

i. This can take place as soon as reasonably practicable;

ii. It is essential not to interrupt the normal business conduct of the customer. This may include:

a. Non face-to-face business.

b. Securities transactions

c. Life insurance business.

iii. The ML/TF&PF risks can be effectively managed.

b. Where a customer is permitted to utilize the business relationship prior to verification, MOs shall adopt risk management procedures including a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship and have no apparent or visible economic or lawful purpose.

1.11 FAILURE TO COMPLETE CDD

a. An MO which does not comply with section 1.7. shall :

i. not open the account, commence business relations or perform the transaction; and

ii. submit a Suspicious Transaction Report (STR) to the Financial Intelligence Centre (FIC) within twenty four hours.

b. The MO that has already commenced the business relationship (without having performed section 1.10) shall terminate the business relationship and submit a Suspicious Transaction Report (STR) to the Financial Intelligence Centre (FIC) within twenty four hours.

c. In addition, in the event that an MO does not comply with section 1.7 and it is detected during on-site inspection, the Commission shall apply the appropriate sanctions against the MO.

1.12 EXISTING CUSTOMERS

a. MOs shall apply CDD requirements to existing customers on the basis of materiality and risk and continue to conduct due diligence on such existing relationships at appropriate times.

b. An MO shall conduct CDD where:

i. A transaction of significant value takes place,or

ii. Customer documentation standards change substantially,or

iii. There is a material change in the way that the account is operated, or

iv. The MO becomes aware that it lacks sufficient information about an existing customer.

An MO shall identify the customer in accordance with the above mentioned criteria and make the records available to the AMLRO and competent authorities.

1.13 POLITICALLY EXPOSED PERSONS (PEPs)

a. An MO shall, in addition to performing CDD procedures, put in place appropriate risk management systems to determine whether a potential customer or existing customer or the beneficial-owner is a politically exposed person.

b. An MO shall ensure that its senior management gives approval before it establishes a business relationship with a PEP.

c. Where a customer has been accepted or has an ongoing relationship with the MO and the customer or beneficial-owner is subsequently found to be or becomes PEP, the MO shall obtain senior management approval in order to continue the business relationship.

An MO shall take reasonable measures to establish the sources of wealth and funds of customers and beneficial-owners identified as PEPs and report all anomalies immediately to the FIC, SEC and the relevant competent authorities.

d. MOs in business relationships with PEPs are required to conduct enhanced ongoing monitoring of that relationship. In the event of any transaction that is unusual, MOs are required to flag the account and to report immediately to the FIC , SEC and the relevant competent authorities.

1.14 NEW TECHNOLOGIES AND NON-FACE-TO-FACE TRANSACTIONS

a. An MO shall have policies in place or take such measures as may be needed to prevent the misuse of technological developments in ML/TF&PF schemes such as internationally accepted credit or debit cards, mobile telephone banking, transactions in virtual assets, financial technology (FINTECH) and other technology.

b. MOs shall have policies and procedures in place to identify and address any risks associated with non-face-to-face business relationships or transactions. These policies and procedures shall be applied when establishing customer relationships and in conducting ongoing due diligence.

1.15 RELIANCE ON INTERMEDIARIES AND THIRD PARTIES ON CDD FUNCTION

a. An MO that relies on intermediaries or other third parties who has no outsourcing or agency relationships, business relationships, accounts or transactions for its clients shall be required to perform some of the elements of the CDD process on the introduced business including:

i. Immediately obtaining from the third party the necessary information concerning certain elements of the CDD process;

ii. Taking adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;

iii. Satisfying themselves that the third party is regulated and supervised in accordance with principles of AML/CFT & PF and has measures in place to comply with the CDD requirements set out in these Guidelines;

iv. In determining which countries the third party that meet the conditions can be based, MOs should have regard to information available on the level of country risk; and

v. Making sure that adequate KYC provisions are applied to the third party in order to get account information for competent authorities.

b. Where an MO relies on a third party which is part of the same financial group, the MO shall ensure that the requirements of the criteria above are met in the following circumstances:

i. The group applies CDD and record keeping requirements in line with FATF Recommendations 10 and 11 and programmes against money laundering and terrorist financing, in accordance with FATF Recommendation 18;

ii. The implementation of those CDD, record keeping requirements and AML/CFT & PF programmes are supervised at a group level by the competent authority; and

iii. Any higher country risk is adequately mitigated by the group's AML/CFT & PF

policies.

c. Without prejudice to the above, An MO, that relies on the third party for a CDD shall have ultimate responsibility for customer identification and verification.

1.16 AML/CFT & PF EMPLOYEE EDUCATION AND TRAINING PROGRAMME

a. An MO shall design comprehensive employee education and training programmes to make all employees fully aware of their obligations and equip them with relevant skills required for the effective discharge of their AML/CFT & PF obligations.

b. An MO shall submit its annual AML/CFT & PF employee training programme for the ensuing year to the SEC and FIC not later than the 31st of December every financial year.

c. The employee training programme shall be developed by management with support of the AMLRO and approved by the Board.

The training programme shall include:

- **i.** AML/TF&PF regulations and offences
- **ii.** The nature of money laundering
- **iii.** ML/TF&PF 'red flags' and suspicious transactions, including trade-based money laundering typologies
- **iv.** Reporting requirements
- **v.** Customer due diligence
- **vi.** Risk-based approach to AML/CFT & PF Regime
- **vii.** Record keeping and retention policy
- **viii.** Training on SEC/FIC AML/CFT&PF Guidelines and Administrative Sanctions
- **ix.** Other emerging ML/TF&PF risks.

d.MOs shall fully participate in all AML/CFT & PF programmes or activities organized by SEC in collaboration with FIC, ACAMRO and other bodies. Failure to participate shall attract sanctions from SEC.

1.17 MONITORING OF EMPLOYEE CONDUCT

a. An MO shall monitor its employees' accounts for potential signs of ML/TF&PF and subject employees' accounts, including accounts of key management personnel, to the same AML/CFT & PF procedures.

b. The AMLRO's account shall be reviewed by the Internal Auditor.

c. Any findings on the employees' account including the AMLRO's account shall be submitted to the SEC and FIC immediately.

1.18 WHISTLE BLOWING/ PROTECTION OF STAFF WHO REPORT AML/CFT & PF VIOLATIONS

a. An MO shall direct its employees in writing to co-operate fully with the Regulators and Law Enforcement Agencies. A director or employee shall report any violations of the MO's AML/CFT & PF compliance programme to the AMLRO or a designated higher authority where the violation involves the AMLRO.

b. An MO shall ensure compliance with the Whistleblower Act, 2006 (Act 720) with respect to protection for making disclosure of impropriety.

1.19 MAINTENANCE OF RECORDS ON TRANSACTIONS

a. An MO shall maintain records of transactions, both domestic and international, for at least seven (7) years after completion of the transaction to which they relate.

b. An MO shall ensure that all customers' transaction records and information are available on a timely basis to the SEC and the FIC.

1.20 TESTING FOR THE ADEQUACY OF THE AML/CFT & PF COMPLIANCE PROGRAMME

a. An MO shall make a policy commitment and subject its AML/CFT&PF compliance programme to independent testing, to determine its adequacy, completeness and effectiveness.

b. Where an independent testing is conducted, it shall be done by an internal auditor, external auditor, or a consultant with knowledge in AML/CFT&PF.

c. The independent testing shall not be performed by persons involved with the MO's AML/CFT & PF Compliance function.

d. The independent testing shall be performed every two (2) years.

e. Report on the testing shall be submitted to the MO's Board of Directors or to a designated board committee and copies submitted to the SEC and FIC not later than 31st December of the year in which it was conducted.

f. Any identified weaknesses or inadequacies shall be promptly addressed by the MO.

1.21 SHELL COMPANIES

a. These are companies which have no physical presence in any country. MOs are not allowed to establish correspondent relationships with high-risk foreign companies (e.g. shell companies) with no physical presence in any country or with correspondent institutions that permit their accounts to be used by such companies.

b. MOs shall take all necessary measures to satisfy themselves that respondent MOs in a foreign country do not permit their accounts to be used by shell companies.

1.22 ATTENTION TO HIGH RISK COUNTRIES

a. An MO shall give special attention to business relationships and transactions with persons (including legal persons and arrangements) from or in countries which do not or insufficiently apply the FATF recommendations.

b. An MO shall report, as stated below, transactions that have no apparent economic or visible lawful purpose. The background and purpose of such transactions shall, as far as possible, be examined and findings made available to assist auditors and competent authorities such as SEC, FIC, and Law Enforcement Agencies (LEAs) to carry out their duties.

c. An MO that does business with foreign institutions which do not continue to apply or insufficiently apply the provisions of FATF Recommendations, shall take measures including:

i. Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories to MOs for identification of the beneficial owners before business relationships are established with individuals or companies from those jurisdictions;

ii. Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious;

iii. Warning non-financial sector businesses that transactions with natural or legal persons within those countries might run the risk of ML/TF&PF; and

iv. Limiting business relationships or financial transactions with the identified countries or persons in those countries.

1.23 FOREIGN BRANCHES AND SUBSIDIARIES

a. An MO shall ensure that their foreign branches and subsidiaries or parents observe group AML/CFT & PF procedures consistent with the provisions of these Guidelines and to apply them to the extent that the local/host country's laws and regulations permit.

b. MOs shall ensure that the above principle is observed with respect to their branches and subsidiaries in countries which do not or insufficiently apply such requirements as contained in these Guidelines. Where these minimum AML/CFT & PF requirements and those of the host country differ, branches and subsidiaries or parent of Ghanaian MOs in the host country are required to apply the higher standard and such must be applied to the extent that the host country's laws, regulations or other measures permit.

c. An MO shall inform the SEC in writing when its foreign branches or subsidiaries or parent is unable to observe the appropriate AML/CFT & PF procedures because they are prohibited by the host country's laws, regulations or other measures.

d. An MO is subject to these AML/CFT & PF principles, and shall apply consistently the CDD procedures at their group level, taking into account the activity of the customer with the various branches and subsidiaries.

e. Financial groups shall implement group-wide programmes against ML/TF&PF which shall be applicable and appropriate to all branches and majority-owned subsidiaries of the financial group. These measures include:

i. Compliance management arrangements (including the appointment of a compliance officer at the management level)
ii. Screening procedures to ensure high standards when hiring employees
iii. Ongoing employee training programme
iv. An independent audit function to test the system
v. Policies and procedures for sharing information required for the purpose of CDD and ML/TF & PF risk management
vi. The provision at group level compliance, audit and/or AML/CFT & PF functions of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT & PF purposes.
vii. Branches and subsidiaries receiving information from group level functions when the information is relevant and appriopriate to risk management.
viii. The fact that tipping-off provisions should not inhibit information sharing in the group.
ix. Adequate safeguards on the confidentiality and use of information exchanged including safeguards to prevent tipping-off.

f. An MO is subject to these AML/CFT & PF principles and shall apply consistently the CDD procedures at their group level, taking into account the activity of the customer with the various branches and subsidiaries.

1.24 ADDITIONAL PROCEDURES AND MITIGANTS

a. An MO shall review the AML/CFT & PF framework and identify new areas of potential money laundering vulnerabilities and risks, and design additional procedures and mitigants as contingency plan in its AML/CFT & PF Compliance Programme.

b. Details of the contingency plan shall be submitted to the SEC and FIC not later than 31st December of every financial year.

1.25 AML/CFT & PF COMPLIANCE PROGRAMME

a. The Board of an MO shall retain ultimate responsibility for the AML/CFT & PF compliance.

b. An MO shall have a comprehensive AML/CFT compliance programme approved by the Board. (Refer to Appendix H and Section 49 of Act 1044)

c. An MO shall submit copies of the approved Compliance Programme to the Commission within one (1) month of the release of the document.

d. Quarterly reports on the AML/CFT & PF compliance status of the MO shall be presented to the Board for its information and necessary action.

1.26 CULTURE OF COMPLIANCE

An MO shall establish a culture of compliance to minimize the risks of being used to launder the proceeds of crime and provide protection against fraud as well as reputational and financial risks.

1.27 TERRORIST FINANCING & FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

A person who willfully provides or collects funds by any means, directly or indirectly, with the intention that they shall be used, or in the knowledge that they are to be used, in full or in part to carry out a terrorist act by a terrorist organization or by an individual terrorist commits a Terrorist financing offence in accordance with the Anti-Terrorism Act, 2008 (Act 762) (as amended).

REPORTING REQUIREMENTS

a. An MO shall submit the following reports:

i. Fraud and defalcation report to SEC and FIC as and when they are detected;

ii. FIC semi-annual compliance report to SEC and FIC

iii. FIC end of year compliance report to SEC and FIC

iv. Semi-annual SEC Data Capture returns to SEC.

v. Semi-annual SEC Risk Management returns to SEC

vi. End of year AML/CFT& PF employee education and training report to the SEC and FIC

vii. End of year Contigency plan report to be submitted to SEC and FIC

2.0 PART B

2.1 KNOW YOUR CUSTOMER (KYC) PROCEDURES

An MO shall not establish a business relationship until all relevant parties to the relationship have been identified and the nature of the business they intend to conduct ascertained.

Where an on-going business relationship is established, any inconsistent activity shall be examined to determine whether or not there is an element of ML/TF/PF.

2.2 DUTY TO OBTAIN IDENTIFICATION EVIDENCE

a. An MO shall conduct know your customer procedures to ascertain the identity of a prospective customer.

b. In the case of a person acting on behalf of another, the MO shall be obliged to obtain sufficient evidence of identities of the two persons involved.

c. An MO has a duty to obtain evidence in respect of its customers except under 2.5.1. (c) of these Guidelines.

2.3 NATURE AND LEVEL OF THE BUSINESS

a. An MO shall obtain sufficient information on the nature of the business its customers intend to undertake, including the expected or predictable pattern of transactions.

The information collected shall include:

- **i.** The purpose and reason for opening the account or establishing the relationship;
- **ii.** Nature of the activity that is to be undertaken;
- **iii.** Expected origin of the funds to be used during the relationship and
- **iv.** Details of occupation/employment/business activities and sources of wealth or income.

b. An MO shall take steps to keep the information up to date. Information obtained during any meeting, discussion or other communication with the customer shall be recorded and kept in the

customer's file to ensure that current customer information is readily accessible to the AMLRO or relevant competent authorities.

2.4 COMMERCIAL JUDGMENT

a. An MO shall take a risk-based approach to the KYC requirements.

b. An MO shall determine and record the number of times to verify the customers' records during the relationship, the identification evidence required and when additional checks are needed.

c. A holder of a personal account including joint-accounts holders shall be verified.

d. In respect of a private company or a partnership, the identities of the principal owners/controllers shall be verified.

e. The identification evidence collected shall be viewed against the inherent risks in the business or service.

2.5 ESTABLISHMENT OF IDENTITY

a. The customer identification process shall not end at the point of establishing the business relationship but shall continue as far as the business relationship subsists. The process of confirming and updating identity and address, and the extent of obtaining additional KYC information collected may however differ from one type of MO to another.

b. The general principles for establishing the identity of both legal and natural persons and the procedures on obtaining satisfactory identification evidence set out in these Guidelines are by no means exhaustive.

2.5.1. VERIFICATION OF IDENTITY

a. Identity shall be verified whenever a business relationship is to be established, on account opening or during one-off transaction or when series of linked transactions take place.

b. Once identification procedures have been satisfactorily completed and the business relationship established, as long as contact or activity is maintained and records concerning that customer are complete and kept, no further evidence of identity is needed when another transaction or activity is subsequently undertaken.

c. In the case of a natural person, the date of birth shall be obtained as an important identifier in support of the name. It is, however, not mandatory to verify the date of birth provided by the

customer. Where an international passport, national identity card, or any other acceptable identification as provided in these Guidelines are taken as evidence of identity, the number, date and place/country of issue (as well as expiry date where applicable) shall be recorded.

d. Where the customer is acting on behalf of another (i.e. the funds are supplied by someone else or the investment is to be held in the name of someone else), the MO shall verify the identity of both the customer and the third party (agents, trustees, nominees).

e. In the case of syndicated transactions, the syndicate lead shall supply a confirmation letter as evidence that it has obtained the required identity of members of the syndicate.

f. The MO may not look beyond the client where:

i. The agent is acting on its own account (rather than for a specific client or group of clients);

ii. The client is a bank, broker, fund manager or another regulated MO and

iii. All the businesses are to be undertaken in the name of a regulated MO.

h. Where the client is an MO acting as agent on behalf of one or more clients within Ghana, and has given written assurance that it has obtained the recorded evidence of identity to the required standards, identification evidence shall be verified for:

i. The named account holder/person in whose name an investment is registered;

ii. Any principal beneficial owner of funds being invested who is not the account holder or named investor;

iii. The principal controller(s) of an account or business relationship (i.e. those who regularly provide instructions); and

iv. Any intermediate parties (e.g. where an account is managed or owned by an intermediary).

i. An MO shall take appropriate steps to identify directors and all the signatories to an account.

j. Where it is a joint account, identification evidence shall be obtained for the account holders.

k. In the case of high risk private companies (i.e. those not listed on the securities exchange) evidence of identity and address shall be verified in respect of the principal underlying beneficial owner(s) of the company in accordance with the threshold as set in the Companies Act, 2019 (Act 992).

l. An MO shall be alert to circumstances that might indicate any significant changes in the nature of the business or its ownership and make enquiries accordingly and to observe the additional provisions for High Risk Categories of customers as provided in these Guidelines.

m. Where it is a trust account, An MO shall obtain and verify the identity of those providing funds for the trust, including the settlor and those who are authorized to invest, transfer funds or make decisions on behalf of the trust such as the principal trustees and controllers who have power to remove the trustees.

2.6 REDEMPTIONS

a. Where an investor redeems his investment (wholly or partially), the identity of the investor shall be verified and recorded where it had not been done previously.

b. An MO shall take reasonable measures to establish the identity of the investor where payment is made to:

i. The legal owner of the investment by means of a cheque crossed "account payee only" or

ii. A bank account held (solely or jointly) in the name of the legal owner of the investment by any electronic means for transfer of funds.

2.7 INVESTMENT SCHEMES AND INVESTMENTS IN THIRD PARTY NAMES

Where an investor sets up an investment account or a regular investment scheme whereby the funds are supplied by one person for investment in the name of another (such as a spouse or a child), the person who funds the subscription or makes deposits into the investment accounts shall be regarded as the applicant for business for whom identification evidence must be obtained in addition to the beneficiary.

2.8 PERSONAL PENSION SCHEMES

a. Identification evidence shall be obtained at the outset for investors, except personal pensions connected to a policy of insurance taken out by virtue of a contract of employment or pension scheme.

b. Personal Pension Advisers (PPA) are charged with the responsibility of obtaining the identification evidence on behalf of the pension fund provider. MOs shall demand confirmation of identification evidence given on the transfer of a pension to another provider.

2.9 TIMING OF IDENTIFICATION REQUIREMENTS

a. An acceptable time-span for obtaining satisfactory evidence of identity shall be determined by the nature of the business, the geographical location of the parties and whether it is possible to obtain the evidence before commitments are entered into or money changes hands. However, any occasion when business is conducted before satisfactory evidence of identity has been obtained must be exceptional and shall be justified with regard to the risk.

b. Subject to 2.9 (a) above An MO shall:

i. Obtain identification evidence as soon as reasonably practicable after it has contact with a client with a view to agreeing with the client to carry out an initial transaction; or reaching an understanding (whether binding or not) with the client that it may carry out future transactions; and

ii. Where the client does not supply the required information as stipulated in (a) above, the MO shall immediately discontinue any activity it is conducting for the client; and bring to an end any understanding reached with the client.

c. An MO shall also observe the provision in the Timing of Verification under the AML/CFT & PF under these Guidelines.

d. An MO may start processing the business or application immediately, provided that it:

i. Promptly takes appropriate steps to obtain identification evidence and;

ii. Does not transfer or pay any money out to a third party until the identification requirements have been satisfied.

e. The failure or refusal by an applicant to provide satisfactory identification evidence within a reasonable time frame without adequate explanation may lead to a suspicion that the investor or client is engaged in ML/TF&PF. The MO shall therefore submit an STR to the FIC based on the information in its possession.

f. An MO shall have in place written and consistent policies of closing an account or unwinding a transaction where satisfactory evidence of identity cannot be obtained.

g. An MO shall respond promptly to enquiries made by competent authorities.

2.10 CANCELLATION & COOLING-OFF RIGHTS

Where an investor exercises cancellation rights or cooling-off rights, the sum invested must be repaid. Since cancellation/cooling-off rights could offer readily available route for ML, MOs shall

be alert to any abnormal exercise of these rights by an investor or in respect of business introduced through an intermediary. In the event where abnormal exercise of these rights becomes apparent, the matter shall be treated as suspicious and reported to the FIC.

2.11 IDENTIFICATION PROCEDURES

GENERAL PRINCIPLES

a. An MO shall ensure that it is dealing with a "real" person or organization (natural or business entity) by obtaining sufficient identification evidence. Where reliance is being placed on a third party to identify or confirm the identity of an applicant, the overall responsibility for obtaining satisfactory identification evidence rests with the account holding MO.

b. The requirement in all cases is to obtain satisfactory evidence that a person of that name lives at the address given and that the applicant is that person or that the company has identifiable owners and that its representatives can be located at the address provided.

c. A single form of identification cannot be fully guaranteed as genuine or representing correct identity therefore the identification process may be cumulative.

d. The procedures adopted to verify the identity of private individuals and whether or not identification was done face to face or remotely shall be stated in the customer's file. The reasonable steps taken to avoid single, multiple fictitious applications, impersonation or fraud shall be stated by the MO.

e. An introduction from a known customer, a person personally known to a Director or Manager or a member of staff may provide comfort but shall not replace the need for identification evidence requirements to be complied with as set out in these Guidelines. Details of the person who initiated and authorized the introduction shall be kept in the customer's mandate file along with other records. It is therefore mandatory that Directors/Senior Managers shall insist on following the prescribed identification procedures for every applicant.

NEW BUSINESS FOR EXISTING CUSTOMERS

a. Where an existing customer closes one account and opens another or enters into a new agreement to purchase products or services, there is no need to verify the identity or address for

such a customer unless the name or the address provided does not tally with the information in the MO's records. However, procedures shall be put in place to guard against impersonation or fraud.

b. The customer shall be required to confirm the relevant details and to provide any missing KYC information, particularly where:

- **i.** an existing business relationship with the customer and identification evidence had not previously been obtained; or
- **ii.** there had been no recent contact or correspondence with the customer within the past twelve (12) months; or
- **iii.** a previously dormant account is re-activated.

c. In the circumstances above, details of the previous account(s) and any identification evidence previously obtained or any introduction records shall be linked to the new account records and retained for the prescribed period in accordance with the provision of these Guidelines.

2.13 CERTIFICATION OF IDENTIFICATION DOCUMENTS

a. An MO shall not require a prospective customer to send by post originals of valuable personal identity documents.

b. Where there is no face to face contact with the customer and documentary evidence is required, copies certified by a lawyer, notary public/court of competent jurisdiction, senior public servant or their equivalent in the private sector shall be obtained. The person undertaking the certification must be known and capable of being contacted if necessary.

c. In the case of foreign nationals, the copy of international passport, national identity card or documentary evidence of his/her address shall be certified by:

i. The embassy, consulate or high commission of the country of issue; or

ii. A lawyer, attorney or notary public.

d. Certified copies of identification evidence are to be stamped, dated and signed "original sighted by me" by an authorized officer of the MO. MOs shall always ensure that a good production of the photographic evidence of identity is obtained. Where this is not possible, a copy of evidence certified as providing a good likeness of the applicant could only be acceptable in the interim.

2.14 RECORDING IDENTIFICATION EVIDENCE

a. An MO shall keep record of the supporting evidence and methods used to verify identity for a minimum period of seven (7) years after the account is closed or the business relationship has ended.

b. Where the supporting evidence could not be copied at the time it was presented, the reference numbers and other relevant details of the identification evidence shall be recorded to enable the documents to be obtained later. Confirmation shall be provided that the original documents were seen by certifying either on the photocopies or on the record that the details were taken down as evidence.

c. Where checks are made electronically, a record of the actual information obtained or of where it can be re-obtained must be retained as part of the identification evidence.

d. An MO may appoint a person to keep records on its behalf and shall within seven days, inform the SEC and FIC of the appointment in writing.

e. Despite subsection (d), ultimate responsibility to comply with the requirements of this section shall not be delegated and remains at all times with the MO that relied on the appointed person.

f. MOs shall not outsource record keeping to a third party in another jurisdiction where that jurisdiction is listed in domestic and international sanctions lists.

2.15 CONCESSION IN RESPECT OF POSTAL AND ELECTRONIC PAYMENTS SYSTEMS

a. An MO may not require further evidence of identity for products or services, where the ML/TF/PF risk is considered to be low, in respect of purchase of investment products where payment is to be made from an account held in the customer's name (or jointly with one or more other persons) with an MO's .

b. Waiver of additional verification requirements for postal or electronic transactions does not apply to the following:

i. Products or accounts where funds can be transferred to other types of products or accounts which provide cheque or money transfer facilities;

ii. Situations where funds can be repaid or transferred to a person other than the original customer;

iii. Investments where the characteristics of the product or account may change subsequently to enable payments to be made to third parties.

c. Postal concession is not an exemption from the requirement to obtain satisfactory evidence of a customer's identity. Payment debited from an account in the customer's name shall be capable of constituting the required identification evidence in its own right.

d. Where a customer uses a third-party cheque, draft or electronic payment drawn on a bank, the MO may rely upon the required documentary evidence of the third party, without further verification of the identity, except where there is apparent inconsistency between the name in which the application is made and the name on the payment instrument. The name of the account-holder(s) from where the funds have been provided shall be clearly indicated on the record reflecting the payment/ receipt.

e. Where payment for a product is to be made by direct debit or debit card/notes, and the applicant's account details have not previously been verified through sighting of a bank statement or cheque drawn on the account, repayment proceeds shall be returned to the account from which the debits were drawn.

f. Records shall be maintained indicating how a transaction arose, including details of the MO's branch and the account number from which the cheque or payment is drawn.

g. The concession can apply both where an application is made directly to the MO and where a payment is passed through a regulated intermediary.

h. An MO that has relied on the postal concession to avoid additional verification requirements, which must be so indicated on the customer's file, cannot introduce the customer to another MO for the purpose of offering accounts or other products that provide cheque or money transmission facilities.

i. Where a customer wishes to migrate to an account that provides cheque or third-party transfer facilities, then additional identification checks must be undertaken at that time. Where these circumstances occur on a regular basis, MOs shall identify all the parties to the relationship at the outset.

2.16 TRANSFER OF INVESTMENT FUNDS

Where the balance in an investment fund's account is transferred from one MO to another and identification evidence has neither been taken nor confirmation obtained from the original MO, then such evidence shall be obtained at the time of the transfer.

2.17 ESTABLISHING IDENTITY

Establishing identity under these Guidelines are divided into four broad categories:

- **i.** Private individual customers;
- **ii.** Quasi corporate customers;
- **iii.** Unincorporated businesses/partnerships; and
- **iv.** Corporate customers.

2.18 PRIVATE INDIVIDUALS

GENERAL INFORMATION

a. The following information is to be established and independently validated for all private individuals whose identities need to be verified:

- **i.** The full name(s) used; and
- **ii.** The permanent home address, including landmarks and postcode, where available.

b. The information obtained shall provide satisfaction that a person of that name exists at the address given and that the applicant is that person. Where an applicant has recently relocated, the previous address shall be validated.

c. date of birth may be required to confirm identity.

However, the information need not be verified. It is also important for the residence/nationality of a customer to be ascertained to assist risk assessment procedures.

d. A risk-based approach shall be adopted when obtaining satisfactory evidence of identity. The extent and number of checks can vary depending on the perceived risk of the service or business sought and whether the application is made in person or through a remote medium such as telephone, post or the internet. The source of funds of how the payment was made, from where and by whom must always be recorded to provide an audit trail.

However, for higher risk products, accounts or customers, additional steps shall be taken to ascertain the source of wealth/funds.

e. For low-risk accounts or investment products such as investment accounts without cheque-books or automated money transmission facilities, there is an overriding requirement for the MO to satisfy itself as to the identity and address of the customer.

2.19 PRIVATE INDIVIDUALS RESIDENT IN GHANA

a. The confirmation of name and address shall be established by reference to a number of sources. The checks shall be undertaken by cross-validation that the applicant exists at the stated address either through the sighting of actual documentary evidence or by undertaking electronic checks of suitable databases, or by a combination of the two. The overriding requirement to ensure that the identification evidence is satisfactory rests with the MO opening the account or providing the product/service.

b. Where an individual is unable to provide a photo-bearing identity document, an MO may accept other non-photo bearing document which shall have an authenticated passport-size photograph affixed to the certificate or document.

2.20 DOCUMENTING EVIDENCE OF IDENTITY

In order to guard against forged or counterfeit documents, care shall be taken to ensure that documents offered are originals. Copies that are dated and signed 'original sighted by me' by a senior public servant or equivalent in a reputable private organization may be accepted in the interim, pending presentation of the original documents within six (6) months. Acceptable documentary evidence for private individuals resident in Ghana are:

a. Valid Passport

b. Resident Permit issued by the Ghana Immigration Service

c. Valid Driver's License issued by the Driver, Vehicle and Licensing Authority (DVLA)

d. National Identity Card

e. Birth Certificate

f. Voters ID

g. SSNIT Biometric Card

2.21 DOCUMENTARY EVIDENCE OF ADDRESS

a. Acceptable documentary evidence for address include

i. Record of home visit by the MO

ii. Confirmation from the electoral register that a person of that name lives at that address

iii. Recent utility bill - including Water, Electricity and Telephone bills

iv. Property Rate bill

v. Bank statement or passbook containing current address

vi. Solicitor's letter confirming recent house purchase or search report from the Lands Commission

vii. Tenancy Agreement

viii. Search reports on prospective customer's place of employment and residence signed by an AMLRO of the MO.

ix. Letter from a Public Authority/Statutory Declaration

x. State/Local Government Rates documents

b. Checking of a local or national telephone directory may be used as additional corroborative evidence and this shall not be used as a primary check.

2.22 PHYSICAL CHECKS ON PRIVATE INDIVIDUALS RESIDENT IN GHANA

a. An MO shall establish the true identity and address of its customers.

b. Additional confirmation of the customer's identity shall be obtained through one or more of the following procedures:

i. A direct mailing of account opening documentation to a named individual at an independently verified address;

ii. An initial deposit cheque drawn on a personal account with another MO in Ghana in the applicant's name ;

iii. Telephone contact with the applicant prior to opening the account on an independently verified home or business number or a "welcome call" to the customer before transactions are permitted, utilizing a minimum of two pieces of personal identity information that had been previously provided during the setting up of the account;

iv. Internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which had been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address; and

v. Card or account activation procedures.

c. MOs shall ensure that additional information concerning the nature and level of the business to be conducted and the origin of the funds to be used during the relationship are also obtained from the customer.

2.23 ELECTRONIC CHECKS

a. The applicant's identity, address and other available information may be checked electronically by accessing other databases or sources, and each source may be used separately as an alternative to one or more documentary checks.

b. An MO shall use a combination of electronic and physical checks to confirm different sources of the same information provided by its customers.

c. Reliability of information supplied shall be established by cumulative checks across a range of sources, covering a period of time or through qualitative checks that assess the validity of the information supplied.

d. The number or quality of checks to be undertaken may vary depending on the diversity, breadth and depth of information available from each source. The MO shall ensure that the applicant is the data-subject and the same as the physical person being verified which shall be consistent with attributes such as name, age, gender of the person in the database.

e. electronic sources of information may include:

- **i.** An electronic search of the Electoral Register (is not to be used as a sole identity and address check);
- **ii.** Access to internal or external account database; and
- **iii.** An electronic search of public records where available.

2.24 PRIVATE INDIVIDUALS NOT RESIDENT IN GHANA

a. International passports or national identity cards may be acceptable as evidence for prospective customers not resident in Ghana but make face-to-face contact with An MO. Reference numbers,

date and country of issue shall be obtained and the information recorded in the customer's file as part of the identification evidence.

b. An MO shall obtain separate evidence of the applicant's permanent residential address from the best available official source. A "P.O. Box number" alone is not acceptable as evidence of address. The applicant's residential address shall be such that it can be physically located by way of a recorded description or other means.

c. An MO shall obtain evidence directly from the customer or through a credit institution or MO in the applicant's home country or country of residence. However, particular care must be taken when relying on identification evidence provided from other countries. An MO shall ensure that the customer's true identity and current permanent address are actually confirmed. In such cases, copies of relevant identity documents shall be sought and retained.

d. Where a foreign national arrives in Ghana, reference may be made to his/her employer, educational institutions, evidence of traveling documents to verify the applicant's identity and residential address.

2.25 PRIVATE INDIVIDUALS NOT RESIDENT IN GHANA: SUPPLY OF INFORMATION

a. An MO shall use a risk-based approach where a private individual not resident in Ghana, wishes to supply documentary information by post, telephone or electronic means. The MO shall obtain evidence of identity in respect of the name and address of the customer.

b. Documentary evidence of name and address shall be obtained:

- **i.** By way of original documentary evidence supplied by the customer; or
- **ii.** By way of a certified true copy of the customer's passport or national identity card and a separate certified document verifying address e.g. a driving license, utility bill, etc.;

c. Where the applicant does not already have a business relationship with the MO that is supplying the information or the MO is not within Ghana, certified true copies of relevant underlying documentary evidence must be sought, obtained and retained by the MO.

d. Where necessary, an additional comfort shall be obtained by confirming the customer's name, address and date of birth from a reputable credit institution in the customer's home country. An MO shall use these requirements in conjunction with Appendix A to these Guidelines.

2.26 NON FACE-TO-FACE IDENTIFICATION

a. In keeping with the requirements on non-face-to-face customers, or where customers are unable to provide original documentation, an MO shall only accept customer information that has been certified by:

i. The embassy, consulate or high commission of the country of issue; or

ii. A lawyer, attorney or notary public.

b. The identification evidence required shall depend on the nature and characteristics of the product or service and the assessed risk. The MO shall ensure that the same level of information is obtained from customers who use the internet or the post/telephone.

c. Where reliance is placed on intermediaries to undertake the processing of applications on the customer's behalf, checks shall be undertaken to ensure that the intermediaries are regulated for ML/ TF&PF prevention and that the relevant identification procedures are applied. In all cases, evidence as to how identity has been verified shall be obtained and retained with the account opening records.

d. An MO shall conduct regular monitoring of internet-based business/clients. Where a significant proportion of the business is operated electronically, computerized monitoring systems/solutions that are designed to recognize unusual transactions and related patterns of transactions shall be put in place to recognize suspicious transactions, and the AMLRO shall review these systems/solutions, record exemptions and report same half yearly to the SEC and FIC.

2.27 ESTABLISHING IDENTITY FOR REFUGEES AND ASYLUM SEEKERS

a. A refugee or asylum seeker who wishes to open an investment account without being able to provide evidence of identity. In such circumstances, authentic references from the Ministry of the Interior or an appropriate government/international agency should be used in conjunction with other readily available evidence.

b. Additional monitoring procedures shall be undertaken to ensure that the use of the account is consistent with the customer's circumstances and returns submitted half yearly to the FIC.

2.28 ESTABLISHING IDENTITY FOR MINORS

a. When opening accounts for minors, the identification procedures set out in these Guidelines shall be followed. Where such procedures do not provide satisfactory identification evidence, verification could be obtained:

- **i.** Via the home address of the parent(s); or
- **ii.** By obtaining confirmation of the applicant's address from his/her institution of learning; or
- **iii.** By seeking evidence of a tenancy agreement or student accommodation contract.

b. An account for a minor may be opened by a parent or guardian. Where the adult opening the account does not already have an account with the MO, the identification evidence for that adult, or of any other person who will operate the account shall be obtained in addition to the birth certificate or passport of the child. It shall be noted that this type of account could be opened to abuse and therefore strict monitoring shall then be undertaken and maintained.

c. For accounts opened through a school-related scheme, the school shall provide the date of birth and permanent address of the student and to complete the standard account opening documentation on behalf of the student.

2.29 QUASI CORPORATE CUSTOMERS

2.29.1 ESTABLISHING IDENTITY – TRUSTS, NOMINEES AND FIDUCIARIES

a. An MO shall adopt identification and "Know Your Customer Business" procedures to manage trusts, nominees and fiduciary accounts according to the perceived risks

b. In the case of trusts, nominees and fiduciaries, the MO shall verify the identity of the provider of funds such as the settlor and those who have control over the funds.

c. In the case of discretionary or offshore trust, the nature and purpose of the trust and the original source of funding shall be ascertained.

d. An MO is ultimately responsible for identity checks of a customer where it relies on another MO to undertake the identity checks.

e. Identification requirements shall be obtained and not waived for any trustee who does not have authority to operate an account and cannot give relevant instructions concerning the use or transfer of funds.

2.29.2 OFFSHORE TRUSTS

a. An MO shall perform additional checks where Trusts or Special Purpose Vehicles (SPVs) and international business companies connected to trusts are set up in offshore locations with strict bank secrecy or confidentiality rules and without equivalent ML/TF/PF procedures.

b. An MO shall obtain evidence of identity for a trust company or a corporate service provider where the applicant for business is not a regulated MO.

c. An MO shall obtain certified true copies of evidence of identity for the underlying principals such as settlors and controllers on whose behalf the applicant for business is acting.

d. Where the applicant is itself an MO that is regulated for ML/TF&PF purposes for overseas trusts, nominee and fiduciary accounts:

- **i.** Reliance can be placed on an introduction or intermediary certificate or letter stating that evidence of identity exists for all underlying principals and confirming that there are no anonymous principals;
- **ii.** The trustees/nominees shall be asked to state from the onset the capacity in which they are operating or making the application;
- **iii.** Documentary evidence of the appointment of the current trustees shall also be obtained.

e. Where the underlying evidence is not retained within Ghana, enquiries shall be made to determine that there are no overriding MO secrecy or confidentiality constraints that will restrict access to the documentary evidence of identity, shall it be needed in Ghana.

f. An application to open an account or undertake a transaction on behalf of another without the applicant's identifying the trust or nominee capacity shall be regarded as suspicious and shall lead to further enquiries and submission of reports to the FIC.

g. Where an MO in Ghana is itself the applicant to an offshore trust on behalf of a customer, where the corporate trustees are not regulated, then the Ghanaian MO shall undertake the due diligence on the trust itself.

h. Where funds have been drawn on an account that is not under the control of the trustees, the identity of the authorized signatories and their authority to operate the account shall also be

verified. Where the identity of beneficiaries has not previously been verified, verification shall be undertaken when payments are made to them.

2.29.3 CONVENTIONAL FAMILY AND ABSOLUTE GHANAIAN TRUSTS

a. In the case of conventional Ghanaian trusts, identification evidence shall be obtained for:

- **i.** Those who have control over the funds (the principal trustees who may include the settlor);
- **ii.** The providers of the funds (the settlors, except where they are deceased); and
- **iii.** Where the settlor is deceased, written confirmation shall be obtained for the source of funds (grant of probate or copy of the Will or other document creating the trust).

b. Where a corporate trustee such as an MO acts jointly with a co-trustee, any non-regulated co-trustees shall be verified even if the corporate trustee is covered by an exemption. The relevant procedure contained in the Guidelines for verifying the identity of persons, institutions or companies shall be followed.

c. Where an MO is not required to review an existing trust, confirmation of the settlor and the appointment of any additional trustee(s) shall be obtained.

d. An MO shall ensure that copies of any underlying documentary evidence shall be certified as true copies and carry out checks to ensure that any investment account on which the trustees have drawn funds is in their names. Any additional authorized signatories to the investment account shall also be verified.

e. Where payment is made directly to beneficiaries on receiving a request from the trustees, the payment shall be made to the named beneficiary by way of a crossed cheque marked “account payee only” or a bank transfer direct to an account in the name of the beneficiary.

2.29.4 RECEIPT AND PAYMENT OF FUNDS

Where money is received or payment is made on behalf of a trust, an MO shall take reasonable steps to ensure that:

i. the source of the funds is properly identified;
ii. the nature of the transaction or instruction is understood; and
iii. payments are properly authorized in writing by the trustees.

2.29.5 IDENTIFICATION OF NEW TRUSTEES

Where a trustee who has been verified is replaced, the identity of the new trustee shall be verified before he/she is allowed to exercise control over the funds.

2.29.6 POWER OF ATTORNEY AND THIRD PARTY MANDATES

a. The MO shall obtain identification evidence from holders of power of attorney and third party mandates in addition to that of the customer.
b. The MO shall obtain identification evidence for holders of power of attorney for corporate or trust business ascertain the reason for granting of the power of attorney.
c. Records of all transactions undertaken in accordance with the power of attorney shall be maintained as part of the client's record.

2.29.7"CLIENT ACCOUNTS" OPENED BY PROFESSIONAL INTERMEDIARIES

a. A Stockbroker, fund manager, solicitor, accountant, estate agent or any professional intermediary may hold fund, omnibus or singular, on behalf of its clients and shall be distinguished from those where an intermediary introduces a client who himself becomes a customer of the MO.

b. Where the professional intermediary is itself covered and is monitored under the AML/CFT & PF Legislation, identification can be waived on production of evidence.

c. Where the professional intermediary is not covered under the AML/CFT & PF Legislation, the MO shall verify the identity of the professional intermediary and the person on whose behalf the professional intermediary is acting.

d. Where it is impossible for an MO to establish the identity of the person(s) for whom a solicitor or accountant is acting, it will need to take a commercial decision based on its knowledge of the intermediary, as to the nature and extent of business that they are prepared to conduct if the

professional firm is not itself covered by the Guidelines. An MO shall be prepared to make reasonable enquiries about transactions passing through client accounts that give cause for concern and shall report any transaction where suspicions cannot be verified to the FIC.

2.29.8 PARTNERSHIPS

a. Where the applicant is a partnership whose principal partners do not already have a business relationship with the MO, identification evidence shall be obtained for the principal beneficial owners. This shall entail identifying one or more signatories in whom significant control has been vested by the principal beneficial owners.

b. An MO shall obtain evidence of the trading address of the partnership.

c. The nature of the partnership shall be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose. A mandate from the partnership authorizing the opening of an account or undertaking the transaction and conferring authority on those who will undertake transactions shall be obtained.

2.30 CORPORATE CUSTOMERS

2.30.1 GENERAL PRINCIPLES

a. An MO shall verify, from official documents or sources, the legal existence of an applicant-company that represents an organization with complex structures and other legal entities and ensure that persons purporting to act on its behalf are fully authorized. Enquiries shall be made to confirm that the legal person is not merely a "brass-plate company" where the controlling principals cannot be identified.

b. An MO shall identify a corporate body by the following:

- **i.** Registration number;
- **ii.** Registered corporate name and any trading names used;
- **iii.** Registered address and any separate principal trading addresses;
- **iv.** Directors;
- **v.** Shareholders;
- **vi.** The Objectives of the company's business;
- **vii.** Trademarks and logos;

viii. Regulations of the company;

ix. Tax Identification Number (TIN)

2.30.2 NON FACE-TO-FACE BUSINESS

a. Additional procedures shall be undertaken to ensure that the applicant's business, company or society exists at the address provided and it is for a legitimate purpose.

b. Where the characteristics of the product or service permit, the MO shall obtain relevant evidence to confirm that any individual representing the company has the necessary authority to do so. For example power of attorney, board resolution etc.

c. Where the principal owners, controllers or signatories need to be identified within the relationship, the relevant requirements for the identification of personal customers shall be followed.

2.30.3 LOW RISK CORPORATE BUSINESS

2.30.3.1 LISTED COMPANIES

a. An MO shall verify the identity of a shareholder or director of a listed company where there is suspicion

b. An MO shall obtain Board resolution or other authority for any representative acting on behalf of a listed company to confirm that the representative has the authority to act, The MO shall ensure that the individual officer or employee (past or present) does not use the name of the company or the relationship with the MO for unlawful activity. Phone calls can be made to the Chief Executive Officer/or the designated officer of such a company to inform him of the application to open the account.

c. Further steps may not be taken to verify identity over and above the usual commercial checks where the applicant company is listed on the securities exchange; or there is independent evidence to show that it is a wholly owned subsidiary or a subsidiary under the control of such a company.

2.30.3.2 UNQUOTED COMPANIES

a. Where the applicant is an unquoted company and none of the principal directors or shareholders already have an account with the MO, the following documents shall be obtained from an official or recognized independent source to verify the business itself:

- **i.** A copy of the certificate of incorporation/registration, evidence of the company's registered address and the list of shareholders and directors;
- **ii.** A search at the Registrar General's Department or an enquiry via a business information service to obtain the information in (a) above; and
- **iii.** An undertaking from a firm of lawyers or accountants confirming the documents submitted to the Registrar General's Department.

b. Attention shall be paid to the place of origin of the documents and the background against which they were produced. Where comparable documents cannot be obtained, then verification of principal beneficial owners/controllers shall be undertaken.

2.31 HIGH RISK BUSINESS

2.31.1 PUBLIC COMPANIES

a. Where a high-risk business applicant is seeking to enter into a full business relationship where third party funding and transactions are permitted, the following evidence shall be obtained either in physical or electronic form:

- **i.** For established companies (those incorporated for eighteen (18) months or more) a set of the latest annual report shall be produced;
- **ii.** A search report at the Registrar General's Department or an enquiry via a business information service or an undertaking from a firm of lawyers or accountants confirming the documents submitted to the Registrar General's Department;
- **iii.** A certified true copy of the resolution of the Board of Directors to open an account and confer authority on those who will operate it; and
- **iv.** The regulations of the company.

2.31.2 PRIVATE COMPANIES

a. Where a private company is undertaking a high-risk business, the MO in addition to verifying the legal existence of the business shall look behind the corporate entity to identify those who have ultimate control over the business and the company's assets. Evidence of identification shall be obtained for shareholders with interest threshold provided in accordance with the Companies Act, 2019 (Act 992).

b. The MO shall obtain evidence of identification for the principal-beneficiary owner(s) of the company and any other person with principal control over the company's assets. Where the principal owner is another corporate entity or trust, the MO shall look behind that company or vehicle and verify the identity of the beneficial-owner(s) or settlors. An MO shall conduct similar identity checks where there is a change in principal beneficiary owners or controllers.

c. MOs shall also identify directors who are not principal controllers and signatories to an account for risk based approach purpose.

d. The MO may visit the place of business to confirm the existence of business premises and nature of the business activities conducted.

e. Where the MO becomes suspicious due to a change in the nature of the business transacted or the profile of payments through an investment account, further checks shall be made to ascertain the reason for the changes.

f. The MO shall make periodic enquiries to establish whether there have been any changes to controllers, shareholders or to the original nature of the business or activity.

g. An MO shall ensure that full identification and "KYC" requirements are met if the company is an International Business Company (IBC) registered in an offshore jurisdiction and operating out of a different jurisdiction.

2.31.3 FOREIGN MOs

In the case of a foreign MO, confirmation of existence and regulatory status shall be checked by one of the following means:

i. Checking with the home country's Securities Regulator or relevant supervisory body; or

ii. Checking with another office, subsidiary, branch, or correspondent MO in the same country; or

iii. Checking with Ghanaian regulated correspondent MO of the overseas institution; or

iv. Obtaining evidence of its license or authorization to conduct business; or

v. Administrators.

2.32 OTHER INSTITUTIONS

a. Clubs and Societies

i. Where applications are made on behalf of clubs or societies, an MO shall take reasonable steps to satisfy itself as to the legitimate purpose of the organization by sighting its constitution. The identity of all authorized signatories shall be verified initially in line with the requirements for private individuals. The signing authorities shall be structured to ensure that all authorized signatories that authorize any transaction have been verified. When signatories change, MOs shall ensure that the identity of all authorized current signatories are verified.

ii. Where the purpose of the club or society is to purchase the shares of regulated investment company or where all the members would be regarded as individual clients, all the members in such cases are required to be identified in line with the requirements for personal customers. MOs are required to look at each situation on a case-by-case basis.

b. Occupational Pension Schemes

i. In all transactions undertaken on behalf of an occupational pension scheme, where the transaction is not in relation to a long term policy of insurance, the identities of both the principal employer and the trust shall be verified.

ii. In addition to the identity of the principal employer, the source of funding shall be verified and recorded to ensure that a complete audit trail exists if the employer is dissolved or wound up.

iii. In the case of trustees of occupational pension schemes, satisfactory identification evidence can be based on the inspection of formal documents concerning the trust which confirm the names of the current trustees and their addresses for correspondence. In addition to the documents, confirming the trust identification can be based on extracts from public registers or references from professional advisers or investment managers.

iv. Any payment of benefits by or on behalf of the trustees of an occupational pension scheme will not require verification of identity of the recipient.

v. Where individual members of an Occupational Pension Scheme are to be given personal investment advice, their identities shall be verified. However, where the trustees and principal employer have been satisfactorily identified (and the information is still current) it may be appropriate for the employer to provide confirmation of the identity of individual employees.

2.33 CHARITIES

a. An MO shall obtain confirmation of the authority to act in the name of the charity. That confirmation is mandatory.

b. Accounts for charities shall be operated by a minimum of two signatories, duly verified and documentation evidence obtained.

c. An MO shall obtain and confirm the name and address of the charity concerned when dealing with an application from a registered charity.

d. Where the person making the application or undertaking the transaction is not the official correspondent or the recorded alternate, an MO shall obtain written confirmation from the official correspondent of the charity, informing him of the charity's application before it.

e. The official correspondent shall be requested to respond as a matter of urgency especially where there is a reason to suggest that the application has been made without authority.

f. Applications on behalf of un-registered charities shall be dealt with in accordance with procedures for clubs and societies set out in item 2.32 of these Guidelines.

2.34 RELIGIOUS ORGANIZATIONS (ROs)

The MO shall confirm the identity of the religious organization, including its headquarters or regional area of the denomination, from the Registrar General's Department. The identity of at least two signatories to its account shall be verified.

2.35 MINISTRIES, DEPARTMENTS AND AGENCIES (MDAs) AND OTHER PUBLIC INSTITUTIONS

Where the applicant for business is any of the above, the MO shall verify the legal status of the applicant, including its principal ownership and the address. A certified copy of the resolution or other relevant documents authorizing the opening of the account or to undertake the transaction shall be obtained in addition to evidence that the official representing the body has the relevant authority to act. Telephone contacts shall be made with the Chief Executive Officer/or such person designated of the organization concerned, informing him of the application to open the account in the MO.

Appropriate authorization from Controller and Accountant General's Department is a pre-requisite for any of the MDAs and public institutions to open accounts with MOs in Ghana.

2.36 FOREIGN CONSULATES

The authenticity of applicants that request to open accounts or undertake transactions in the name of Ghanaian-resident foreign consulates and documents of authorization presented in support of the application shall be checked with the Ministry of Foreign Affairs or the relevant authorities in the Consulate's home country.

2.37 INTERMEDIARIES OR OTHER THIRD PARTIES TO VERIFY IDENTITY OR TO INTRODUCE BUSINESS

a. Who to rely upon and the circumstances

An MO may rely on another MO to:

- **i.** Undertake the identification procedure when introducing a customer and to obtain any additional KYC information from the client; or
- **ii.** Confirm the identification details if the customer is not resident in Ghana ; or
- **iii.** Confirm that the verification of identity has been carried out (if an agent is acting for underlying principals).

b. Introductions from Authorized Financial Intermediaries

Where an intermediary introduces a customer to an MO the customer shall become the applicant for the business and the identity of the customer shall be verified in line with the requirements provided under these Guidelines.

c. Written Applications

In the case of a written application (unless other arrangements have been agreed that the service provider will verify the identity itself), A financial intermediary shall provide along with each application, the customer's introduction letter together with certified true copies of the evidence of identity which shall be placed in the customer's file.

d. Non-Written Application

An MO receiving non-written applications from financial intermediaries (where a deal is placed over the telephone or by other electronic means) has an obligation to verify the identity of customers and shall ensure that the intermediary provides specific confirmation that identity has been verified.

A record must be made of the answers given by the intermediary and retained for a minimum period of seven (7) years.

e. Introduction from Foreign Intermediaries

Where a business is introduced by a regulated financial intermediary outside Ghana, the reliance that may be placed on that intermediary to undertake the verification of identity check shall be assessed by the Anti-Money Laundering Reporting Officer (AMLRO) or some other competent person within the MO.

f. Financial Group Introductions

Where a customer is introduced by a member of financial group to another member within the financial group, it may not be necessary for identity of the customer to be re-verified or for the records to be duplicated provided that:

- **i.** The identity of the customer has been verified by the introducing parent company, branch, subsidiary or associate in line with the Anti-Money Laundering requirements to equivalent standards and taking account of any specific requirements such as separate address verification;
- **ii.** No exemptions or concessions have been applied in the original verification procedures that would not be available to the new relationship;

iii. A group introduction letter is obtained and placed with the customer's account opening records; and

iv. where the introduction is from a member of a group outside Ghana, the MO shall ensure that the identity of the customer is verified in accordance with requirements and that the underlying records of identity in respect of introduced customers are retained for the necessary period.

g. Where an MO has day-to-day access to all the Group's "KYC" information and records, it may not be necessary to identify an introduced customer or obtain a group introduction letter if the identity of that customer has been verified previously. Where the identity of the customer has not previously been verified, any missing identification evidence shall be obtained and a risk-based approach taken on the extent of KYC information that is available.

h. An MO shall ensure that there is no secrecy or data protection legislation that would restrict free access to the records on request by competent authorities, under court order or relevant mutual legal assistance procedures. Where it is found that such restrictions apply, copies of the underlying records of identity shall, wherever possible, be sought and retained.

i. Where identification records are held outside Ghana, it is still the responsibility of the MO to ensure that the records available do, in fact, meet the requirements in these Guidelines.

j. Business Conducted by Agents.

Where an applicant is dealing in its own name as agent for its own client, an MO shall, in addition to verifying the agent, establish the identity of the underlying client.

An MO may regard evidence as sufficient if it has established that the client:

i. Is bound by and has observed the Guidelines or the provisions of the AML Act, 2020 (Act 1044) and

ii. Is acting on behalf of another person and has given a written assurance that he has obtained and recorded evidence of the identity of the person on whose behalf he is acting.

k. Where another MO deals with its own client (regardless of whether or not the underlying client is disclosed to the MO) then:

i. where the agent is an MO, there is no requirement to establish the identity of the underlying clients or to obtain any form of written confirmation from the agent concerning the due diligence undertaken on its underlying clients or

ii. Where a regulated agent from outside Ghana deals through a customer omnibus account or for a named customer through a designated account, the agent shall provide a written assurance that the identity of all the underlying clients has been verified in accordance with their local requirements. Where such an assurance cannot be obtained, the business shall not be undertaken.

l. Where an agent is either unregulated or is not covered by the relevant AML/CFT&PF Legislation, the Risk-based approach shall be observed by the MO under such circumstances.

m. Correspondent Relationship

Transactions conducted through correspondent relationships may be managed, using a risk-based approach. "Know Your Correspondent" procedures shall be established to ascertain whether or not the correspondent entity or the counterparty is itself regulated for ML/TF&PF. Where regulated, the correspondent shall verify the identity of its customers in accordance with FATF standards. Where this is not the case, additional due diligence shall be required to ascertain and assess the correspondent's internal policy on ML/TF&PF prevention and know your customer procedures.

n. The volume and nature of transactions flowing through correspondent accounts with MOs from high risk jurisdictions or those with inadequacies or material deficiencies shall be monitored against expected levels and destinations and any material variances shall be checked.

o. An MO shall maintain records to ensure that, sufficient due diligence has been undertaken by the remitting entity on the underlying client including the origin of the funds.

p. An MO shall guard against establishing correspondent relationships with high risk foreign entities, shell companies with no physical presence in any country or with correspondent entities that permit their accounts to be used by such MO.

q. Staff of an MO that deals with correspondent entity accounts shall be trained to recognize higher risk circumstances and be prepared to challenge the correspondents over irregular activity (whether isolated transactions or trends) and to submit a suspicious transaction report to the FIC.

r. MOs shall terminate their accounts with correspondent entities that fail to provide satisfactory answers to reasonable questions including confirming the identity of customers involved in unusual or suspicious transactions.

2.38 ACQUISITION OF ONE MARKET OPERATOR BY ANOTHER

a. Where an MO acquires the business and accounts of another MO together with the underlying customers' records, it may not need to perform identity checks on the existing customers but shall carry out due diligence enquiries to confirm that the acquired institution had conformed to the requirements in these Guidelines.

b. The acquiring MO shall verify the identity of the transferred customers who were not verified by the transferor in line with the requirements for existing customers that open new accounts, where:

i. The AML procedures previously undertaken have not been in accordance with the requirements of these Guidelines.

ii. The AML procedures cannot be checked or the customer records are not available to the acquiring MO.

2.39 VULNERABILITY OF RECEIVING MOs AND AGENTS

a. A Receiving MO shall obtain satisfactory identification evidence of new applicants to securities issuances.

b. Where funds to be invested are provided by or on behalf of a third party, the identification evidence for both the applicant and the provider of the funds shall be obtained to ensure that the audit trail for the funds is preserved.

2.40 APPLICATIONS RECEIVED THROUGH BROKERS

a. Where the application is submitted (payment made) by a broker or an intermediary acting as agent, it may not be necessary to verify the identity of the underlying applicants provided that:

i. The lodging agent's stamp shall be affixed on the application form or allotment letter; and

ii. Application/acceptance forms and cover letters submitted by lodging agents shall be identified and recorded in the MO's records.

b. The terms and conditions of the issue shall state that any requirements to obtain identification evidence are the responsibility of the receiving broker/agent.

c. Where the original application has been submitted by a regulated broker, no additional identification evidence will be necessary for subsequent calls in respect of shares issued and partly paid.

2.41 APPLICATIONS RECEIVED FROM FOREIGN BROKERS

Where the broker or other intermediary is a regulated person or institution (including an overseas branch or subsidiary) from a country with equivalent legislation and financial sector procedures, and the broker or introducer is subject to anti-money laundering rules or regulations, then a written assurance can be taken from the broker that he/she has obtained and recorded evidence of identity of any principal and underlying beneficial owner that is introduced.

2.42 MULTIPLE FAMILY APPLICATIONS

a. Where multiple family applications are received supported by one cheque then identification evidence will not be required for:

i. A spouse or any other person whose surname and address are the same as those of the applicant who has signed the cheque;

ii. A joint account holder; or

iii. An application in the name of a child where the shares are to be registered with the name of the family member of full age on whose account the cheque is drawn and who has signed the application form.

b. Identification evidence of the signatory of the financial instrument shall be required for any multiple family applications supported by a cheque signed by someone whose name differs from that of the applicants.

Where an application is supported by an MO's cheque or banker's draft, the MO shall provide supporting documents.

2.43 LINKED TRANSACTIONS

a. Where it appears to a person handling applications that a number of single applications under different names are linked (e.g. payments from the same MO account) apart from the multiple family applications above, identification evidence shall be obtained in respect of parties involved in each transaction.

b. Installment payment issues shall be treated as linked transactions either at the outset or when a particular point has been reached, identification evidence must be obtained.

c. Applications that are believed to be linked where ML/TF&PF is suspected shall be processed on a separate batch for investigation after allotment and registration has been completed. Returns

with the documentary evidence are to be submitted to the FIC accordingly. Copies of the supporting cheques, application forms and any repayment cheque must be retained to provide an audit trail until the receiving MO is informed by FIC or the investigating officer that the records are of no further interest.

2.44 EXEMPTION FROM IDENTIFICATION PROCEDURES

Where a customer's identity was not properly obtained as contained in these Guidelines and an MO's own requirements for account opening, an MO shall re-establish the customer's identity in line with the contents of these Guidelines, except where it concerns:

a. An MO regulated by the requirements of these Guidelines and

b. Re-investment of Income.

2.45 FINANCIAL INCLUSION

a. An MO shall have a Financial Inclusion Policy

b. The MOs financially inclusion policy shall include policies for socially and financially disadvantaged applicants resident in Ghana.

c. Where an MO has reasonable grounds to conclude that an individual client is not able to produce the detailed evidence of his identity and cannot reasonably be expected to do so, the institution may accept as identification evidence a letter or statement from a person in a position of responsibility such as solicitors, doctors, ministers of religion and teachers who know the client, confirming that the client is who he says he is, and to confirm his permanent address. The ID of the guarantor must be obtained and verified.

d. Where an MO has decided to treat a client as "financially excluded", it shall record and maintain the reasons for doing so along with the account opening documents.

e. The MO shall satisfy itself that such customer is the person he/she claims to be.

f. An MO shall put in place additional monitoring of accounts opened under the financial inclusion exception procedures to ensure that such accounts are not misused.

2.46 SANCTIONS FOR NON-COMPLIANCE

Failure to comply with the provisions contained in these Guidelines will attract appropriate sanctions as prescribed in **SEC/FIC AML/CFT&PF Administrative Sanctions/ Penalties.**

APPENDIX A:

INFORMATION TO ESTABLISH IDENTITY

A. Natural Persons

For natural persons the following information shall be obtained, where applicable:

- **i.** Legal name and any other names used by the prospective client;
- **ii.** Location including important landmarks close to the prospective client's residence;
- **iii.** Telephone number, fax number and mailing address;
- **iv.** Date and place of birth;
- **v.** Nationality;
- **vi.** Hometown;
- **vii.** Occupation, position held and employer's name;
- **viii.** Identity document;
- **ix.** Nature of business;
- **x.** Type of account and nature of the investment relationship;
- **xi.** Signature;
- **xii.** Tax Identification Number (TIN); and
- **xiii.** Student identity card.

An MO shall verify this information by at least one of the following methods:

- **a.** Confirming the date of birth from an official document (e.g. birth certificate, passport, identity card, social security records);
- **b.** Confirming the permanent address (e.g. utility bill, tax assessment, bank statement, a letter from a public authority);
- **c.** Contacting the customer by telephone, letter or e-mail to confirm the information supplied after an account has been opened (e.g. a disconnected phone, returned mail, or incorrect e-mail address shall warrant further investigation);
- **d.** Confirming the validity of the official documentation provided through certification by an authorized person (e.g. embassy official, notary public) and
- **e.** Any other means of verification the MO deems appropriate.

An MO shall apply the same standard of identification and verification in respect of non-face-to-face customers.

Risk Profiling

Based on the information provided, an MO shall assess the risk profile of their customers taking into consideration the following:

- **i.** Evidence of an individual's permanent address sought through an accredited reference agency, or through independent verification by home visits;
- **ii.** Personal reference (i.e. by an existing customer of the same MO);
- **iii.** Prior MO reference and contact with the MO regarding the customer;
- **iv.** Source(s) of wealth/funds;
- **v.** Verification of employment, public position held (where appropriate).

An MO's customer acceptance policy shall not be so restrictive as to deny the general public access to financial services.

B. Institutions

The term institution includes any entity that is not a natural person. In considering the customer identification guidance for the different types of institutions, particular attention shall be given to the different levels of risk involved.

i.Business Entities

a. Identification and Verification

For business entities the following information shall be obtained:

1. Name of institution;
2. Principal place of institution's business operations;
3. Mailing address of institution;
4. Contact telephone, fax numbers, e-mail address and website address;
5. Some form of official identification number, if available (e.g. tax identification number);
6. The original or certified true copy of the certificate of registration and certificate of incorporation and

7. Regulations;
8. The resolution of the Board of Directors to open an account and identification of those who have authority to operate the account;
9. Nature and purpose of business and its legitimacy.

An MO shall verify this information by at least one of the following methods:

1. For established corporate entities - reviewing a copy of the latest annual report (audited, if available);
2. Conducting an enquiry by a business information service, or an undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
3. Undertaking a company search to determine its state as to whether the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated;
4. Utilizing an independent information verification process, such as accessing public and private databases;
5. Obtaining prior bank references;
6. Visiting the corporate entity and
7. Contacting the corporate entity by telephone, mail or e-mail.

An MO shall take reasonable steps to verify the identity and reputation of any agent that opens an account on behalf of a corporate customer, if that agent is not an officer of the corporate customer.

b. Ownership and Control

The principal guidance is to look behind the institution to identify those who have control over the business and the entity's assets, including those who have ultimate control.

Particular attention shall be paid to shareholders, signatories, or others who inject a significant proportion of the capital or financial support or otherwise exercise control. Where the owner is another corporate entity or trust, the objective is to undertake reasonable measures to look behind that company or entity and to verify the identity of the principals.

What constitutes control for this purpose shall depend on the nature of the entity, and may rest in those who are mandated to manage the funds, accounts or investments without requiring further authorization, and who shall be in a position to override internal procedures and control mechanisms.

For partnerships, each partner shall be identified and it is also important to identify immediate family members that have ownership control.

Where a company is listed on a recognized securities exchange or is a subsidiary of such a company then the company itself may be considered to be the principal to be identified. However, consideration shall be given to whether there is effective control of a listed company by an individual, small group of individuals or another corporate entity or trust. If this is the case then those controllers shall also be considered to be principals and identified accordingly.

ii.Other Types of Institutions

The following information shall be obtained in addition to that required to verify the identity of the principals in respect of Retirement Benefit Programme, Mutual/Friendly Societies, Cooperatives and Provident Societies, Charities, Clubs and Associations, Trusts and Foundations and Professional Intermediaries and any other institution as specified under the AML Legislation:

1. Name of account;
2. Mailing address;
3. Contact telephone, fax number, website and email address;
4. Some form of official identification number, such as the National Identifiction Number, Tax Identification Number;
5. Description of the purpose/activities of the account holder as stated in a formal constitution; and
6. Copy of documentation confirming the legal existence of the account holder such as register of charities.

An MO shall verify this information by at least one of the following:

1. Obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
2. Obtaining prior bank references; and
3. Accessing public and private databases or official sources.

a. Retirement Benefit Programme

Where an occupational pension Programme, employee benefit trust or share option plan is an applicant for an account, the trustee and any other person who has control over the relationship such as the administrator, Programme manager, and account signatories shall be considered as principals and an MO shall take steps to verify their identities.

b. Mutual/Friendly, Cooperative and Provident Societies

Where these entities are an applicant for an account, the principals to be identified shall be considered to be those persons exercising control or significant influence over the organization's assets. This often includes board members, executives and account signatories.

c. Charities, Clubs and Associations

In the case of accounts to be opened for charities, clubs and societies, an MO shall take reasonable steps to identify and verify at least two signatories along with the institution itself. The principals who shall be identified shall be considered to be those persons exercising control or significant influence over the organization's assets. This includes members of the governing body or committee, the President, board members, the treasurer, and all signatories.

In all cases, independent verification shall be obtained that the persons involved are true representatives of the institution. Independent confirmation shall also be obtained for the purpose of the institution.

d. Trusts and Foundations

When opening an account for a trust, an MO shall take reasonable steps to verify the trustee, the settlor of the trust (including any persons settling assets into the trust) any protector, beneficiary and signatories. Beneficiaries shall be identified when they are defined. In the case of a foundation, an MO shall take steps to verify the founder, the managers/directors and the beneficiaries.

e. Professional Intermediaries

When a professional intermediary opens a client account on behalf of a single client, that client must be identified. Professional intermediaries will often open "pooled" accounts on behalf of a number of entities.

Where funds held by the intermediary are not co-mingled but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary shall be identified.

In an open or closed ended Investment Company (unit trust or a mutual fund) an MO shall take steps to identify the following:

- **a.** The fund itself;
- **b.** Its directors or any controlling board;
- **c.** Its trustee/custodian, where it is a unit trust/mutual fund;
- **d.** Its managing (general) partner, where it is a limited partnership;
- **e.** Account signatories; and
- **f.** Any other person who has control over the relationship such as fund administrator or manager.

Where other investment vehicles are involved, the same steps shall be taken as in above. In addition, all reasonable steps shall be taken to verify the identity of the beneficial owners of the funds and of those who have control over the funds.

Intermediaries shall be treated as individual customers of an MO and the standing of the intermediary shall be separately verified by obtaining the appropriate information itemized above.

APPENDIX B:

DEFINITION OF TERMS

For the proper understanding of these Guidelines, certain terms used within are defined as follows:

Terms	**Definition**
Applicant for Business	The person or company seeking to establish a 'business relationship' or an occasional customer undertaking a 'one-off' transaction whose identity must be verified.
Beneficial owner	Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
Beneficiary	Beneficiary includes those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of Non-Profit Organizations (NPO). They comprise all trusts (other than charitable or statutory, permitted non-charitable trusts) that must have beneficiaries, who may include the settlor, and a maximum time, known as the perpetuity period, normally of 100 years.
Business Relationship	Business relationship is any arrangement between an MO and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on frequent, habitual or regular basis and where the monetary

	value of dealings in the course of the arrangement is not known or capable of being ascertained at the onset.
Business Entity	Business entity includes: **(a)** A firm, **(b)** An individual licensed to carry out a business, **(c)** A limited liability company, or **(d)** A partnership,
Competent Authorities	Include regulators, supervisory bodies, law enforcement agencies, etc.
Cooling-off rights	"cooling-off rights" means the rights of an investor to return products purchased and get a Refund if the individual changes his/her mind.
Country Risk	Is the level of ML/TF&PF risk of a particular country.
Cross-border transfer	Cross-border transfer means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element.
Customer Due diligence	CDD is the identification and verification of both the client and beneficiary on the basis of documents, data or information from a reliable and independent source including but not limited to continuous monitoring of the business relationship with an MO.
Designated	Designated categories of offences means:

categories of offences	**1.** Participation in an organized criminal group and racketeering; **2.** Terrorism, including terrorist financing; **3.** Trafficking in human beings and migrant smuggling; **4.** Sexual exploitation, including sexual exploitation of children; **5.** Illicit trafficking in narcotic drugs and psychotropic substances; **6.** Illicit arms trafficking; **7.** Illicit trafficking in stolen and other goods; **8.** Corruption and bribery; **9.** Fraud; **10.** Counterfeiting currency; **11.** Counterfeiting and piracy of products; **12.** Environmental crime; **13.** Murder, grievous bodily injury; **14.** kidnapping, illegal restraint and hostage-taking; **15.** Robbery or theft; **16.** Smuggling; **17.** Tax evasion **18.** Extortion; **19.** Forgery; **20.** Piracy; and **21.** Insider trading and market manipulation.
Designated nonfinancial businesses and professions	Designated non-financial businesses and professions means: **1.** Casinos (which also includes internet casinos). **2.** Real estate agents.

	3. Dealers in precious metals. **4.** Dealers in precious stones. **5.** Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to "internal" professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat ML/TF&PF. **6.** Trust and Company Service Providers refers to all persons or businesses that are not covered under these Guidelines, and which as a business, provide any of the following services to third parties: **i.** Acting as a formation agent of legal persons; **ii.** Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of partnership, or a similar position in relation to other legal persons; **iii.** Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; **iv.** Acting as (or arranging for another person to act as) trustee of an express trust;

	v. Acting as (or arranging for another person to act as) a nominee shareholder for another person.
FATF	Financial Action Task Force (FATF) is the global ML/TF&PF watchdog that sets international standards aimed at preventing ML/TF&PF activities and the harm they cause to society.
The FATF Recommendations	The FATF Recommendations refer to the FATF's Forty Recommendations.
False declaration	False declaration refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
False disclosure	False disclosure refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.
CDD measures for companies	They include those who own the controlling interests and comprise the mind and management of the company.
CDD measures for trusts	They include those who are the settlors, the trustees and persons that exercise effective control over the trust.

High-risk customers include:	**i.** Non-resident customers; **ii.** Non-face-to-face customers; **iii.** High net worth customers; **iv.** Legal persons or legal arrangements such as trusts; **v.** Companies that have nominee shareholders or shares in bearer form; **vi.** Politically exposed persons (PEPs); **vii.** Cross-border investment and business relationships; **viii.** Non-profit organizations **ix.** Designated Non-Financial Businesses and Professions and **x.**Any customer deemed high risk by an MO.
Identity	Identity means a set of attributes such as name(s) used, date of birth and the residential address including the code and digital address at which the customer can be located. These are features which can uniquely identify a natural or legal person.
Know Your Customer (KYC)	This refers to the collection of all the information relating to a customer account that has been collected from CIP, CDD and/or EDD procedures.
Legal arrangements	Legal arrangement refers to express trusts or other similar legal arrangements.
Legal persons	Legal persons refer to bodies corporate, foundations, partnerships, or associations, or any similar bodies that can establish a permanent

	customer relationship with an MO or otherwise own property.
Low risk customers include:	**i.** Other MOs; **ii.** Public companies listed on a securities exchange; **iii.** Ministries, Department and Agencies (MDAs) and other public institutions; **iv.** insurance companies; **v.** Insurance policies for pension schemes if there is no surrender-value clause and the policy cannot be used as collateral; **vi.** A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme; and **vii.** Beneficial-owners of pooled-accounts held by Designated Non-Financial Businesses and Professions (DNFBPs) provided that they are subject to requirements to combat money laundering and the financing of terrorism & proliferation of weapons of mass destruction consistent with the provisions of AML Legislation.
Non-profit Organizations/ Non-governmental Organizations	The term non-profit organization/non-governmental organizations refer to a legal entity or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal

	purposes, or for the carrying out of other types of good works.
One-off Transaction	A 'one-off transaction' means any transaction carried out other than in the course of an established business relationship. It is important to determine whether an applicant for business is undertaking a one-off transaction or whether the transaction is or will be part of a business relationship as this can affect the identification requirements.
Payable through account	Payable through account refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.
Politically Exposed Persons (PEPs)	PEPs are individuals who are or have been entrusted with prominent public functions both in Ghana and foreign countries and those associated with them. Examples of PEPs include, but are not limited to; **i.** Heads of State or government; **ii.** Ministers of State; **iii.** Politicians; **iv.** High ranking political party officials; **v.** An artificial politically exposed person (an unnatural legal entity. belonging to a PEP); **vi.** Senior public officials; **vii.** Senior Judicial officials **viii.** Senior military officials; **ix.** Chief executives of state owned companies/corporations; and

	x. Family members or close associates of PEPs.
Property	Property means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Risk	All references to risk in these Guidelines refers to the risk of ML/TF&PF.
Risk Based Approach	Means that countries and MOs identify, assess, and understand the money laundering and terrorist financing **risk** to which they are exposed, and take the appropriate mitigation measures in accordance with the level of **risk**.
Settlor	Settlors are persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trust's assets, the deed shall be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets
Shell company	Shell company means a company that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.
Suspicious Transaction	Suspicious transaction may be defined as one which is unusual because of its size, volume, type or pattern or otherwise suggestive of known

	ML/TF&PF methods. It includes such a transaction that is inconsistent with a customer's known legitimate business or personal activities or normal business for that type of account or that lacks an obvious economic rationale.
Terrorist	It refers to an individual who: **(i)** commits or attempts to commit, terrorist acts by any means, directly or indirectly; **(ii)** participates as an accomplice in terrorist act; **(iii)**organizes or directs others to commit terrorist act; or **(iv)**Contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Terrorist act	A terrorist act includes but are not limited to: **(i)** An act which constitutes an offence within the scope of, and as defined in one of the following treaties in the annex to the 1999 International Convention for the Suppression of the Financing of Terrorism, successor

	Resolutions and other relevant Resolutions. **(ii)** Any other act intended to cause death or serious bodily injury to a civilian, or to any other persons not taking an active part in the hostilities in the situation of arm conflicts, when the purpose of the act, by its nature or context, is to intimidate a population, or compel a government or international organisations to do or to abstain from doing any act.
Terrorist financing	Terrorist financing (FT) includes the financing of terrorist acts, and of terrorists and terrorist organizations.
Terrorist financing offence	A terrorist financing (FT) offence refers not only to the primary offence or offences relating to terrorism but also to ancillary offences.
Terrorist organization	Refers to any group of terrorists that: **(i)** commits or attempts to commit, terrorist acts by any means, directly or indirectly; **(ii)** participates as an accomplice in terrorist act;

	(iii)organizes or directs others to commit terrorist act; or **(iv)**Contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Those who finance Terrorism	Those who finance terrorism refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they shall be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts.
Trustee	Trustees, include paid professionals or companies or unpaid persons who hold the assets in a trust fund separate from their own assets. They invest and dispose of them in accordance with the settlor's trust deed, taking account of any letter of wishes. There may also be a protector who may have power to veto the trustees 'proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.

Unique identifier	A unique identifier refers to any unique combination of letters, numbers or symbols that refer to a specific originator.
Unquoted Companies	They are companies that are not listed on any securities exchange.
Virtual Asset	A virtual asset is digital representation of value that can be digitally traded, or trsfered, or can be used for payment or investment purposes.

APPENDIX C:

ML/TF&PF "RED FLAGS"

1. INTRODUCTION

Monitoring and reporting of suspicious transactions is key to effective AML/CFT &PF compliance. An MO put in place effective and efficient transaction monitoring programmes to facilitate the process. Although the types of transactions which could be used for ML/TF&PF are numerous, it is possible to identify certain basic features which tend to give reasonable cause for suspicion of ML/TF&PF.

This appendix, which lists various transactions and activities that indicate potential ML/TF&PF is not exhaustive. It does reflect the ways in which criminals have been known to operate.

Transactions or activities highlighted in this list are not necessarily indicative of actual ML/TF&PF if they are consistent with a customer's legitimate business. Identification of any of the types of transactions listed here shall put an MO on enquiry and provoke further investigation to determine their true legal status.

2. SUSPICIOUS TRANSACTIONS "RED FLAGS"

i. Potential Transactions Perceived or Identified as Suspicious

a. Transactions involving high-risk countries/jurisdictions vulnerable to money laundering, subject to this being confirmed.

b. Transactions involving shell companies.

c. Transaction activity involving amounts that are just below the stipulated reporting threshold or enquiries that appear to test an MO's own internal monitoring threshold or controls.

ii. Money Laundering Using Cash/Electronic Transactions

a. Significant increases in cash deposits or electronic transfer of an individual or business entity without apparent cause, particularly if such deposits are subsequently transferred within a short period out of the account to a destination not normally associated with the customer.

b. Unusually large cash deposits made by an individual or a business entity whose normal business are transacted by cheques and other non-cash instruments.

c. Frequent exchange of cash into other currencies.

iii. Money Laundering Using An MO

The following transactions may indicate possible money laundering, especially if they are inconsistent with a customer's legitimate business:

a. Minimal, vague or fictitious information on the transaction provided by a customer that an MO is not in a position to verify.

b. Lack of reference or identification in support of an account opening application by a person who is unable or unwilling to provide the required documentation.

c. A prospective customer does not have a local residential or business address and there is no apparent legitimate reason for opening an account.

d. Customers maintaining multiple accounts with an MO or different MOs for no apparent legitimate reason or business rationale. The accounts may be in the same names or have different signatories.

e. Customers depositing/withdrawing or electronically transferring large amounts of cash with no apparent source or in a manner inconsistent with the nature and volume of the business.

f. Customer requests for early redemption of certificates of deposit or other investment soon after the purchase, with the customer willing to suffer loss of interest or incur penalties for premature realization of investment.

g. Customer requests for disbursement of the proceeds of certificates of deposit or other investments by multiple cheques, each below the prescribed reporting threshold.

h. Accounts with large volumes of activity but low balances or frequently overdrawn positions.

i. Substantial cash deposits or electronic transfer by professional customers into client, trust or escrow accounts.

j. Customers who appear to have accounts with several institutions within the same locality, especially when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

k. Large cash withdrawals or electronic transfer from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

l. Substantial increase in deposits of cash, electronic transfer or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.

m. Large number of individuals making payments into the same account without an adequate explanation.

n. High velocity of funds that reflects the large volume of money flowing through an account.

o. An account operated in the name of an off-shore company with structured movement of funds. An MO shall take into account the possibility that a principal beneficial owner may be registered as an off-shore company.

iv.Terrorist Financing "Red flags"

a. Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g. student, unemployed, or self-employed).

b. Financial transaction by a non-profit or charitable organization, for which there appears to be no logical economic purpose or for which there appears to be no link between the stated activity of the organization and other parties in the transaction.

c. A safe deposit box held on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

d. Large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves designated high-risk locations.

e. The stated occupation of the customer is inconsistent with the type and level of account activity.

f. Funds transfer does not include information on the originator, or the person on whose behalf the transaction is conducted, the inclusion of which shall ordinarily be expected.

g. Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and channel funds to a small number of foreign beneficiaries.

h. Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries /jurisdictions.

i. Funds generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from designated high-risk countries.

v. Proliferation Financing "Red flags''

a. Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.
b. When customer is vague about the ultimate beneficiaries and provides incomplete information or is resistant when requested to provide additional information.
c. The transaction(s) involve an individual or entity in any country of proliferation concern.

d. Transaction involves person or entity in foreign country of diversion concern.
e. The transaction(s) related to dual-use, proliferation-sensitive or military goods, whether licensed or not.
f. Involvement of a person connected with a country of proliferation concern (e.g. a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.
g. The customer or counter-party or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions
h. Customer activity does not match business profile, or end-user information does not match end-user's business profile.
i. Transaction involves possible shell companies (e.g. companies do not have a high level of capitalisation or displays other shell company indicators).
j. Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
k. Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose
l. Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
m. Use of cash or precious metals (e.g. gold) in transactions for industrial items.
n. Transactions between companies on the basis of "ledger" arrangements that obviate the need for international financial transactions.
o. Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated).
p. Involvement of a university in a country of proliferation concern.
q. Use of personal account to purchase industrial items

Refer to FATF Guidance on Proliferation Financing Red Flags for further details.

v. Virtual Assets "Red Flags"

- **a.** Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.
- **b.** Customer uses a virtual asset exchange or foreign-located money value transfer service in a high-risk jurisdiction known to have inadequately regulated for virtual asset entities, including inadequate CDD or KYC measures.
- **c.** Transactions involving more than one type of virtual assets, particularly those that provide higher anonymity, such as anonymity enhanced cryptocurrency or privacy coins and despite additional transaction fees.
- **d.** Virtual assets moved from a public, transparent blockchain to a centralised exchange and then immediately traded for anonymity enhanced cryptocurrency or privacy coin.
- **e.** Abnormal transaction activity of virtual assets from peer-to-peer platform associated wallets with no logical business explanation.
- **f.** Structuring transactions in small amounts and under the record-keeping or reporting thresholds.
- **g.** Transferring virtual assets immediately to multiple virtual asset service providers, including those registered or operated in other countries.
- **h.** Transactions involve multiple virtual assets, or multiple accounts, without a logical business explanation.
- **i.** New users make a large initial deposit to open a new relationship with a virtual asset service provider, inconsistent with the customer profile.
- **j.** irregularities during the customer due diligence process, for example incomplete or insufficient customer information, forged identification document during onboarding.
- **k.** Irregularities in customer profile, such as shared credentials or presence on forums associated with illegal activity.
- **l.** Irregularities during account creation, such as creating different accounts under different names, or transactions initiated from IP addresses from sanctioned jurisdictions.

m. Potential mule or scam victims, who are often unfamiliar with virtual assets technology.

Refer to FATF Guidance on Virtual Assets Red Flags for further details.

vi. Other Unusual or Suspicious Activities

n. Employee exhibits a lavish lifestyle that cannot be justified by his/her salary.

o. Employee is reluctant to apply for leave.

p. Customer uses a personal account for business purposes.

q. Official Embassy business is conducted through personal accounts.

r. Embassy accounts are funded through substantial currency transactions.

s. Embassy accounts directly fund personal expenses of foreign nationals.

APPENDIX D:

FURTHER GUIDANCE FOR AN MO's RISK ASSESSMENT AND BUSINESS/CUSTOMER RISK PROFILING

ML/FT & PF RISK ASSESSMENT AND PROFILING — OVERVIEW

This heading explains the concept of an MO's assessment and management of its ML/TF & PF risks (including assignment of risk profiling scores of business/customer ML/TF & PF risks into the categories of "low risk", "medium risk" and "high risk"). The notes relating to risk assessment, customer risk factors, geographic or country risk factors, product, service and delivery channel risk factors and risk variables are primarily sourced from the FATF Recommendation 1 on Risk Assessment and Recommendation 10 on Customer Due Diligence and the accompanying Interpretative Notes.

The same risk management principles that an MO uses in traditional operational areas shall be applied to assessing and managing ML/FT & PF risk. A well-developed risk assessment and profiling will assist in identifying an MO's ML/FT&PF risk profile and properly rating its

business/customer ML/TF & PF risk. Understanding the risk profile enables an MO to apply appropriate risk management processes to the ML/FT & PF Compliance Programme to mitigate risk. This risk assessment process enables management to better identify and mitigate gaps in an MO's controls.

ML/FT & PF risk assessment and rating generally involves two steps: first, identify the specific risk categories (i.e., for customers, countries or geographic areas; and products, services, transactions or delivery channels) unique to an MO; and second, conduct a more detailed analysis of the data identified to better assess the risk within these categories and risk rating each customer.

Identification of Specific Risk Categories

The first step of the risk assessment process is to identify the customers, geographic areas, products /services and transactions or delivery channels unique to an MO. Although attempts to launder money, finance terrorism, or conduct other illegal activities through an MO can emanate from many different sources, certain customers, geographic areas, products/services and transactions or delivery channels may be more vulnerable or have been historically abused by money launderers and criminals. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, shall be considered when an MO prepares its risk assessment.

Product/service, transaction or delivery channel risk factors:

Certain products/services offered by an MO may pose a high risk of ML/TF&PF depending on the nature of the specific product or service offered. Such products/services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Some of these products/services are listed below, but the list is not all inclusive:

a. Private investment.

b. Anonymous transactions (which may include cash).

c. Non-face-to-face business relationships or transactions.

d. Payment received from unknown or un-associated third parties.

Customer risk factors

FATF has set out the categories of PEPs as categories which are considered as high-risk or which require specific due diligence measures. In addition, an MO shall consider the following customer risk factors:

a. The business relationship is conducted in an unusual circumstances (e.g. significant unexplained geographic distance between an MO and a customer).

b. Non-resident customers.

c. Legal persons or arrangements that are personal asset-holding vehicles.

d. Companies that have nominee shareholders or shares in bearer form.

e. Business that are cash-intensive.

f. The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

Geographical areas risk factors:

It is essential that an MO's AML/CFT & PF compliance program is designed in such a way as to identify geographic locations that may pose a high risk to an MO. An MO shall understand and evaluate the specific risks associated with doing business, opening accounts for customers from, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not necessarily determine a customer's or transaction's risk level, either positively or negatively.

International high risk geographic locations generally include:

a. Countries identified by credible sources, such as FATF and GIABA, as not having strategic deficiencies in their AML/CFT & PF regimes.

b. Countries subject to sanctions, embargos or similar measures issued by bodies such as the United Nations Security Council (UNSC).

c. Countries identified by credible sources as having significant levels of corruption or other criminal activity.

d. Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

Analysis of Specific Risk Categories and Risk Variables

The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess ML/FT & PF risk. When assessing the ML/TF&PF risks relating to types of customers, geographical areas, and particular products, services, transactions or delivery channels risk, An MO shall take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures.

Examples of such variables include:

a. The purpose of an account or relationship.
b. The level of assets to be deposited by a customer or the size of transactions undertaken.
c. The regularity or duration of the business relationship.

Developing An MO's AML/CFT & PF Compliance Program Based on Its Risk Assessment

The management of an MO shall structure their AML/CFT & PF compliance program to adequately address its risk profile, as identified by the risk assessment. Management shall understand an MO's ML/FT & PF risk exposure and develop the appropriate policies, procedures, and processes to monitor and control ML/FT & PF risks. For example, an MO's monitoring systems to identify, research, and report suspicious activity shall be risk-based, with particular emphasis on higher-risk products/services, customers, entities, and geographical locations as identified by an MO's ML/FT & PF risk assessment.

Audit shall review an MO's risk assessment for reasonableness. Additionally, management shall consider the staffing resources and the level of training necessary to promote adherence with these

policies, procedures, and processes. For an MO that assumes a higher-risk ML/FT & PF profile, management shall provide a more robust AML/CFT & PF compliance program that specifically monitors and controls the higher risks that management and the board have accepted.

Consolidated AML/CFT & PF Compliance Risk Assessment

An MO that implements a consolidated or partially consolidated AML/CFT & PF compliance program shall assess risk both individually within business lines and across all activities and legal entities. Aggregating ML/FT & PF risks on a consolidated basis for larger or more complex organizations may enable an organization to better identify risks and risk exposures within and across specific lines of business or product categories. Consolidated information also assists senior management and the board of directors in understanding and appropriately mitigating risks across the organization. To avoid having an outdated understanding of the ML/FT & PF risk exposures, an MO shall continually reassess its ML/FT & PF risks, review its risk profiling of customers and communicate with business units, functions, and legal entities. The identification of an ML/FT & PF risk or deficiency in one area of business may indicate concerns elsewhere in the organization, which management shall identify and control.

Updating of An MO's Risk Assessment and Profiling

An effective AML/CFT & PF compliance program controls risks associated with an MO's products/services, customers, entities, and geographical locations; therefore, an effective risk assessment shall be **an ongoing process**, not a one-time exercise. Management shall update its risk assessment to identify changes in an MO's risk profile, as necessary (e.g., when new products and services are introduced, existing products/services change, higher-risk customers open and close accounts, or an MO expands through mergers and acquisitions). Even in the absence of such changes, it is a sound practice for an MO to periodically reassess their ML/FT & PF risks at least every 12 to 18 months.

APPENDIX E:

RELEVANT LEGISLATION:

1. Companies Act, 2019 (Act 992)
2. Securities Industry Act, 2016 (Act 929)
3. Anti-Money Laundering Act, 2020 (Act 1044)
4. Anti-Money Laundering Regulations, 2011 (L.I. 1987)
5. Anti-Terrorism Act, 2008 (Act 762)
6. Anti-Terrorism (Amendment) Act, 2014 (Act 875)
7. Anti-Terrorism Regulations, 2012 (L.I. 2181)
8. Criminal Offences (Amendment) Act, 2012 (Act 849)
9. Whistle Blower Act, 2006 (Act 720)
10. Revised SEC/FIC AML/CFT & PF Guidelines for Market Operators, 2021

OTHER RELEVANT LEGISLATION INCLUDE:

1. EOCO Regulation 2012, LI2183
2. Economic and Organized Crime Act 2010, Act 804
3. Executive Instrument 2
4. Executive Instrument 1.8
5. Executive Instrument 1.9

APPENDIX F:

LIST OF RELEVANT BODIES:

1. All Supervisory Bodies
2. All Regulatory Bodies
3. All Law Enforcement Agencies
4. Financial Action Task Force (FATF)
5. EGMONT Group-A Network of Financial Intelligence Units (FIC is a member)
6. GIABA

7. IOSCO

These Guidelines are designed to manage the risks faced by an MO on the laundering of the proceeds of crime and shall provide protection against fraud, reputational and other risks faced by an MO. Consequently, an MO shall adopt a risk–based approach in the identification and management of their ML/TF&PF risks in line with the requirements of these Guidelines.

These Guidelines are in accordance with the Financial Action Task Force (FATF)'s Recommendations, International Organization of Securities Commissions' (IOSCO) principles and international best practice in managing AML/ CFT & PF issues.

An MO shall note that AML/CFT&PF Legislation have prescribed sanctions for non-compliance. It is, therefore, in the best interest of an MO to ensure compliance at all times with the prescriptions contained herein.

These Guidelines shall be read in conjunction all AML/CFT&PF Legislation, FATF Recommendations.

As part of our commitment to continual improvement, readers of these Guidelines shall identify improvement opportunities and bring them to the attention of the SEC for evaluation and subsequent incorporation into these Guidelines.

APPENDIX G:

REASONS FOR THE REVISION:

The events that have occurred since the launch of the AML/CFT & PF Guidelines have necessitated a review. These events include:

1. The enactment of the new AML Act 2020, Act (1044)
2. Revisions to the FATF's Recommendations in 2020
3. Lessons learnt from the implementation of the SEC/FIC AML/CFT&PF Guidelines for MOs.

4. Lessons learnt from the implementation of the SEC/FIC AML/CFT&PF Administrative Sanctions/Penalties for MOs.

5. Lessons learnt from Ghana's National Risk Assessment Report (2018)

6. Lessons learnt from Ghana's Mutual Evaluation Report (2016)

APPENDIX H:

CHECKLIST FOR MO'S AML/CFT & PF COMPLIANCE PROGRAM

The AML Compliance program ***shall*** provide for procedures including the following:

- **a.** Policy statement on AML/CTF&PF compliance
- **b.** Designation of the AMLRO and responsibilities
- **c.** Internal ML/FT & PF Risk Assessment Procedures
- **d.** Risk management procedures
- **e.** Requirements for assessing risks of new products, services and technologies
- **f.** Adequate screening procedures on before and after hiring employees
- **g.** Staff training requirements
- **h.** Procedures and obligations to report STRs
- **i.** Obligation to submit CTRs
- **j.** Prohibition against Tipping off or disclosing to unauthorized external persons that an STR is being filed
- **k.** Record keeping requirements
- **l.** Procedures related to identifying potential terrorist financing
- **m.** Know Your Customer (KYC) Policy:
  - **(i)** Customer Acceptance Policy (CAP)
  - **(ii)** Customer Identification Programme:
- **n.** Type of information an MO must obtain from prospective customers
- **o.** Methodologies employed to verify such information
- **p.** How to deal with customers who refuse to provide information
- **q.** How to handle situation where customer identity cannot be verified

r. When to rely on another institutions' identity verification process

s. PEP identification

t. Review of clients against an appropriate sanction list

u. Monitoring of clients transactions

v. Customer notification of an MO identification and verification procedures

APPENDIX I:

FRAUD AND DEFALCATION REPORT REQUIREMENTS:

The reporting requirements on Fraud or Defalcation shall include the following:

a. Report Number

b. Date of Occurrence

c. Date of Detection

d. Amount Involved

e. Name of Customer Involved

f. Principal Persons Suspected

g. Description of the Incident

h. Other Financial Institutions Involved

i. Remedial Action Taken