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

FOR MARKET OPERATORS (MOs) IN GHANA

NOVEMBER 1, 2023

Table of Contents

LIST OF ACRONYMS AND ABBREVIATION

AML/CFT/CPF	-	Anti-Money Laundering/Combating the Financing of Terrorism/ 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
GIPC	-	Ghana Investment Promotion Centre
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/CPF) efforts in Ghana, policy makers still face challenges in their ability to combat this menace.

Full and effective implementation of the new AML Act, 2020 (Act 1044) 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/CPF Guidelines have been revised to provide effective guidance 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:

i. The Anti-Money Laundering Act, 2020 (Act 1044)
ii. The Securities Industry Act, 2016 (Act 929), as amended
iii. The Companies Act, 2019 (Act 992)
iv. The Anti-Money Laundering Regulations, 2008 (LI 1987)
v. The Anti-Terrorism Regulations 2012, (LI 2181)
vi. The Anti-Terrorism (Amendment Act), 2012 (Act 842)
vii. The Anti-Terrorism (Amendment Act), 2014 (Act 875)
viii. The Revised FATF 40 Recommendations
ix. Lessons drawn from working with the previous SEC/FIC/ AML/CFT/CPF Guidelines for MOs in Ghana.
x. Lessons learnt from Ghana's National Risk Assessment Reports
xi. Lessons learnt from Ghana's Mutual Evaluation Reports

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

INTRODUCTION

Given the prominence that financial crimes especially Money Laundering (ML), Terrorist Financing (TF) and the Financing of 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, there is need for a comprehensive effort to fight this menace. It is against this background that SEC and the FIC in accordance with:

1. The Anti-Money Laundering Act, 2020 (Act 1044)
2. The Securities Industry Act, 2016 (Act 929), as amended
3. The Anti-Terrorism Act, 2008 (Act 762)
4. The Anti-Terrorism (Amendment Act), 2012 (Act 842)
5. The Anti-Terrorism (Amendment Act), 2014 (Act 875)
6. The Anti-Money Laundering Regulations, 2011 (L.I.1987) and
7. The Financial Action Task Force (FATF) 40 Recommendations

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 shall be read in conjunction with all AML/CFT/CPF Legislation and FATF Recommendations.

An MO shall note that AML/CFT/CPF Legislation has prescribed sanctions for non-compliance. It is, therefore, in the best interest of an MO to always ensure compliance with the prescriptions contained herein.

OBJECTIVE OF THESE GUIDELINES

These Guidelines are being issued pursuant to Section 52 of Act 1044 and are intended to assist MOs to:

1. Understand and comply with AML/CFT/CPF laws and regulatory requirements;
2. Develop and implement effective risk-based AML/CFT/CPF compliance programmes that enable adequate identification, monitoring and reporting of suspicious activities;
3. Understand the expectations of the SEC with respect to the minimum standards for AML/CFT/CPF regime;
4. Provide guidance on Know Your Customer/ Customer Due Diligence/ Enhanced Due Diligence (KYC/CDD/EDD) measures; and
5. Understand the implications of non-compliance with AML/CFT/CPF requirements. (Refer to the SEC/FIC AML/CFT/CPF Administrative Sanctions).

OVERVIEW OF THESE GUIDELINES

There have been growing concerns about the major threats that ML/TF/PF pose to international peace and security. These threats have the tendency to undermine Ghana's development and progress.

Consequently, Ghana and by extension the Securities Sector has made concerted efforts to check these crimes. MOs, in particular, have come under sustained regulatory pressure to improve their monitoring and surveillance systems with a view to detecting, preventing, and responding effectively to the threat of ML/TF/PF. These Guidelines cover among others the following key areas of AML/CFT/CPF policy:

i. Anti-Money Laundering Reporting Officer designation and duties;
ii. The need to co-operate with the supervisory authority;/competent authority
iii. Customer due diligence;
iv. Monitoring and reporting of suspicious transactions /activities;
v. Statutory reporting requirements;
vi. Record keeping; and
vii. AML/CFT/CPF employee-education training programme.

MOs are exposed to varying ML/TF/PF risks and serious financial and reputational damage if they fail to manage these risks adequately. Diligent implementation of the provisions of these Guidelines would not only minimize the risk faced by MOs of being used to launder the proceeds of crime but also provide protection against economic and organized crime, reputational and financial risks. In this regard, institutions are directed to adopt a risk-based approach in the identification and management of their ML/TF/PF risks.

MOs are also reminded that AML/CFT/CPF policies governing their operations should not only prescribe money laundering and predicate offences but also prescribe sanctions for non-compliance with the relevant AML/CFT/CPF requirements. It is, therefore, in the best interest of the institutions to entrench a culture of compliance which would be facilitated by these Guidelines. MOs shall be required to conduct their AML/CFT/CPF audits using these revised AML/CFT/CPF Guidelines.

SANCTIONS FOR NON-COMPLIANCE

Failure to comply with the provisions contained in these Guidelines shall attract appropriate administrative sanctions as prescribed in the SEC/FIC AML/CFT/CPF Administrative Sanctions.

These Guidelines are structured as follows;

Part A – Obligations and co-operations among competent authorities

Part B – Elements for effective AML/CFT/CPF Regime

Part C – Further Guidance on KYC/CDD/EDD Procedures Appendices References

……	…….
DIRECTOR-GENERAL	CHIEF EXECUTIVE OFFICER
SECURITIES AND EXCHANGE COMMISSION	FINANCIAL INTELLIGENCE CENTRE

PART A

1.0 OBLIGATIONS AND CO-OPERATIONS AMONG COMPETENT AUTHORITIES

1.1 AML/CFT/CPF OBLIGATIONS OF THE SECURITIES AND EXCHANGE COMMISSION

1. In compliance with section 52(1) and (5) of Act 1044, the SEC is hereby designated as a supervisory body to ensure supervision and enforcement of compliance by MOs in relation to AML/CFT/CPF requirements.
2. The SEC shall carry out the following functions:
    i. Adopt a risk-based approach in supervising and monitoring MOs;
    ii. Monitor and periodically assess the level of ML/TF/PF risk of the MOs;
    iii. Carry out an examination of MOs based on the SEC risk-assessment framework.
    iv. Request production of, access to, the records, documents, or any other information relevant to the supervision and monitoring of MOs;
    v. Develop guidelines, directives, circulars or notices to ensure compliance;
    vi. Provide feedback on compliance with obligations under Act 1044 by MOs; and
    viii. Undertake any other activity necessary for assisting MOs to understand their obligations under Act 1044.

1.2 CO-OPERATION AND INFORMATION SHARING WITH COMPETENT AUTHORITIES

1. In accordance with section 52(5)(f) of Act 1044, the SEC shall co-operate and share information with any other competent authorities in the performance of functions and the exercise of powers under Act 1044.
2. In this regard, the SEC shall;
    i. initiate and act on a request from a foreign counterpart and notify FIC immediately;
    ii. impose administrative penalties for non-compliance with Act 1044;
    iii. issue Guidelines/Notices/Directives/Circulars to ensure compliance with Act 1044 and Act 929 as amended;
    iv. any other function as may be required to ensure compliance with Act 1044;
3. During an examination, require Employees, Directors, or Third Parties

of the MO to:

i. answer questions relating to the records and documents of that MOs; and
ii. provide any other information that the SEC may require for the purpose of the examination.

1.3. MARKET OPERATORS' CO-OPERATION WITH COMPETENT AUTHORITIES

1. An MO shall declare its commitment in its AML/CFT/CPF policy 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. The 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 per Section 36 of Act 1044 and
   iii. protect the security and confidentiality of such requests.
2. Notwithstanding the above, a competent authority shall have access to information in order to perform its functions in combating ML/TF/PF. This shall include the sharing of information between competent authorities, either domestically or internationally, and also the sharing of information between MOs.

PART B

2.0 ELEMENTS FOR EFFECTIVE AML/CFT/CPF REGIME

2.1 AML/CFT/CPF INSTITUTIONAL POLICY FRAMEWORK

1. An MO shall develop and implement policies indicating their commitment to comply with AML/CFT/CPF obligations under Act 1044, these Guidelines and other relevant regulations to prevent ML/TF/PF risks.
2. The MO shall formulate and implement internal rules, procedures and other controls that will deter criminals from using their facilities for ML/TF/PF activities and shall ensure compliance with the relevant laws and regulations.

2.2 ASSESSING ML/TF/PF RISK AND APPLYING A RISK–BASED APPROACH

1. An MO's AML/CFT/CPF risk management function shall be aligned and integrated with its overall risk management control function.
2. The 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.
3. The MO shall use the results of its risk assessment to design its AML/CFT/CPF Compliance Programme in accordance with Section 49 of Act 1044 and its Regulations.
4. The MO, in assessing ML/TF/PF risks, shall:
    i. document its risk assessments methodology and submit a Board Approved copy to the SEC;
    ii. document its risk assessment findings in the form of a risk assessment report and submit a Board Approved 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 significant review and or upon a request.
5. The MO shall:
    i. conduct additional risk assessment when required by the SEC;
    ii. be guided by the findings of National Risk Assessment and Mutual Evaluation Reports in conducting its risk assessments;
    iii. submit timely reporting of the following to the Board of Directors;

a. ML/TF/PF risk assessment;
b. ML/TF/PF risk profile (risk categorization) and
c. The effectiveness of risk control and mitigation measures.

6. The frequency of the reporting shall be determined by the Board but shall not be more than two (2) years.
7. Further Guidance on MOs Risk Assessment and Business/Customer Risk Profiling is provided in **Appendix D**.

2.3 AML/CFT/CPF RISK ASSESSMENT FOR NEW PRODUCTS AND SERVICES

1. An MO shall review, identify and record areas of potential ML/TF/PF risks for new products and services and submit a report for SEC's approval before they are launched.
2. The MO shall review its AML/CFT/CPF framework from time to time with a view to determining their adequacy and identification of other areas of potential risks when introducing new products.

2.4 AML/CFT/CPF GOVERNANCE FRAMEWORK

2.4.1 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.

2.4.2 ROLE OF THE BOARD OF DIRECTORS (BOARD)

1. The Board has ultimate responsibility for ensuring the effectiveness of the AML/CFT/CPF compliance programme. In this regard, the Board's oversight in respect of AML/CFT/CPF shall align with the SEC's Corporate Governance Guidelines.
2. Approving the appointment of the AMLRO.
3. Approving the AML/CFT/CPF compliance programme, training programme, compliance reports, Internal Risk Assessment Framework.
4. Ensuring the establishment of appropriate mechanisms to periodically review key AML/CFT/CPF policies and procedures to ensure their continued relevance in line with changes in the MO's products and services and to address new and emerging ML/TF/PF risks.
5. Ensuring the establishment of an appropriate AML/CFT/CPF risk management framework with clearly defined lines of authority and responsibility for AML/CFT/CPF and effective

separation of duties between those implementing the policies and procedures and those enforcing the controls.

6. Ensuring that the Board receives the requisite training on AML/CFT/CPF generally as well as on the institution's specific AML/CFT/CPF risks and controls at least once a year.
7. Ensuring receipt of regular and comprehensive reports on the MO's AML/CFT/CPF function from the AMLRO for its information and necessary action including but not limited to:
    a. Remedial action plans if any, to address the results of Independent Audits (either internal or external); regulatory reports received from the Securities and Exchange Commission or other regulators on its assessment of the institution's AML/CFT/CPF programme;
    b. Results of compliance testing and self-identified instances of non-compliance with AML/CFT/CPF requirements;
    c. Recent developments in AML/CFT/CPF laws and regulations and their implications if any, to the MOs;
    d. Details of recent significant risk events and potential impact on the MO; and
    e. Statistics of statutory report to the FIC, orders from law enforcement agencies, refused or declined business and de-risked relationships.

2.4.3 ROLE OF SENIOR MANAGEMENT

1. Senior Management is responsible for the day-to-day implementation, monitoring and management of the MO's AML/CFT/CPF compliance programme, including ensuring adherence to established AML/CFT/CPF policies and procedures. Among other things, Senior Management should ensure that policies and procedures:
    a. Are risk based, proportional and adequate to mitigate ML/ TF/PF risks of the MO;
    b. Comply with all relevant AML/CFT/CPF laws, regulations and guidelines;
    c. Are implemented effectively across relevant business areas or throughout the financial group as applicable; and
    d. Exist for succession planning for the AMLRO function.

2. Senior Management must review policies and procedures periodically for consistency with the MO's business model, product and service offerings, and risk appetite. Attention should be paid to new and developing technologies and MOs should identify and assess the ML/TF/PF risks arising from new products/services and delivery channels; new business practices, new

delivery mechanisms and new or developing technologies for new and pre-existing products; and put measures in place to manage and mitigate such risks. Risk assessments should take place prior to the launch or use of such products/services, channel, business practices and technologies.

3. Senior Management shall also ensure that:
   a. All significant recommendations made by internal and external auditors and regulators in respect of the AML/CFT/CPF programme are addressed in a timely manner;
   b. Relevant, adequate and timely information regarding AML/CFT/CPF matters is provided to the Board;
   c. The AMLRO receives appropriate training on an ongoing basis to effectively perform his duties;
   d. There is an ongoing employee-education training programme (at least twice a year) which enables employees to have adequate and relevant knowledge to understand and discharge their AML/CFT/CPF responsibilities; and
   e. The Compliance Officer/ AMLRO and Internal Audit functions are resourced adequately in terms of personnel, IT systems and budget to implement, administer and monitor the AML/CFT/CPF programme requirements effectively.

2.4.4 THE APPOINTMENT, ROLE AND DUTIES OF THE ANTI-MONEY LAUNDERING REPORTING OFFICER (AMLRO)

1. An MO shall appoint a person to act as an AMLRO who shall be at a key management level who shall have sufficient authority, independence and seniority to be able to effectively carry out his duties in accordance with Act 1044 and these Guidelines.
2. The identity of the AMLRO must be treated with the strictest confidence by the employees of the MO.
3. The MO shall ensure that the AMLRO acquires professional qualification in anti-money laundering and financial crime.
4. The AMLRO shall have relevant AML/CFT/CPF qualification(s) and experience as may be approved by the Commission from time to time.
5. The AMLRO shall operationally report to its Board in accordance with section 50(b) of Act 1044 and Regulation 5(1) of AML Regulations, 2011, L.I. 1987.
6. The MO shall notify the SEC and the FIC on appointment and resignation of an AMLRO.

7. The duties of the AMLRO shall include but not limited to the following:
    a. Report quarterly to the Board or a Sub-Committee of the Board to ensure operational independence.
    b. Conduct regular risk assessments of the inherent ML/TF/PF risks including timely assessments of new products, services and business acquisition initiatives to identify potential ML/TF/PF risks and develop appropriate control mechanisms;
    c. Develop and implement an AML/CFT/CPF Compliance Programme;
    d. Keep the AML/CFT/CPF programme current relative to the institution's identified inherent risks and give consideration to local and international developments in ML/TF/PF;
    e. Receive reports from staff and conduct preliminary investigations of suspicious transactions;
    f. File suspicious transaction/activity report, cash transaction report and electronic transaction report with the FIC;
    g. Coordinate the training of staff in AML/CFT/CPF awareness, detection methods and reporting requirements;
    h. 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/PF;
    i. Shall be involved in decisions to offer new products or services or to make significant changes in existing products or services;
    j. Undertake other duties relevant to AMLRO's function and
    k. Ensure that the systems and other processes that generate information used in reports to Senior Management and the Board are adequate and appropriate.
8. The 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.
9. 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.

2.4.5 INTERNAL CONTROLS, COMPLIANCE AND AUDIT

1. An MO shall establish and maintain internal procedures, policies and controls to prevent ML/TF/PF and to communicate these to their employees. These procedures, policies and controls should cover the CDD, record retention, the detection of unusual and suspicious transactions/activities, the reporting obligation, among other things.
2. The AMLRO and appropriate staff are to have timely access to customer identification data, CDD information, transaction records and other relevant information.
3. The MO is therefore required to develop programmes against ML/TF/PF to include:
    a. The development of internal policies, procedures and controls, including appropriate compliance management arrangement and adequate screening procedures to ensure high standards when hiring employees;
    b. Ongoing Staff, Management and Board training programmes to ensure that employees are kept informed of new developments, including:
    c. Information on current ML/TF/PF techniques, methods and trends;
    d. Clear explanation of all aspects of AML/CFT/CPF laws and obligations; and
    e. Requirements concerning CDD and suspicious transaction/activity reporting.
    f. Adequately resourced and independent audit function to test compliance with the procedures, policies and controls.
4. The MO shall put in place a structure that ensures the operational independence of the AMLRO.

2.4.6 TESTING FOR THE ADEQUACY OF THE AML/CFT/CPF COMPLIANCE PROGRAMME

1. An MO shall make a policy commitment and subject its AML/CFT/CPF compliance programme to independent testing, to determine its adequacy, completeness and effectiveness.
2. It is important that this independent testing is performed by Auditors (Internal or External) who have had appropriate AML/CFT/CPF training and experience in respect of ML/TF/PF risk and an appropriate level of knowledge of the regulatory requirements and guidelines.
3. The independent testing shall not be performed by persons involved with the MO's AML/CFT/CPF Compliance function.
4. The Independent Testing shall be performed every two (2) years.

5. The report on the Independent 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 January 31 of every other financial year in which it is conducted.
6. Any identified weaknesses or inadequacies shall be promptly addressed by the MO.

2.5 CUSTOMER DUE DILIGENCE (CDD) PROGRAMME

1. An MO must develop and implement risk-based policies and procedures to mitigate the ML/TF/PF risks identified in their business and customer risk assessments. The risk assessment framework should identify which customers or categories of customers present higher risk and therefore require the application of enhanced due diligence (EDD).
2. Similarly, where the MOs determine that a customer or a category of customers presents low risk, simplified due diligence (SDD) should be applied. Where SDD measures are applied on the basis of an assessment of low ML/TF/PF risk, the customer due diligence (CDD) policies and procedures should clearly articulate the rationale and the applicable measures to be undertaken.
3. CDD is the identification and verification of both the customer and beneficiary including but not limited to continuous monitoring of the business relationship with the MOs. MOs are not permitted to operate anonymous accounts or accounts in fictitious names.

2.5.1 CUSTOMER DUE DILIGENCE (CDD)

CDD shall be conducted in accordance with section 30 of Act 1044.

1. An 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 and other financial technologies to effect the transaction. The following transactions are however, exempted:

i. where there is MO-to-MO transfers and settlements and both the originator person, and the beneficial person are MOs acting on their own behalf.
ii. there is a suspicion of ML/TF/PF, regardless of any exemptions or any other thresholds that may be referred to in these Guidelines or
iii. there are doubts about the veracity or adequacy of previously obtained customer identification data.

2. The MOs are not permitted to operate numbered accounts, anonymous accounts or accounts with fictitious names.

2.5.2 CUSTOMER DUE DILIGENCE (CDD) PROCEDURES

1. 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.
2. Types of customer information to be obtained and identification data to be used to verify the information are provided in **Appendix A**.
3. In respect of customers that are legal persons or legal arrangements, MOs shall:
    a. Verify the identity of the person purporting to have been authorized to act on behalf of such a customer and
    b. Verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from the Office of the Registrar of Companies or similar evidence of establishment or existence and any other relevant information.
4. The 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.
5. The MO shall, in respect of all customers, determine whether 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.
6. The MO shall take reasonable measures in respect of customers that are legal persons or legal arrangements to:

a. Understand the ownership and control structure of such a customer and
b. Determine the natural persons that ultimately own or control the customer.

7. Natural people include persons who exercise ultimate and effective control over the legal person or arrangement. Examples of types of measures needed to satisfactorily perform this function include;
    a. For companies – the natural persons are those who own the controlling interest and those who comprise the mind and the management of the company: and
    b. For trusts – the natural persons are the settlors, the trustees and person exercising effective control over the trust and the beneficiaries.
8. Where the customer or the owner of the controlling interest is a public company listed on a recognized securities exchange, a risk-based approach should be applied to identify and verify the identity of such a public company.
9. The MO shall obtain information on the purpose and intended nature of the business relationship of their potential customers.
10. The MO shall conduct ongoing due diligence on the business relationship as stated in **(9)**.
11. The ongoing due diligence in **(10)** 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.
12. The MO 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.
13. The MO shall screen all customers (both existing and new) against all domestic and international sanctions lists including Targeted Financial Sanctions (TFS) as well as TFS relating to Proliferation Financing (PF).

2.5.3 TIMING OF VERIFICATION

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

a. This can take place as soon as reasonably practicable;
b. It is essential not to interrupt the normal business conduct of the customer. This may include:
    i. non-face-to-face business
    ii. securities transactions
    iii. life insurance business
c. The ML/TF/PF risks can be effectively managed.

2. 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.

2.5.4 FAILURE TO COMPLETE CUSTOMER DUE DILIGENCE (CDD)

1. An MO which does not comply with Part B (2.5.2) shall:
    a. Not open the account, commence business relations or perform the transaction; and
    b. Submit an STR to the FIC within twenty-four (24) hours.
2. The MO that has already commenced the business relationship (without having performed the requirements under Part B (2.5.3) shall terminate the business relationship and submit an STR to the FIC within twenty-four (24) hours.
3. In addition, in the event that the MO does not comply with Part B (2.5.2), and it is detected during on-site inspection, the Commission shall apply the appropriate sanctions against the MO.

2.5.5 EXISTING CUSTOMERS

1. An MO 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.
2. The MO shall conduct CDD where:
    a. A transaction of significant value takes place, or

b. Customer documentation standards change substantially, or
c. There is a material change in the way that the account is operated, or
d. The MO becomes aware that it lacks sufficient information about an existing customer.

3. The MO shall identify the customer in accordance with the above-mentioned criteria and make the records available to the AMLRO and competent authorities as and when needed.

2.5.6 NEW BUSINESS FOR EXISTING CUSTOMERS

1. 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.
2. The customer shall be required to confirm the relevant details and to provide any missing KYC information, particularly where:
    a. An existing business relationship with the customer and identification evidence had not previously been obtained; or
    b. There had been no recent contact or correspondence with the customer within the past twelve (12) months; or
    c. A previously dormant account is re-activated.
3. 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.

2.5.7 RISK-BASED CUSTOMER DUE DILIGENCE (CDD)

While CDD measures are an important component of a robust AML/CFT/CPF framework, it is important to strike a balance between the objectives of ensuring financial inclusion and addressing ML/TF/PF risks in a risk sensitive manner. It is important that MO's CDD policy is not so restrictive or inflexible that it results in a denial of access to basic financial services, especially for those who are economically or socially vulnerable such as low-income groups, the elderly, the disabled, students and minors. This flexibility is relevant for financial inclusion since the vulnerable population find entry into the regulated financial system difficult as they often do not possess the required identification documents.

2.6 LOW RISK CUSTOMERS, TRANSACTIONS OR PRODUCTS

1. MOs shall apply reduced or simplified measures where there are low risks. There are low risks in circumstances where the risk of ML/TF/PF is low, where information on the identity of the customer and the beneficial owner of a customer is publicly available or where adequate checks and controls exist elsewhere in other public institutions. In circumstances of low risk, MOs shall apply the simplified or reduced CDD procedures when identifying and verifying the identity of their customers and the beneficial owners.
2. SDD procedures shall not be applied 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.
3. Examples of low-risk customers include but not limited to:
    i. MO-to-MO, provided they are subject to requirements for the AML/CFT/CPF which are consistent with the provisions of these Guidelines;
    ii. Public companies (listed on a stock exchange) that are subject to regulatory disclosure requirements;
    iii. Insurance policies for pension schemes if there is no surrender-value clause and the policy cannot be used as collateral;
    iv. 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;
    v. Refugees and asylum seekers; and
    vi. Any other low risk as may be determined by the National Risk Assessment findings
4. MOs shall prepare an internal risk assessment framework to identify, assess and take effective action to mitigate its ML/TF/PF risks.

2.7 HIGH-RISK CATEGORIES OF CUSTOMERS

1. An MO shall perform Enhanced Due Diligence (EDD) for high-risk categories of customers, business relationship or transaction. The MO is to adopt EDD procedures on a risk sensitive basis. In adopting the EDD procedures in determining the risk profile, the MO shall have regard to the type of customer, product, transaction, the location of the customer and other relevant factors.
2. Examples of high-risk customer categories include but not limited to:
    i. Non-resident customers;

ii. Legal persons or legal arrangements such as trusts, customer account that are personal assets holding vehicles;
iii. Companies that have nominee-shareholders or shares in bearer form;
iv. Politically Exposed Persons (PEPs);
v. Ministries, Department and Agencies (MDAs);
vi. Metropolitans, Municipals and District Assemblies (MMDAs) and other public institutions; High Net Worth individuals;
vii. Religious Leaders;
viii. Chief Executives and Board Members of private-owned companies/corporations or High-Risk industries/sectors using ISIC-Code
ix. Cross-border business relationships;
x. Natural or legal persons who do business in precious metals/minerals, petroleum;
xi. Designated Non-Financial Businesses and Professions (DNFBPs);
xii. Beneficial-owners of pooled-accounts held by DNFBPs provided that they are subject to requirements to AML/CFT/CPF consistent with the provisions of Act 1044.
xiii. Any customer deemed high-risk by the MO; and
xiv. And other high risk as may be determined by the National Risk Assessment findings.

3. The MO is required to take the following EDD procedures by making enquiries on:
    a. The purpose for opening the account;
    b. The level and nature of trading activities intended;
    c. The ultimate beneficial owners of the account;
    d. The source of funds; and
    e. The source of wealth.

2.8 SPECIFIC HIGH-RISK CUSTOMERS, ENTITIES, LOCATIONS OR TRANSACTIONS

2.8.1 POLITICALLY EXPOSED PERSONS (PEPs)

1. 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.
2. The MO shall ensure that its senior management gives approval before it establishes a business relationship with a PEP.

3. 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.
4. The 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 and the relevant competent authorities.
5. The MO 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 and the relevant competent authorities. Refer to Appendix **B** on categories of PEPs.

2.8.2 CROSS-BORDER CORRESPONDENT TRANSACTIONS

Cross-border correspondent transactions is the provision of financial services by one MO (the correspondent institution) to another MO (the respondent institution). Large international Financial Institutions typically act as correspondents for several others around the world. Respondent Institutions may be provided with a wide range of services, including securities trading such as shares, bonds, notes and private equity.

1. In relation to cross-border correspondent transactions and other similar relationships, MOs shall, in addition to performing the EDD procedures, take the following measures:
    i. Gather sufficient information about a correspondent institution to understand fully the nature of its business; and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether or not it has been subjected to a ML/TF/PF investigation or a regulatory action;
    ii. Assess the correspondent institution's AML/CFT/CPF controls and ascertain that the latter are in compliance with FATF standards;
    iii. Obtain approval from senior management before establishing correspondent relationships; and
    iv. Document the respective AML/CFT/CPF responsibilities of correspondent Institution.

2.8.3 SHELL COMPANIES

1. 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.
2. The MO 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.

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

1. 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 technologies.
2. The MO 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.

2.8.5 RELIANCE ON INTERMEDIARIES AND THIRD PARTIES ON CUSTOMER DUE DILIGENCE FUNCTION

1. 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:
   - **a.** Immediately obtaining from the third party the necessary information concerning certain elements of the CDD process;
   - **b.** 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;
   - **c.** Satisfying themselves that the third party is regulated and supervised in accordance with principles of AML/CFT/CPF and has measures in place to comply with the CDD requirements set out in these Guidelines;

d. 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

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

2. 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 the FATF Recommendations 10 and 11 and programmes against money laundering and terrorist financing, in accordance with the FATF Recommendation 18;
    ii. The implementation of those CDD, record keeping requirements and AML/CFT/CPF 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/CPF policies.
3. Without prejudice to the above, the MO, that relies on the third party for CDD shall have ultimate responsibility for customer identification and verification.

2.8.6 ATTENTION TO HIGH-RISK COUNTRIES

1. 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.
2. The 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.
3. The 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:
    a. 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;

b. 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;

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

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

2.8.7 FOREIGN BRANCHES AND SUBSIDIARIES

1. An MO shall ensure that their foreign branches and subsidiaries or parents observe group AML/CFT/CPF 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.
2. The MO 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/CPF 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.
3. The MO shall inform the SEC in writing when its foreign branches or subsidiaries or parent is unable to observe the appropriate AML/CFT/CPF procedures because they are prohibited by the host country's laws, regulations or other measures.
4. The MO is subject to these AML/CFT/CPF 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.
5. 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/CPF functions of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT/CPF purposes.
vii. Branches and subsidiaries receiving information from group level functions when the information is relevant and appropriate to risk management.
viii. Tipping-off provisions should not inhibit information sharing in the group.
i. Adequate safeguards on the confidentiality and use of information exchanged including safeguards to prevent tipping-off.

6. The MO is subject to these AML/CFT/CPF 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.

2.8.8 NON-PROFIT ORGANIZATIONS

2.8.8. 1 CLUBS AND SOCIEITIES

1. 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.
2. 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.

2.8.8.2 REGISTERED CHARITIES

1. An MO shall ensure that accounts are only opened for registered charities.
2. The MO shall obtain confirmation of the authority to act in the name of the charity. That confirmation is mandatory.

3. Accounts for charities shall be operated by a minimum of two signatories, duly verified and documentation evidence obtained.
4. The MO shall obtain and confirm the name and address of the charity concerned when dealing with an application from a registered charity.
5. 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.
6. 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.

2.8.8.3 RELIGIOUS ORGANIZATIONS (ROs)

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

2.9 TRANSACTION MONITORING, SUSPICIOUS ACTIVITY AND TRANSACTION REPORTING

2.9.1 DEFINITION OF A SUSPICIOUS TRANSACTION/ACTIVITY

For the purpose of these Guidelines, a suspicious transaction may be defined as one which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering methods. It includes 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 the transaction lacks an obvious economic rationale.

2.9.2 DEVELOPMENT AND IMPLEMENTATION OF INSTITUTIONAL POLICY

1. An MO shall have a written policy framework that would guide and enable its staff to monitor, recognize and respond appropriately to suspicious transactions. A list of Money Laundering "Red Flags" is provided in Appendix **C** of these Guidelines.
2. AMLROs shall supervise the monitoring and reporting of suspicious transactions/activities.
3. The MO shall be alert to the various patterns of conduct that have been known to be suggestive of ML/TF/PF and maintain a check list of such transactions/activities which shall be disseminated to the relevant staff.

4. When any staff of the MO detects any “red flag” or suspicious ML/TF/PF activity, the staff is required to promptly report to the AMLRO. Every action taken shall be recorded. The institution and its staff shall maintain confidentiality in respect of such investigation and any suspicious transaction report that may be filed with the FIC. This action is, however, in compliance with the provisions of Act 1044 which criminalizes “tipping off” (i.e., doing or saying anything that might alert or give information to someone else that he/she is under suspicion of ML/TF/PF).
5. The MO that suspects or has reason to suspect that funds or the proceeds of unlawful activity are related to terrorist financing, shall report within twenty-four (24) hours, its suspicions to the FIC. All suspicious transactions, including attempted transactions, are to 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.
6. The MO, their directors and employees (permanent and temporary) are prohibited from disclosing the fact that a report is required to be filed or has been filed with the FIC and any competent authority.

2.9.3 COMPLEX, UNUSUAL OR LARGE TRANSACTIONS

1. The MO shall pay special attention to all complex, unusual or large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. Examples of such transactions or patterns of transactions include significant transactions relative to a relationship, transactions that exceed prescribed limits, very high account turnover inconsistent with the size of the balance or transactions falls out of the regular pattern of the account activity.
2. The MO are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing. They are required to report such findings to the FIC within twenty-four (24) hours upon confirmation of suspicion.

2.10 TRANSACTION REPORTING

2.10.1 CASH TRANSACTION REPORT (CTR)

An MO shall report to the FIC through a prescribed medium all cash transactions within Ghana in any currency and with a threshold of GHS50,000.00 (or its foreign currency equivalent) or amounts as may be determined by the FIC.

2.10.2 ELECTRONIC CASH TRANSACTION REPORT (ECTR)

1. An MO shall institute policies and procedures to ensure funds transfer into or out of Ghana on behalf of a customer satisfy AML/CFT/CPF Regulations. Where The MO through electronic means and in accordance with the Foreign Exchange Act 2006 (Act 723) and Regulations made under that Act:
    a. transfers currency outside the country, or
    b. Receives currency from outside the country.
2. On behalf of a customer which exceeds the amount prescribed by the SEC, the MO shall within twenty-four (24) hours after the transfer or receipt of the currency, report the particulars of the transfer or receipt to the FIC through a prescribed medium all Electronic Transactions with a threshold of $1,000.00 or its Cedi equivalent for both.

2.10.3 OBLIGATIONS TO FILE CASH TRANSACTION REPORT (CTR) AND ELECTRONIC CASH TRANSACTION REPORT (ECTR)

An MO shall file CTRs and ECTRs to the FIC on transactions involving their customers whether or not the transactions are done directly or indirectly to the MO.

2.11 TRANSACTION MONITORING SYSTEMS

3. An MO must have appropriate processes in place that allow for the identification of unusual transactions, patterns and activities that are not consistent with the customer's risk profile.
4. The MO shall implement processes to analyze transactions, patterns and activities to determine if they are suspicious and meet the reporting threshold.
5. Transaction monitoring processes or systems may vary in scope or sophistication (automated and complex systems which integrate the customer data information. Regardless, the key element of any system is having up-to-date customer information to facilitate the identification of unusual activity.

6. Monitoring can be either:
    a. In real time, in those transactions and/or activities can be reviewed as they take place or are about to take place; or
    b. After the event through an independent review of the transactions and/or activities that a customer has undertaken.
7. The MO shall also have systems and procedures to deal with customers who have not had contact for some time, such as dormant accounts or relationships, to be able to identify future reactivation and unauthorized use.
8. In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer, product risk and delivery channels. Monitoring processes and systems shall enable trend analysis of transaction activities including monitoring of transactions with parties in high-risk countries or jurisdictions, to identify unusual or suspicious business relationships and transactions. The monitoring system shall enable AMLRO to monitor and report to Board and senior management on significant customer relationships and activities on an individual or consolidated basis across the financial group and identify activities that are inconsistent with the MO's knowledge of the customer, their business and risk profile.
9. The parameters and thresholds used to generate alerts of unusual transactions/activities shall be customized to be commensurate with MO's ML/TF/PF risk profile and the complexity and extent of its business activities. Standard parameters provided by the vendor may be used but the MO must be able to validate and demonstrate to the SEC that these are appropriate for the institution's risk position. The monitoring system shall be tested at most on a yearly basis to ensure that the parameters are performing as expected and remain relevant.
10. Modifications may be required as a result of such testing. Findings, analysis and the proposed modifications shall be documented indicating:
    a. The rationale for reviewing the parameters and thresholds;
    b. Details of testing; any assumptions made and the analysis of outcomes; and
    c. The changes made to the parameters and thresholds.
11. The MO shall refer to the guidance on conducting ML/TF/PF risk assessment of customers in Appendix **A** of these Guidelines for the implementation of a robust transaction monitoring system.

2.12 IDENTIFICATION OF DESIGNATED ENTITIES AND PERSONS AND FREEZING OF FUNDS

1. An MO must be able to identify and to comply with reporting and freezing instructions issued by the FIC regarding individuals and entities designated by the United Nations Security Council, OFAC, EU, His Royal Majesty or a competent authority as terrorist entities.
2. Notices issued by the FIC in this regard and the consolidated list shall be duly communicated to MOs.
3. In accordance with section 63 of Act 1044, MOs shall have specific obligations to immediately report to the FIC where any of the following apply:
    a. A person or entity named on the UN or third-party lists has funds in the MO;
    b. The MO has reasonable grounds to believe that the designated person or entity has funds in Ghana; and
    c. If the designated person or entity attempts to enter into a transaction or continue a business relationship, a suspicious transaction/activity report must be submitted immediately to the FIC.
4. The MO shall not enter into or continue such transaction with the designated person or entity. Funds already deposited with or held by the MO must remain frozen subject to the laws of Ghana.
5. It shall be noted that third party lists as set out in section 63 of Act 1044 and Act 762 as amended include an obligation to immediately freeze the funds of the listed entity.
6. In such cases, where the MO identifies funds of a listed person in Ghana, the MO should treat such funds as frozen pursuant to the Act 1044 and Act 762 as amended.
7. Terrorist screening is not a risk-based due diligence measure and must be carried out regardless of the customer's risk profile. MOs shall have processes in place to screen customer details and payment instructions against the designated lists of persons and entities and to ensure that the lists being screened against are up to date.
8. Screening measures shall consider:
    a. Continuous risk-based screening of customer records;
    b. Immediate screening of one-off, occasional transactions before the transaction is completed; and
    c. Procedures to screen applicable payment messages;
9. The MO's policies and procedures shall address:

a. The information sources used by the MOs for screening (including commercial databases used to identify designated individuals and entities);
b. The roles and responsibilities of the MO's employees and officers involved in the screening, reviewing and dismissing of alerts, maintaining and updating of the various screening databases and escalating potential matches;
c. The frequency of review of such policies, procedures and controls;
d. The frequency of periodic screening;
e. How potential matches from screening are to be resolved by the MO's employees and officers, including the process for determining that an apparent match is a positive hit and for dismissing a potential match as a false match; and
f. The steps to be taken by the AMLRO for escalating potential or positive matches to senior management and reporting suspicious or positive matches to the FIC.

2.12.1 TRADE/ECONOMIC SANCTIONS

1. Economic and trade sanctions are imposed against countries, governments, entities and persons with a view to bringing about changes in policies and behavior. Governments typically impose economic sanctions to give effect to decisions made by international organizations such as the United Nations or individual or groups of countries such as the United States, United Kingdom (His Royal Majesty), Canada or the European Union, AU, ECOWAS.
2. These may take the form of:
    a. Prohibitions against providing financial services;
    b. Travel bans;
    c. Embargoes on arms and military products; and
    d. Prohibitions or control of trade involving certain markets, services and goods.
3. The MO shall be aware of such sanctions and consider whether these affect their operations and any implications to the MO's policies and procedures particularly with respect to international transfers and its correspondent relationships. In addition to screening payment instructions to identify designated terrorists, MOs shall screen or filter payment instructions prior to their execution in order to prevent making funds available in breach of sanctions, embargoes or other measures.

4. In processing wire/electronic transfers, MOs shall take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per obligations set out in the relevant UNSCRs relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCRs 1267 and 1373 and their successor resolutions.

2.13 KNOW YOUR EMPLOYEE

1. In addition to knowing the customer, MOs shall have robust procedures in place for knowing its employees. In this regard, every MOs shall have a recruitment policy to attract and retain employees with the highest levels of integrity and competence. The ability to implement an effective AML/CFT/CPF programme depends in part on the quality and integrity of employees.
2. Consequently, MOs shall undertake due diligence on prospective employees and throughout the course of employment. At a minimum, the MOs shall:
    a. Verify the applicant's identity and personal information including employment history and academic qualification and also consider credit history checks on a risk-based approach;
    b. Develop a risk-based approach to determine when pre-employment background screening is considered appropriate or when the level of screening should be increased, based upon the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which shall include verification of references, experience, education and professional qualifications;
    c. Maintain an ongoing approach to screening for specific positions, as circumstances change, or for a comprehensive review of employees over a period. Internal policies and procedures shall be in place (e.g. codes for conduct, ethics, conflicts of interest) for assessing employees;
    d. Have a policy that addresses appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or employee provided. Verification shall generally include the following:
        i. Reference checks

ii. Checking the authenticity of academic qualifications
iii. Verifying Employment History
iv. Police background checks
v. Integrity checks against SEC Engaged and Disengaged Database of Directors, AMLROs and Licensed Representatives of MOs, Market Register and Reviewer's Checklist
vi. The MO shall document and keep evidence of the above processes.

3. The MO shall in addition maintain records of the names, addresses, position, titles and other official information pertaining to employees appointed or recruited in accordance with Section 32 of Act 1044.
4. The MO, to the extent permitted, shall ensure the laws of the relevant country and similar recruitment policies are followed by its branches, subsidiaries and associate companies abroad, especially in those countries which are not sufficiently compliant with FATF standards.
5. In addition to a robust recruitment policy, MOs shall implement ongoing monitoring of employees to ensure that they continue to meet the institution's standards of integrity and competence.
6. The MO shall establish and maintain procedures to ensure high standards of integrity among employees, including the meeting of statutory "fit and proper" criteria of the officers of the MO. Integrity standards shall be documented and accessible to all employees. These internal procedures may include standards for:
    a. Acceptance of gifts from customers;
    b. Social liaisons with customers;
    c. Disclosure of information about customers who may be engaged in criminal activity;
    d. Confidentiality;
    e. Detection of any unusual growth in employees' wealth; and
    f. Deterring employees from engaging in illegal activities that can be detected by reference to his investment records.
7. The standards shall include a code of ethics for the conduct of all employees and procedures shall allow for regular reviews of employees' performance and their compliance with established rules and standards. It shall also provide for disciplinary action in the event of breaches of these rules.

2.13.1 MONITORING OF EMPLOYEE CONDUCT

1. An MO shall monitor employees' accounts for potential signs of ML/TF/PF and pay particular attention to employees whose lifestyles cannot be supported by their salary or known financial circumstances. Supervisors and managers shall be encouraged to know the employees in their department and investigate any substantial changes in their lifestyles which do not match their financial position.
2. The MO shall also subject employees' accounts, including accounts of key management personnel, to the same AML/CFT/CPF procedures as applicable to other customers' accounts. This is required to be performed under the supervision of the AMLRO.
3. The AMLRO's account is to be reviewed by the Internal Auditor or any other Senior Officer designated by the Management of the MO.
4. Compliance reports including findings on the AMLRO's account shall be submitted to the SEC and FIC on/or before 31st July (half-year) and on/or before 31st January (End of Year) of the following year.
5. The AML/CFT/CPF performance review of staff shall be part of employees' annual performance appraisal.

2.13.2 AML/CFT/CPF STAFF, MANAGEMENT AND BOARD EDUCATION AND TRAINING PROGRAMME

1. An MO shall design comprehensive staff, management and board of directors' 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/CPF obligations.
2. The MO shall submit its annual AML/CFT/CPF staff, management and board training programme for the ensuing year to the SEC and FIC not later than the 31st of December every financial year.
3. The staff, management and board training programme shall be developed by management with the support of the AMLRO and approved by the Board.
4. The training programme shall include:
    - **i.** ML/TF/PF regulations and offences;
    - **ii.** The nature of money laundering;
    - **iii.** ML/TF/PF 'red flags' and suspicious transactions, typologies related to the Securities Sector;

iv. Reporting requirements;

v. Customer due diligence;

vi. Risk-based approach to AML/CFT/CPF regime;

vii. Record keeping and retention policy;

viii. Training on SEC/FIC AML/CFT/CPF Guidelines and Administrative Sanctions; and

ix. Other emerging ML/TF/PF risks such as digital products.

5. The MO shall fully participate in all AML/CFT/CPF programmes or activities organized by SEC or FIC. Failure to participate shall attract sanctions from SEC.

2.13.3 WHISTLE BLOWING/ PROTECTION OF STAFF WHO REPORT AML/CFT/CPF VIOLATIONS

An MO shall develop policies on whistleblowing. These policies shall at a minimum:

1. Direct its employees in writing to co-operate fully with the Regulators and Law Enforcement Agencies.
2. Make provision for the Board, Management and Staff to report any violations of the MO's AML/CFT/CPF compliance programme to the AMLRO or a designated higher authority where the violation involves the AMLRO. In cases where the violations involve the AMLRO, Board, Management and Staff are required to report such to a designated higher authority such as the Internal Auditor.
3. Ensure compliance with the SEC Conduct of Business Guidelines and the Whistleblower Act, 2006 (Act 720) with respect to protection for making disclosure of impropriety and
4. Inform their Board, Management and Staff in writing to make such reports confidential and that they will be protected from victimization for making them.

2.14 RECORD KEEPING

An MO shall keep books and records with respect to customers and transactions in accordance with Section 32 of Act 1044.

2.14.1 MAINTENANCE OF RECORDS ON TRANSACTIONS

1. An MO is required to maintain all necessary records of transactions, both domestic and international, in accordance with Section 32 of Act 1044.
2. The MO shall maintain these records in a manner that upon request by the SEC, FIC or any other competent authority can be made readily available.
3. The above requirements apply regardless of whether the account or business relationship is ongoing or has been terminated.
4. Examples of the necessary components of transaction-records include:
    a. Customer's and beneficiary's names;
    b. Addresses (or other identifying information normally recorded by the intermediary);
    c. The nature and date of the transaction;
    d. The currency and amount involved; and
    e. The type and identification number of any account involved in the transaction.
5. The MO shall maintain records of the identification data, account files and business correspondence in accordance with Section 32 of Act 1044.
6. The MO shall ensure that all customer-transaction records and information are made available on a timely basis.
7. The MO shall maintain records of transactions, both domestic and international, for at least five (5) years after completion of the transaction to which they relate.
8. The MO shall ensure that all customers' transaction records and information are available on a timely basis to the SEC and the FIC.

2.14.2 RECORDING IDENTIFICATION EVIDENCE

a. An MO shall keep record of the supporting evidence and methods used to verify identity for a minimum period of five (5) years after the account is closed or the business relationship has ended.

b. The MO shall keep record of the actual information obtained or of where it can be re-obtained after electronic checks are made. The record must be retained as part of the identification evidence.

c. The 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.

d. Despite subsection (c), 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.

2.15 ADDITIONAL PROCEDURES AND MITIGANTS

1. An MO shall review the AML/CFT/CPF 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/CPF Compliance Programme.
2. Details of the contingency plan shall be submitted to the SEC and FIC not later than 31st December of every financial year.

PART C
3.0 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 suspicion.

3.1 WHAT IS IDENTITY

1. It is important to distinguish between identifying the customer and verifying identification. Customer identification entails the gathering of information on the prospective customer to enable identification.
2. Identity as set out in the National Identity Register Act, 2008 (Act 750), its Regulations and the SEC notice on the use of the Ghana Card as the sole identifier is a set of attributes such as name(s), date of birth, residential address including the GPS code and digital address, biometric data and other information of the customer. These are features which are unique and identify a customer.
3. Where an international passport is taken as evidence of identity for diplomats, the number, date and place/country of issue (as well as expiry date where applicable) shall be recorded.
4. The identity of a customer who is a legal person is a combination of its constitution, its business and its legal and ownership structure.

3.2 DUTY TO OBTAIN IDENTIFICATION EVIDENCE

1. An MO shall conduct know your customer procedures to ascertain the identity of a prospective customer.
2. In the case of a person acting on behalf of another, the MO shall be obliged to obtain sufficient evidence of the identities of the two persons involved.
3. The MO has a duty to obtain evidence in respect of its customers except under Part C 3.6. (3) of these Guidelines.

3.3 NATURE AND LEVEL OF THE BUSINESS

1. 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.
2. The information collected shall include:

a. The purpose and reason for opening the account or establishing the relationship;
b. Nature of the activity that is to be undertaken;
c. Expected origin of the funds to be used during the relationship and
d. Details of occupation/employment/business activities and sources of wealth or income.

3. The 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.

3.4 COMMERCIAL JUDGMENT

1. An MO shall take a risk-based approach to the KYC requirements.
2. The 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.
3. The holder of a personal account including joint-accounts holders shall be verified.
4. In respect of a private company or a partnership, the identities of the principal owners/controllers shall be verified.
5. The identification evidence collected shall be viewed against the inherent risks in the business or service.

3.5 ESTABLISHMENT OF IDENTITY

1. 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.
2. The process of verification, validating and updating identity, and the extent of obtaining additional KYC/CDD information shall be the sole prerogative of the National Identification Authority (NIA) for individuals' resident/working in Ghana and the Office of the Registrar of Companies for legal persons (entities).
3. The general principles for establishing the identity of both legal and natural persons and the procedures of obtaining satisfactory identification evidence at minimum are set out below.
4. An MO shall obtain sufficient information on the:

a. nature of the business that their customer intends to undertake, including the expected or predictable pattern of transactions;
b. purpose and reason for opening the account or establishing the relationship;
c. nature of the activity that is to be undertaken;
d. expected origin of the funds to be used during the relationship; and
e. details of occupation/employment/business activities and sources of wealth or funds (income).

5. The MO shall take reasonable steps to keep the information up to date as the opportunities arise, such as when an existing customer opens a new account. Information obtained during any meeting, discussion or other communication with the customer shall be recorded and kept in the customer's file to ensure, as far as practicable, that current customer information is readily accessible to the AMLRO or relevant regulatory bodies.
6. The general principles for establishing the identity of both legal and natural persons and the procedures for obtaining satisfactory identification evidence set out in these Guidelines are by no means exhaustive.

3.6 VERIFICATION OF IDENTITY

1. 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.
2. 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.
3. 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 and national identity card are taken as evidence of identity, the number, date and place/country of issue (as well as expiry date where applicable) shall be recorded.
4. 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).

5. 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.
6. The MO may not look beyond the client where:
    a. The agent is acting on its own account (rather than for a specific client or group of clients);
    b. The client is a bank, broker, fund manager or another regulated MO and
    c. All the businesses are to be undertaken in the name of a regulated MO.
7. 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:
    3. The named account holder/person in whose name an investment is registered;
    4. Any principal beneficial owner of funds being invested who is not the account holder or named investor;
    5. The principal controller(s) of an account or business relationship (i.e., those who regularly provide instructions); and
    6. Any intermediate parties (e.g., where an account is managed or owned by an intermediary).
8. The MO shall take appropriate steps to identify directors and all the signatories to an account.
9. Where it is a joint account, identification evidence shall be obtained for the account holders.
10. 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).
11. The 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.
12. 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.

3.7 CUSTOMERS TO BE VERIFIED

1. The MO shall:
    a. Verify the identity of customers (natural/legal) to ascertain that the customer is the very person he/she claims to be.
    b. Verify the identity of the person acting on behalf of another and obtain and verify the identities of the other persons involved.
    c. Take appropriate steps to identify directors and all signatories to an account.
    d. Verify all parties in joint accounts.
2. For high-risk business undertaken for private companies (i.e. those not listed on the stock exchange) sufficient evidence of identity and EDD procedures shall be conducted in respect of:
    i. the principal underlying beneficial owner(s); and
    ii. persons with a controlling interest in the company.
3. The MO shall be alert to circumstances that might indicate any significant changes in the nature of the business or its ownership (controlling interest) and make enquiries accordingly and to observe the additional provisions for High-Risk Categories of Customers as provided in these Guidelines.
4. The MO shall obtain and verify the identity of those providing funds for the trust. They include 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.
5. When one MO acquires the business and accounts of another MO, it shall identify all the acquired customers. It is also mandatory to carry out due diligence procedures to confirm that the acquired institution has conformed with the requirements in these Guidelines prior to the acquisition.

3.8 TIMING OF IDENTIFICATION REQUIREMENTS

1. 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.

2. Subject to Part 3.8 (1) above an MO shall:
    a. Obtain identification evidence within ninety (90) days after it has contact with a customer with a view to agreeing with the customer to carry out an initial transaction; or reaching an understanding (whether binding or not) with the customer that it may carry out future transactions; and
    b. 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.
3. The MO shall also observe the provision in the Timing of Verification under the AML/CFT/CPF under these Guidelines.
4. The MO may start processing the business or application immediately, provided that it:
    a. Promptly takes appropriate steps to obtain identification evidence; and
    b. Does not transfer or pay any money out to a third party until the identification requirements have been satisfied.
5. The failure or refusal by an applicant to provide satisfactory identification evidence within the timeframe as set above with no 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.
6. The MO shall have in place written and consistent policies for closing an account or unwinding a transaction where satisfactory evidence of identity cannot be obtained.
7. The MO shall respond promptly to enquiries made by competent authorities.

3.9 CERTIFICATION OF IDENTIFICATION DOCUMENTS

1. An MO shall not require a prospective customer to send by post originals of valuable personal identity documents.
2. In order to guard against the dangers of identity fraud and ML/TF/PF risks, MOs shall take adequate steps to verify the authenticity of the documents with the issuing or identification authority in order to guard against the dangers of identity fraud and ML/TF/PF risks, MOs shall take adequate steps to verify the authenticity of the documents with the issuing or identification authority

3. 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:
    a. The embassy, consulate or high commission of the country of issue; or
    b. A lawyer, attorney or notary public; or
    c. Issuing authority.

3.10 RISK-BASED APPROACH TO CUSTOMER IDENTIFICATION AND VERIFICATION

1. An MO shall take a risk-based approach to the KYC/CDD requirements for all customers. Furthermore, MOs shall decide on the number of times to verify the customer's records during the relationship, the identification evidence required and when additional checks are necessary. These decisions shall equally be recorded.
2. The identification evidence collected at the outset shall be viewed against the inherent risks in the business or service.

3.11 RISK-BASED CUSTOMER DUE DILIGENCE

3.11.1 LOW RISK/SIMPLIFIED DUE DILIGENCE

1. With a risk-based approach, where the identified ML/TF/PF risks are low, MOs shall apply SDD. SDD shall be commensurate with the identified low risk factors (e.g., the simplified measures may relate only to customer acceptance measures or to aspects of ongoing monitoring). It shall be noted that SDD never means a complete exemption or absence of CDD measures but rather, MOs may adjust the frequency and intensity of measures to satisfy the minimum CDD standards. MOs are reminded that simplified measures are not acceptable whenever there is suspicion of ML/TF/PF risks or where specific high risk is determined.
2. With respect to beneficial ownership in a financial inclusion context, the beneficial owner will in most instances be the customer himself or a closely related family member. Where there is a suspicion of ML/TF/PF, that the account owner is being used as a rogue and is not the beneficial owner, enhanced due diligence measures shall be applied and an internal suspicious report must be filed with the AMLRO and a subsequent report to FIC.

3. These Guidelines identify the specific instances when SDD measures may be applied including where low risks have been identified through a national risk assessment or through an adequate assessment of ML/TF/PF risk by the MO.
4. In addition, the MO shall, based on their risk assessments, apply SDD to specifically defined low risk customers or products and services. Such instances may include but are not limited to:
    a. Customers whose sole source of funds is a salary credit to an account or with a regular source of income from a known source which supports the activity being undertaken;
    b. Pensioners, social benefit recipients or customers whose income originates from their spouses'/partners' employment; and
    c. Customers represented by those whose appointment is subject to legal instruments.
5. For customers who do not have photo identification or have limited identification documentation such as tourists or those who are socially or economically vulnerable such as the disabled, elderly, minors or students, a 'tiered' SDD approach allows financial access with limited functionality. For example, MO shall offer banking accounts with low transaction/payment/balance limits with reduced documentation requirements. Access to additional services such as higher transaction limits or account balances or access to diversified delivery channels shall only be allowed if and when the customer can satisfy additional identification requirements. Where this applies, the MO shall have monitoring systems to ensure that transaction and balance limits are observed.
6. The MO shall ensure that the customer shall provide the valid identification (Ghana Card) within ninety (90) days.
7. Where there is suspicion of ML/TF/PF risk, the MOs shall not apply SDD measures.

3.11.1.2 ILLUSTRATIONS OF SDD MEASURES

The SDD measures described below are minimum requirements. Where an MO determines, based on its risk assessment that the ML/TF/PF risks are low, the MO shall apply the following SDD measures:

1. Adjust the timing of SDD where the product or transaction has features that limit its use for ML/TF/PF purposes.

MOs shall verify the customer's or beneficial owner's identity after the establishment of the business relationship where financial products or services provided have limited functionality or restricted services to certain types of customers for financial inclusion purposes. For example, limits shall be imposed on the number or total value of transactions per week/month; the product or service shall only be offered to nationals or only domestic transactions shall be allowed. Similarly, general insurance products such as car insurance present low ML/TF/PF risk so verification of identity may be postponed until there is a claim or until the customer requests additional insurance products. In such instances, MOs must ensure that:

i. This does not result in a de facto exemption from SDD and that the customer or beneficial owner's identity will ultimately be verified;
ii. The threshold or time limit is set at a reasonably low level;
iii. Systems are in place to detect when the threshold or time limit has been reached; and
iv. SDD is not deferred or obtaining relevant information about the customer is not delayed where high risk factors exist or where there is suspicion of ML/TF/PF.

2. Adjust the quality or source of information obtained for identification, verification or monitoring purposes.

Where the risk associated with all aspects of the relationship is very low, the MO shall rely on the source of funds to meet some of the SDD requirements. For example, the purpose and intended nature of the relationship shall be inferred where the sole inflow of funds are government pension or benefit payments.

3. Adjust the frequency of SDD updates and reviews of the business relationship.

This shall be applied for example when trigger events occur such as the customer requesting a new product or service or when a certain transaction threshold is reached. The MO shall ensure that this does not result in a de facto exemption from keeping SDD information up to date.

4. Adjust the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only.

Where the MO chooses to do SDD procedures, they shall ensure that the threshold is set at a reasonable level and that systems are in place to identify linked transactions which, when aggregated, exceed the threshold.

3.11.1.3 FINANCIAL INCLUSION

1. An MO shall have financial inclusion policies for the socially and financially disadvantaged citizens in Ghana.
2. Access to basic financial services is a necessary requirement for most adults. It is important therefore that the socially and financially disadvantaged shall not be excluded from opening accounts or obtaining other financial services merely because they do not possess evidence to identify themselves. In circumstances where they cannot reasonably do so, the internal procedures of the MOs shall make allowance for such persons by way of providing appropriate advice to staff on how the identities of such group of persons can be confirmed and what checks shall be made under these exceptional circumstances.
3. Where the MO has reasonable grounds to conclude that an individual customer is not able to produce the detailed evidence of his/her identity and cannot reasonably be expected to do so, the MO shall do the following:
    a. Accept as identification evidence a letter or statement from a person in a position of responsibility who knows the customer and can confirm that the customer is who he/she says he/she is, including confirmation of his/her permanent address;
    b. Accept and verify the identity of the guarantor;
    c. Offer basic low risk account services;
    d. Have a 90-day deferral waiver for the customer to obtain the Ghana Card;
    e. Where the customer does not supply the required information as stipulated above, the MO shall immediately discontinue any activity it is conducting for the customer; and
    f. Where the MO suspects any unusual or ML/TF/PF risks, the MO shall file an STR to FIC.

3.11.2 ENHANCED DUE DILIGENCE (HIGH-RISK)

1. An MO is required to apply EDD for such categories of customers, business relationships or transactions that are determined to present high ML/TF/PF risk due to business activity, ownership structure, nationality, residence status, politically exposed status or other high-risk indicators.

2. The MO's policy framework shall therefore include a description of the type of customers that are likely to pose higher than average risk and the EDD procedures to be applied in such instances. The commencement of a business relationship with a high-risk customer shall be approved by senior management. Senior management shall receive sufficient information to make an informed decision on the level of ML/TF/PF risk the institution would be exposed to if it enters into or continues that business relationship and how well equipped it is to manage that risk effectively.
3. The MO shall also ensure that monitoring systems are appropriately tailored and provide timely and comprehensive reports to facilitate effective monitoring of such relationships and periodic reporting on such relationships to Board and senior management.
4. Act 1044 and these Guidelines identify specific instances that MOs must always treat as high-risk and to which EDD must be applied. EDD shall be applied in the following circumstances:
    a. Business transactions with persons and MOs in or from other countries which do not or insufficiently comply with the FATF Standards;
    b. Complex, unusual or large transactions, whether completed or not, to all unusual patterns of transaction and to insignificant but periodic transactions which have no apparent economic or visible lawful purpose;
    c. Where ML/TF/PF risks are high;
    d. When establishing correspondent banking relationships;
    e. Where high-risks have been identified with a PEP customer; and
    f. Non-face to face business relationships or transactions
5. The MO shall exercise due caution if entering into business relationships or otherwise doing business with persons from high-risk jurisdictions named in Public Statements issued by international organizations such as OFAC, EU, His Royal Majesty (UK), UNSCRs, FATF, AU and ECOWAS.

3.11.2.1 ILLUSTRATIONS OF EDD MEASURES

a. When a new customer falls within high-risk category, or an MO launches a high-risk product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the following shall apply:
    i. Increase the quantity/quality of information obtained for EDD purposes (e.g., request additional information as to the customer's residential status, employment,

salary details and other sources of income) and requesting additional documentary evidence or utilizing publicly available sources (e.g., scrutiny of negative media news, internet searches, use of social media).

ii. Understand the customer's ownership and control structure to ensure that the risk associated with the relationship is well-known. This may include obtaining and assessing information regarding the customer's reputation, including any negative media allegations against the customer.

iii. Understand the intended nature of the business relationship and the reasons for intended or performed transactions. This may include obtaining information on the number, size and frequency of transactions that are likely to be conducted. It may be appropriate to request a customer's business plans, cash flow projections, copies of contracts with vendors etc.

iv. Understand why the customer is requesting a certain service or product particularly when it is unclear why the customer is seeking to establish business relationships in another jurisdiction from where he is domiciled. The account shall be regularly monitored to establish a full view of the nature of activity and whether it fits with the initial risk profile of the customer.

v. Establish the source of funds or source of wealth of the customer. Where the risk associated with the customer is particularly elevated, intrusive measures to verify the source of funds and wealth may be the only adequate risk mitigation measure. Possible sources may be reference to VAT and income tax returns, pay-slips, title deeds or, if from an inheritance, request a copy of the will or documentation to evidence divorce settlement or sale of property or other assets.

vi. Evaluate the principals and conduct reference checks and checks of electronic databases;

vii. Review current financial statements; and

viii. Conduct enhanced, ongoing monitoring of the business relationship, by increasing the number and timing of controls applied, and through more frequent formal reviews.

b. The availability and use of other financial information held is important for reducing the additional costs of collecting customer due diligence information and can help increase AI's

understanding of the risk associated with the business relationship. Where appropriate and practical and where there are no data protection restrictions, MOs shall take reasonable steps to ensure that where customer due diligence information is available in one part of the business, there are information sharing mechanisms to link it to information held in another.

3.11.2.2 ENHANCED MONITORING

The following are examples of measures an MO shall employ to monitor high-risk customers:

a. Conducting more frequent reviews of the business relationship and establishing more stringent thresholds for updating EDD information;
b. Setting specific business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
c. Requiring senior management approval at the transaction level for products and services that are new for the customer;
d. Reviewing transactions more frequently against red flag indicators relevant to the relationship. This may include establishing the purpose and destination of funds and obtaining more information on the beneficiary before conducting the transaction;
e. Flagging unusual activities and escalating concerns and transactions for senior management's attention.

3.11.3 VIRTUAL ASSETS (VAS) AND VIRTUAL ASSETS SERVICE PROVIDERS (VASPS)

a. FATF defines Virtual Asset (VA) as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.
b. Virtual Asset Service Provider (VASP) means any natural or legal person who is not covered elsewhere under the Recommendation and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
    i. Exchange between virtual assets and fiat currencies;
    ii. Exchange between one or more forms of virtual assets;
    iii. Transfer of virtual assets;

iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

c. The emergence of VAs such as virtual currencies has attracted investments and payment infrastructure that provides new methods for creating and transmitting value. Transactions in VAs are largely untraceable and anonymous and making it susceptible to ML/TF/PF activities. VAs are traded on exchange platforms that are unregulated in some jurisdictions. Customers may therefore lose their investments without any regulatory intervention in the event that a VASP collapses or closes their business.

d. Although VASPs are not currently regulated in Ghana, MOs must identify the "Red Flags "relating to VAs and VASPs as stated in **Appendix C**.

e. The following measures should also be considered to identify, assess and understand the ML/TF/PF risk of VAs and VASPs:

i. An MO shall identify and assess the ML/TF/PF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies such as virtual assets and virtual asset service providers for both new and pre-existing products.

ii. The MO shall undertake risk assessment prior to the launch, use or establishment of business relationships with customers in new or developing technologies, products and practices such as VA/VASP.

iii. The MO shall identify and assess the ML/TF/PF risks emerging from virtual assets activities and the activities or operations of VASPs.

iv. The MO shall take appropriate measures to manage and mitigate such risks.

v. The MO, based on their understanding of their risks shall apply a risk-based approach to ensure that measures to prevent or mitigate ML/TF/PF are commensurate with the risks identified.

vi. The MO shall take steps to identify natural or legal persons that carry out VASP activities without the requisite license or registration.

vii. The MO shall report SAR/STR on identified VASP activities to the FIC within twenty-four (24) hours.

3.12 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.

3.13 PENSION SCHEMES

3.13.1 PERSONAL PENSION SCHEMES

1. 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.
2. 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.

3.13.2 OCCUPATIONAL PENSION SCHEMES

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.

3.13.3 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.

3.14 CANCELLATION AND 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.

3.15 REDEMPTIONS

1. 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.
2. An MO shall take reasonable measures to establish the identity of the investor where payment is made to:
    - **a.** The legal owner of the investment by means of a cheque crossed "account payee only" or
    - **b.** 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.

3.16 CLOSURE OF ACCOUNTS

An MO shall put in place policies and procedures to facilitate the closure of a customer account in the following circumstances:

1. Where a customer decides to redeem his/ her funds and close the investment account;
2. Where the MO decides to terminate the business relationship with the customer due to threats or other risk factors that cannot be mitigated;
3. Where the customer closes one investment account and opens another investment account.
4. Any other circumstances that may warrant the closure of an investment account.

3.17 EXEMPTION FROM IDENTIFICATION PROCEDURES

Where a customer's identity was not properly obtained as contained in this 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 this Guidelines, except where it concerns:

1. An MO regulated by the requirements of these Guidelines and
2. Re-investment of Income.

3.18 IDENTIFICATION PROCEDURES

3.18.1 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.

3.18.2 MUTUAL/FRIENDLY, COOPERATIVE AND PROVIDENT SOCIETIES

Where these entities are applicants 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.

3.18.3 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, the MO shall take steps to verify the founder, the managers/directors and the beneficiaries.

3.18.4 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.

3.18.5 CONCESSION IN RESPECT OF POSTAL AND ELECTRONIC PAYMENTS SYSTEMS

i. 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.

ii. 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.

iii. Reliance on the post 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.

iv. 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.

v. 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.

vi. 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.

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

viii. The 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.

ix. 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.

3.18.6 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.

3.19 GENERAL INFORMATION ON ESTABLISHING IDENTITY

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

1. Private individual customers;
2. Quasi corporate customers;
3. Unincorporated businesses/partnerships; and
4. Corporate customers.

3.19.1 PRIVATE INDIVIDUALS

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 new address shall be validated.

c. Date of birth may be required to confirm identity. However, this 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.

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

f. 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.

3.19.1.2 PRIVATE INDIVIDUALS RESIDENT IN GHANA

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.

3.19.1.3 DOCUMENTING EVIDENCE OF IDENTITY

In order to guard against forged or counterfeit documents, care shall be taken to ensure that documents offered are verified.

3.19.1.4 DOCUMENTARY EVIDENCE OF ADDRESS

a. MO shall apply a risk-based approach for documentary evidence of address. Acceptable documentary evidence for address include:

- **i.** Record of home/office visit by the MO
- **ii.** Recent utility bill including Water, Electricity and Telephone bills
- **iii.** Property Rate bill

iv. Bank statement or passbook containing current address
v. Search report from the Lands Commission
vi. Tenancy Agreement
vii. validated in line with the issuing authority
viii. State/Local Government Rates documents
ix. Search reports on prospective customer's place residence signed by an AMLRO of the MO.
x. Statutory Declaration confirming residence.

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.

3.19.1.5 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. The MO 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.

3.19.1.6 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 may 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 public records where available.
- **ii.** Access to internal or external account database; and

3.19.1.7 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. 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. The MO shall obtain evidence directly from the customer or through the MO or any other financial institution 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. The 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 shall be made to his or her evidence of traveling documents to verify the applicant's identity and residential address.

3.19.1.8 SUPPLY OF INFORMATION FOR PRIVATE INDIVIDUALS NOT RESIDENT IN GHANA

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, 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. The MO shall use these requirements in conjunction with **Appendix A** to these Guidelines.

3.19.1.9 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. The 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.

3.19.1.10 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.

3.19.1.11 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 complete the standard account opening documentation on behalf of the student.

3.19.2 QUASI CORPORATE CUSTOMERS

3.19.2.1 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. The 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.

3.19.2.2 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. The 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. The 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.

3.19.2.3 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 the 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 the 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. The 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.

3.19.2.4 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.

3.19.2.5 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.

3.19.2.6 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 records.

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

c. Where the professional intermediary is not covered under the AML/CFT/CPF 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 the 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 these Guidelines. The 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.

3.19.3 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.

3.19.4 CORPORATE CUSTOMERS

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 a shell company where the controlling principals cannot be identified.
b. The MO shall identify a corporate body by the following:
    i. Registration number;
    ii. Incorporation number;
    iii. Registered corporate name and any trading names used;
    iv. Registered address and any separate principal trading addresses;

v. Directors;
vi. Shareholders;
vii. The Objectives of the company's business;
viii. Trademarks and logos;
ix. Regulations of the company;
x. Tax Identification Number (TIN)

3.19.4.1 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. 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.

3.19.4.2 LOW RISK CORPORATE BUSINESS

1. **LISTED COMPANIES**
   i. An MO shall verify the identity of a shareholder or director of a listed company where there is suspicion.
   ii. The 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.
   iii. 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. **UNLISTED 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 Office of the Registrar of Companies 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 Office of the Registrar of Companies.

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.

3.19.4.3 HIGH-RISK BUSINESS

1. PUBLIC COMPANIES

Where a public company is undertaken 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 Office of the Registrar of Companies or an enquiry via a business information service or an undertaking from a firm of lawyers or accountants confirming the documents submitted to the Office of the Registrar of Companies

iii. A certified true copy of the resolution of the Board to open an account and confer authority on those who will operate it; and

iv. The regulations of the company.

2. PRIVATE COMPANIES

i. 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).

ii. 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.

iii. The MO shall also identify directors who are not principal controllers and signatories to an account for risk-based approach purpose.

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

v. 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.

vi. 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.

vii. The 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.

3.19.4.4 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.

3.19.4.5 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 with 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 the MO in Ghana.

3.19.4.6 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.

3.19.4.7 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 or other electronic means (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 other verbal 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 five (5) years.

e. **Introduction from Foreign Financial 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 Introduction of Customers:**

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 AML 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 to the extent of KYC information that is available.

h. The 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, the MO shall, in addition to verifying the agent, establish the identity of the underlying client.

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

i. Is bound by and has observed these Guidelines or the provisions of 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/CPF Legislation, the Risk-based approach shall be observed by the MO under such circumstances.

3.19.4.8 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 who 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.

3.19.4.9 VULNERABILITY OF RECEIVING MARKET OPERATORS 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.

3.19.4.10 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 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.

3.19.4.11 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 AML 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.

3.19.4.12 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.

3.19.4.13 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 have 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.

4.0 TERRORIST FINANCING AND 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) and Anti-Terrorism Act, 2008 (Act 762), as amended.

5.0 REPORTING REQUIREMENTS

An MO shall submit the following reports:

1. Fraud and defalcation report to SEC and FIC as and when they are detected;
2. FIC semi-annual compliance report to SEC and FIC to be submitted not later than 31st July and 31st January of the reporting year.
3. FIC end of year compliance report to SEC and FIC not later than 31st January of the reporting year.
4. Semi-annual SEC Data Capture returns to SEC to be submitted not later than 31st July and 31st January of the reporting year.
5. Semi-annual SEC Risk Management returns to SEC to be submitted not later than 31st July and 31st January of the reporting year.
6. End of year AML/CFT/CPF employee education and training report to the SEC and FIC to be submitted not later than 31st December of every year.

7. CTRs/STRs/ECTRs as and when detected.
8. Updated PEP List.

Refer to **Appendix K** for further information.

APPENDIX A:

INFORMATION TO ESTABLISH IDENTITY

The table below provides the minimum KYC/CDD verification of identity requirements for both foreign and domestic natural and legal persons. These requirements shall be used together with the minimum Standardized KYC Forms as issued by the SEC.

MINIMUM REQUIREMENTS FOR VERIFICATION AND KYC/CDD FOR NEW AND EXISTING CUSTOMERS		
Customer Type	Customer Sub-type	Identification/Verification Requirements

Individuals	Ghanaian Citizen	1. Ghana Card KYC Data Set 2. Additional minimum requirements; Proof of Residential Address: i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized government agency orinstitution.
	Ghanaians Living Abroad	1. Ghana Card KYC Data Set 2. Additional minimum requirements; a. Proof of Residential address (foreign): i. Utility Bill, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized government agency or institution. b. <u>Supplementary requirement</u> Proof of Residential Address (local) i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document
	Foreigners with Permanent Residence in Ghana	1. Non- Citizen Card KYC Data Set 2. Additional minimum requirements; a. Proof of Residential Address (local): i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document. b. Proof of Residential address (foreign) i. Utility Bill, or ii. Tenancy Agreement, or

		iii. Any other relevant document issued by an authorized government agency or institution.
	Students (18+)	1. Ghana Card KYC Data Set 2. Additional minimum requirements; **a.** Introductory letter (school / parent/ Guardian) **b.** Student ID Card **c.** Proof of Residence: i. GPS Address ii. Tenancy / Hostel Agreement iii. Any other relevant document issued by an authorized government agency or institution.
	Minors (Below 18)	1. Ghana Card KYC Data Set of Parent/Guardian 2. Additional Requirements (Minor's Details); a. Full Name b. Date of Birth c. Birth Certificate Parent/Guardian d. Proof of Address Residential: i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized government agency or institution.

	Refugees and Asylum Seekers	1. Non- Citizen Card KYC Data Set 2. Additional minimum requirement; a. References / letter from Ministry of Interior or an appropriate government / international agency b. Proof Residential Address (local): i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized government agency or institution. iv. Details of last Residential address or country of origin (foreign)
	Foreign Diplomats	1. Diplomatic Card / Diplomatic Passport 2. Additional minimum requirements; a. Reference/Letter from i. Ministry of Foreign Affairs and Regional Integration and or ii. Embassy / Consulate Office b. Proof of Residential Address (local) i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized government agency or institution. c. Proof of Residential address (foreign): i. Utility Bill, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized government agency or

		institution.
	Dependents of Foreign Diplomats	1. Diplomatic Card / Diplomatic Passport of the Diplomat 2. Additional Requirements (Dependents Details); i. Full Name ii. Date of Birth iii. Passport Details iv. Proof of Address Residential (local) of the Diplomat: i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized government agency or institution. 3. Proof of Residential address (foreign) of applicant: i. Utility Bill, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized government agency or institution.

Sole Proprietorship / UBO	Sole Proprietorship / UBO	1. Ghana Card KYC Data Set 2. Additional Minimum Requirements; v. Full name of Business vi. Full Registered Business Address vii. Registration Number viii. Country of Registration ix. Date of Business Registration x. Nature of Business xi. Copy of license from a Regulatory Authority (Auxiliary Certificate) xii. Proof of Residential/Business Address: i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized government agency or institution.
Legal Entities	Ghanaian Owned Companies and their Directors / Shareholders / Ultimate Beneficiary Owner (UBO)	1. Ghana Card KYC Data Set for each Director/Shareholder/Ultimate Beneficiary Owner 2. Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner; a. Certificate of Incorporation b. Copy of license from a Regulatory Authority (Auxiliary Certificate) c. Proof of Residential Address for each Director/Shareholder/UBO: i. GPS Address, or ii. Tenancy Agreement, or

		iii. Any other relevant document issued by an authorized government agency or institution
	Foreign Owned Companies and their Foreign Directors and Shareholders/UBO	1. Non- Citizen Card KYC Data Set 2. Additional minimum requirement for each Director / Shareholder / Ultimate Beneficiary Owner; a. Certificate of Incorporation b. GIPC certification c. Relevant Industry license d. Copy of license from a Regulatory Authority (Auxiliary Certificate) e. Proof of Corporate/Residential Address (local) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner: i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document. f. Proof of Residential address (foreign) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner: i. Utility Bill, or ii. Tenancy Agreement, or iii. Any other relevant document

Public Registered Companies (Directors / Shareholders / UBO)	Local Directors / Shareholders with Controlling interest	1. Ghana Card KYC Data Set for each Director/Shareholder/Ultimate Beneficiary Owner 2. Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner; a. Certificate of Incorporation b. Proof of Residential Address for each Director/Shareholder/UBO i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document
	Foreign Directors/Shareholders with Controlling interest	1. Non- Citizen Card KYC Data Set 2. Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner; a. Certificate of Incorporation b. Proof of Corporate/Residential Address (local) for each Foreign Director / Shareholders / Ultimate Beneficiary Owner: i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document. c. Proof of Residential address (foreign) for each Foreign Director / Shareholder / Ultimate Beneficiary Owner: i. Utility Bill, or ii. Tenancy Agreement, or iii. Any other relevant document

	Local UBO	1. Ghana Card KYC Data Set for each Director/Shareholder/Ultimate Beneficiary Owner 2. Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner: a. Certificate of Incorporation b. Proof of Residential Address for each Director/Shareholder/UBO: i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document
	Foreign UBO	1. Non- Citizen Card KYC Data Set 2. Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner; a. Certificate of Incorporation b. Proof of Corporate/Residential Address (local) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner: i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document. c. Proof of Residential address (foreign) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner: i. Utility Bill, or ii. Tenancy Agreement, or iii. Any other relevant document

Government	State Owned Enterprises (SOEs)	Minimum Requirements; a. Ghana Card KYC Data Set for all Directors and Account Signatories b. Board Resolution c. Details of Address of Government
	Ministries, Departments and Agencies	
	Regulatory Bodies /Agencies	
	Public Institutions (E.g., Universities, Hospitals)	

	Foreign Government – Embassies/Consulate	Minimum Requirements; a. Diplomatic Card/Passport of account signatories b. Reference/Introductory Letter c. Details of Address
	Foreign Government – Development Organization	
	International Development Organizations – (E.g., UN, WHO, Africa Development Bank etc.)	

Financial Institutions	Regulated Institutions of; 1. Securities and Exchange Commission 2. Bank of Ghana 3. National Insurance Commission 4. National Pension Regulatory Authority 5. Office of the Registrar of Companies 6. Credit Unions Association and 7. Any other regulated financial institution	Minimum Requirements; a. Board Resolution b. Certificate of Incorporation c. Copy of license from a Regulatory Authority d. Copy of license from a Regulatory Authority (Auxiliary Certificate) e. Ghana Card/ Non-Citizen Card KYC Data Set for Directors/ Account Signatories f. Details of Business Address
Non-Profit Organizations (NPOs)/Clubs and Societies	Non-Profit Organizations (NGOs) Religious Organizations / Bodies	Minimum Requirements; a. Board Resolution b. Certificate of Incorporation c. Copy of license from a Regulatory Authority (Auxiliary Certificate) d. Ghana Card/Non- Citizen Card KYC Data Set for Directors/Account Signatories e. Details of Business Address f. Nature of Business

	Charities /Foundations/ Mutual/Friendly Societies, Cooperatives and Provident Societies	
	Clubs	Minimum Requirements; a. Board Resolution b. Constitution c. Ghana Card KYC Data Set for Account Signatories d. Copy of license from a Regulatory Authority (Auxiliary Certificate) e. Details of Business Address f. Nature of Business
	Societies/ Associations	
Trust	Trust	Minimum requirements; a. Certified copy of Trust Deed and supplemental Trustee, or Equivalent constitutive document detailing purpose and structure of the Trust. b. Details of settlors, trustee and beneficiaries and authorized signatories in the Trust. c. Where signatories are not identified in the

		Trust Deed, a certified copy of the authorized signatories list shall be provided. d. Ghana Card KYC Data Set for; i. Settlors (Donor / Grantors) ii. Trustees iii. Beneficiaries iv. Authorized Signatories
Professional Intermediaries	Lawyers, Notaries, Accountants, Auditors, other Legal Professions and the like.	1. Ghana Card KYC Data Set 2. Additional minimum requirements a. Proof of Residential address (foreign): i. Utility Bill, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized government agency or institution. b. Professional Certificate and evidence in good standing 3. <u>Supplementary requirement</u> a. Proof of Residential Address (local): i. GPS Address, or ii. Tenancy Agreement, or iii. Professional Certificate and evidence in good standing iv. Any other relevant document

APPENDIX B:

DEFINITION OF TERMS

For the proper understanding of this 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, and

	e. Other entities as stated under Section 7 of the Companies Act, 2019 (Act 992)
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 categories of offences/ Predicate Offences	Designated categories of offences mean: 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 and prostitution; 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 and grievous bodily injury; 14. kidnapping, illegal restraint and hostage-taking for ransom; 15. Robbery or theft; 16. Smuggling; 17. Tax crime (related to direct and indirect taxes) and excise evasion 18. Extortion (for instance Blackmail); 19. Forgery 20. Piracy (including maritime); 21. Insider trading and market manipulation 22. Cybercrime.
Designated non-financial businesses and professions	Designated non-financial businesses and professions means: 1. Casinos (which also includes internet casinos). 2. Real estate agents/ brokers. 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 this 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 biometrics, 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.
Omnibus Account	Pooled account is an investment account that allows multiple individuals to pool their resources and invest as a single entity.
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 xi. Traditional rulers
Private Companies	Private companies have the meaning as defined under Section 7 of Act 992
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.
Proliferation Financing	Proliferation financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery

	and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligation.
Public Companies	Private companies have the meaning as defined under Section 7 of Act 992.
Risk	All references to risk in these Guidelines refer 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.
Source of Funds	Source of funds is the origin of funds used for transactions or activities that occur within the business relationship or occasional transaction. In establishing the source of funds, one must understand not only where the funds are coming from but the activities that were involved in generating those funds.
Source of Wealth	Source of wealth describes the economic, business and or commercial activities that generated or significantly contributed to the customers' overall net worth/entire body of wealth. Examples of source of wealth include salaries, inheritances, investments, business ownership, property or gifts.

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.
Targeted Financial Sanctions	The term targeted financial sanctions means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
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 organizations to do or to abstain from doing any act.
Terrorist financing	Terrorist financing (TF) includes the financing of terrorist acts, and of terrorists and terrorist organizations.
Terrorist financing offence	A terrorist financing (TF) 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.
Unlisted 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 transferred, 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/CPF compliance. An MO shall 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 by the FATF and any other relevant bodies.

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 and different signatures.

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 cash, cheques or electronic transfers, 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.

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 offshore 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. 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.

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

e. 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.

f. 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.

g. Where transactions are performed by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries /jurisdictions.

h. 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.

i. Use of false or misleading identification to open an investment account or conduct a transaction.

j. Beneficial owner of an investment account or transaction not properly identified.

k. Use of family, trust or nominee accounts

l. Inclusion of an individual involved in the transaction on the United Nations 1267 Sanctions list.

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 a 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. Transactions involving a person or entity in a foreign country where there are diversion concerns.

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 counterparty 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 which do not have a high level of capitalization or display other shell company indicators).
j. Transaction involves financial institutions with known deficiencies in AML/CFT/ CPF 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 that 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 additional transaction fees.
d. Virtual assets moved from a public, transparent blockchain to a centralized 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 involving 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

a. Employee exhibits a lavish lifestyle that cannot be justified.
b. Employee is reluctant to apply for leave.
c. Customer uses a personal investment account for business purposes.
d. Official Embassy business is conducted through personal accounts.
e. Embassy accounts are funded through substantial currency transactions.
f. 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 unassociated 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 circumstance (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. Businesses 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/CPF 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 having strategic deficiencies in their AML/CFT/CPF regimes.

b. Countries subject to sanctions, embargoes 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/CPF Compliance Program Based on Its Risk Assessment

The management of an MO shall structure their AML/CFT/CPF 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 to 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/CPF compliance program that specifically monitors and controls the higher risks that management and the board have accepted.

Consolidated AML/CFT/CPF Compliance Risk Assessment

An MO that implements a consolidated or partially consolidated AML/CF/CPF 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/F/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/CPF 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. Anti-Money Laundering Act, 2020 (Act 1044)
2. Companies Act, 2019 (Act 992)
3. Criminal Offences (Amendment) Act, 2012 (Act 849)
4. Securities Industry Act, 2016 (Act 929), as amended
5. Anti-Money Laundering Regulations, 2011 (L.I. 1987)
6. Anti-Terrorism Act, 2008 (Act 762)
7. Anti-Terrorism (Amendment) Act, 2014 (Act 875)
8. Anti-Terrorism Regulations, 2012 (L.I. 2181)
9. Revised SEC/FIC AML/CFT/CPF Guidelines for Market Operators, 2021

OTHER RELEVANT LEGISLATION INCLUDE:

1. EOCO Regulation 2012, (L.I. 2183)
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/ Centres
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/CPF issues.

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

These Guidelines shall be read in conjunction with all AML/CFT/CPF 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/CPF Guidelines have necessitated a review. These events include:

1. The enactment of the AML Act 2020, (Act 1044)
2. Revisions to the FATF's Recommendations
3. Lessons learnt from the implementation of the SEC/FIC AML/CFT/CPF Guidelines for MOs for 2021.
4. Lessons learnt from the implementation of the SEC/FIC AML/CFT/CPF Administrative Sanctions/Penalties for MOs for 2021.
5. Lessons learnt from Ghana's National Risk Assessment Reports
6. Lessons learnt from Ghana's Mutual Evaluation Reports
7. Lessons from on-site and off-site inspections of MOs.

APPENDIX H:

CHECKLIST FOR MO'S AML/CFT/CPF COMPLIANCE PROGRAMME

The AML Compliance programme shall provide for procedures including the following:

- **a.** Policy statement on AML/CTF/CPF 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

APPENDIX J

AML/CFT/CPF STATUTORY RETURNS

TYPE OF REPORT	RECEPIENT BODY	CHANNEL	FREQUENCY
Compliance Report: This shall include but not limited to the following key areas: 1. Staff AML/CFT/CPF Trainings 2. Additional AML/CFT/CPF Risk Assessment 3. Additional Procedures and Mitigants 4. New Technologies'/Products, Non-face-to-face Transactions 5. Reliance on Intermediaries or Third-Party Service Providers 6. Update appointment / re-designation / dismissal / resignation / retirement 7. Monitoring of Employee Conduct 8. Fraud activities 9. Review of Risk Assessment Conducted	SEC and FIC	Emails- daniel.effah@sec.gov.gh; emmanuel.sakyi-appiah@sec.gov.gh; precious.oteng@sec.gov.gh; info@fic.gov.gh/ GoAML Platform	**HALF YEARLY** (not later than the 31st day of the month after the half year); and **END OF YEAR** (not later than the

10. Review of AML/CFT/CPF policy/framework 11. Record Keeping Procedures 12. Update on AML/CFT/CPF Software/Application 13. Statistics of STRs, CTRs and ECTRs submitted to the FIC during the review period 14. Other relevant compliance activities			31st day of the month after the end of year)
Employee (Board, Management and Staff) Education and Training Programme	SEC and FIC	Emails- daniel.effah@sec.gov.gh; emmanuel.sakyi-appiah@sec.gov.gh; precious.oteng@sec.gov.gh; info@fic.gov.gh/ GoAML Platform	**YEARLY** (not later than the 31st of December of every financial year)
Independent Audit Report on the AML/CFT/CPF function The report may include but not limited to the following areas: 1. Review of AML/CFT/CPF programme for the year 2. Board/staff training 3. Review of AML/CFT/CPF policy and Risk Assessment Framework 4. Filing of CTRs/STRs/ECTRs 5. Transaction Monitoring 6. KYC/CDD/EDD on customers 7. Review of AMLROs account 8. Due diligence on new staff 9. Any other AML/CFT/CPF related activity	SEC and FIC	Emails- daniel.effah@sec.gov.gh; emmanuel.sakyi-appiah@sec.gov.gh; precious.oteng@sec.gov.gh; info@fic.gov.gh/ GoAML Platform	**EVERY TWO (2) YEARS** (not later than the 31st day of the month after the end of the two (2) year period)
Semi-annual Returns (Data Capture)	SEC	Emails- daniel.effah@sec.gov.gh; emmanuel.sakyi-appiah@sec.gov.gh; precious.oteng@sec.gov.gh	**HALF YEARLY** (not later than the 31st day of the month after the end of the half year)
Semi-annual Returns (Risk Management Questionnaire)	SEC	Emails- daniel.effah@sec.gov.gh; emmanuel.sakyi-appiah@sec.gov.gh; precious.oteng@sec.gov.gh	**HALF YEARLY** (not later than the 31st day of the month after the end of the half year)
Updated PEP List	SEC	Emails- daniel.effah@sec.gov.gh;	**HALF YEARLY** (not later than the

		emmanuel.sakyi-appiah@sec.gov.gh; precious.oteng@sec.gov.gh	31st day of the month after the end of the half year)
Fraud and Defalcation Report	SEC and FIC	Emails- daniel.effah@sec.gov.gh; emmanuel.sakyi-appiah@sec.gov.gh; precious.oteng@sec.gov.gh; info@fic.gov.gh/ GoAML Platform	**As and when**
Disengaged Staff (Directors, AMLROs and Licensed Representatives) Return	SEC	Emails- daniel.effah@sec.gov.gh; emmanuel.sakyi-appiah@sec.gov.gh; precious.oteng@sec.gov.gh	**As and when**
Engaged Staff (Directors, AMLROs and Licensed Representatives)	SEC	Emails- daniel.effah@sec.gov.gh; emmanuel.sakyi-appiah@sec.gov.gh; precious.oteng@sec.gov.gh	**As and when**