SECURITIES AND EXCHANGE COMMISSION (SEC)

AND

FINANCIAL INTELLIGENCE CENTRE (FIC)

REVISED COMPLIANCE MANUAL

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

FOR

CAPITAL MARKET OPERATORS

OCTOBER, 2017

Contents

Comment [PMY1]: Please regenerate entire content for the document.

PREAMBLE

Section 138 of the Securities Industry Act, 2016, (Act 929) (SIA ~~or Act 929~~) empowers SEC to ensure that all its regulated entities operate in a manner so as to comply with the provisions of Anti-Money Laundering, Countering the Financing of Terrorism and Combating the Financing of the Proliferation of Weapons of mass destruction (AML/CFT&CPF) (AML) legislation and FATF's Recommendations revised in 2012, and their amendments. FATF's Recommendation shall be read in conjunction with its interpretative notes.

The SIA and AML Legislation mandate the Securities and Exchange Commission (SEC) as a supervisory body or competent authority to give guidance to its regulated entities or accountable institutions on AML.

Given the prominence that financial crimes especially money laundering (ML), terrorist financing (TF~~T~~), the financing of the p~~P~~roliferation of weapons (PF) of mass destruction and

transnational organized crimes have assumed in ~~i~~International financial markets, and the risks they pose to the financial markets globally and to Ghana in particular, the need for a comprehensive effort to fight this menace has been realized. It is against this background that ~~the Securities and Exchange Commission (~~SEC~~)~~ and the Financial Intelligence Centre (FIC) in accordance with Section 6(d) of the Anti-Money Laundering Act, 2008 (Act 749) as amended ~~(by~~ Act 874), and Regulation 38 of L.I.1987, have developed this manual to guide Capital Market Operators (CMOs) to enhance their 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.

The AML legislation includes:

1. Securities Industry Act, 2016, (Act 929)
2. Anti-Money Laundering Act, 2008 (Act 749)
3. Anti-Money Laundering (Amendment) Act, 2014 (Act 874)
4. Anti-Money Laundering Regulations, 2011 (L.I. 1987)
5. Anti-Terrorism Act, 2008 (Act 762)
6. Anti-Terrorism (Amendment) Act, 2012 (Act 842)
7. Anti-Terrorism Regulations, 2012 (L.I. 2181)
8. Criminal Offences (Amendment) Act, 2012 (Act 848)
9. Compliance Manual for Capital Market Operators, 2017

This manual is also designed to manage the risks faced by CMOs on the laundering of the proceeds of crime and will also provide protection against fraud, reputational and other risks faced by

CMOs. Consequently, all CMOs are required to adopt a risk–based approach in the identification and management of their AML risks in line with the requirements of this manual.

This manual is also in accordance with the Financial Action Task Force (FATF) Recommendations, International Organization of Securities Commissions' (IOSCO) principles and international best practice in managing AML.

CMOs should note that AML Legislation have prescribed sanctions for non-compliance. It is, therefore, in the best interest of CMOs to ensure compliance at all times with the prescriptions contained herein.

This manual must be read in conjunction all AML Legislation.

As part of our commitment to continual improvement, readers of this manual are encouraged to identify improvement opportunities and bring them to the attention of the SEC for evaluation and subsequent incorporation into this manual.

LIST OF ACRONYMS & ABBREVIATIONS

AML - Anti-Money Laundering, Countering the Financing of Terrorism and Combating the Financing of the Proliferation of Weapons of mass destruction (AML/CFT&CPF)

AMLRO - Anti-Money Laundering Reporting Officer

ATM - Automatic Teller Machine

BOG - Bank of Ghana

CDD - Customer Due Diligence

CFT - Combating of the Financing of Terrorism

CMO - Capital Market Operator

CTR - Currency Transaction Report

DA - Domiciliary Account

DNFBPs - Designated Non-Financial Businesses and Professions

FATF - Financial Action Task Force

FIC - Financial Intelligence Centre

KYC - Know Your Customer

LEA - Law Enforcement Agency

MDAs - Ministries, Departments and Agencies

ML - Money Laundering

MVT - Money or Value Transfer

NGO - Non-governmental Organization

NIC - National Insurance Commission

PEP - Politically Exposed Person

PF - Proliferation Financing

RO - Religious Organization

SEC - Securities & Exchange Commission

STR - Suspicious Transaction Report

TF - Terrorist Financing

DEFINITION OF TERMS

For the proper understanding of this Manual, certain terms used are defined as follows:

Applicant for Business: "applicant for business" means ~~T~~the person or company seeking to establish a 'business relationship' or an occasional client undertaking a 'one-off' transaction whose identity must be verified.

Beneficial owner: "b~~B~~eneficial owner" refers to those natural person(s) who ultimately owns or controls a client 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: "b~~B~~eneficiary" includes those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance.

Business Relationship: 'b~~B~~usiness relationship' is any arrangement between the ***CMOs*** and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a 'frequent' habitual or regular basis.

CMOs: "CMOs" means any person (individual or corporate) duly recognised by the Commission to perform specific functions in the Capital Market.

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.

Correspondent Institution: "correspondent institution" means any formal relationship(s) established for a foreign financial institution to provide regular services to effect transactions in securities.

Comment [PMY2]: I don't understand the definition

Cross-border transaction: "c~~C~~ross-border transaction" means any transaction where the originator and beneficiary Operators are located in different jurisdictions. This term also refers to any chain of transaction that has at least one cross-border element.

Designated offences: **Section 1(2)** of the AML Act defines an unlawful activity as conduct which constitutes a serious offence, financing of a terrorist act, or contravention of a law which occurs after the commencement of this Act, whether the conduct occurs in this country or elsewhere.

Comment [PMY3]: Have not given a definitio to "designated offences".

These offences include but are not limited to the following:

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

Designated non-financial businesses and professions (DNFBP)
DNFBP means:

- Casinos (which also includes internet casinos).
- Real estate agents.
- Dealers in precious metals.
- Dealers in precious stones.
- Legal practitioners, notary public 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 money laundering.
- Trust and Company Service providers

Domestic transfer: "d~~D~~omestic transfer" means any wire transfer where the originator and beneficiary institutions are both located in Ghana.

This term therefore refers to any chain of wire transfers that takes place entirely within Ghana's borders, even though the system used to effect the wire transfer may be located in another jurisdiction.

False disclosure: "f~~F~~alse 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.

The FATF Recommendations: ~~The~~ "FATF Recommendations" refers to the FATF Forty Recommendations.

Funds Transfer: ~~The term~~ "funds transfer" refers to any transaction carried out on behalf of an originator (both natural and legal) through a ***CMO*** by electronic

means with a view to making an amount of money available to a beneficiary through another ***CMO***. The originator and the beneficiary may be the same person.

Legal persons: "Legal persons" refer to body corporate, foundations, partnerships, associations, or any similar bodies that can establish a permanent client relationship with a CMO or otherwise own property.

Non-profit/Non-Governmental Organizations: ~~The term~~ "non-profit organization/ non-Governmental organization" refers to a legal entity or organisation 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.

Originator: "~~The~~ originator" means ~~is~~ the accountholder, or where there is no account, the person (natural or legal) that places the order with the ***CMO*** to perform the ***Capital Market Transaction.***

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 a part of a business relationship as this can affect the identification requirements.

Payable through account: "p~~P~~ayable through account" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

Physical presence: "physical presence" m~~M~~eans meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.

Foreign Politically Exposed Persons" (PEPs): "foreign politically exposed persons" ~~Foreign *PEPs*~~ are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Domestic Politically Exposed Persons: "domestic politically exposed persons" (domestic PEPs)

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

Persons' who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Comment [PMY4]: Is it "politically exposed person" or "foreign PEPs" remember to move to columns if the correction is accepted.

Proliferation Financing(PF): " proliferation financing" ~~I~~is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, 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***.

Relevant authority: "relevant authority" ~~M~~means any persons or organization which has mandate over your activity as a person.

Risk: All references to "risk" in this Manual refer to the risk of money laundering and/or terrorist financing and/or proliferation financing.

Settlor: "sSettlors" means ~~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 may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets.

Shell bank: "sShell bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.

Suspicious Transaction: For the purpose of this Manual, 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 such a transaction that is inconsistent with a client's known, legitimate business or personal activities or normal business for that type of account or that lacks an obvious economic rationale.

Terrorist: "~~I~~terrorist" refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; 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: "t~~T~~errorist acts" include 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: Convention for the

Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997); and

(ii) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.

Terrorist financing: "t~~T~~errorist financing", (TF), includes the financing of terrorist acts, and of terrorists and terrorist organisations.

Terrorist financing offence: A terrorist financing (TF) offence refers not only to the primary offence or offences, but also to ancillary offences.

Comment [PMY5]: ???????? Let's check the definition again to be sure.

Terrorist organization: "terrorist organization" Refers to any group of terrorists that:

(i) Commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully;

(ii) Participates as an accomplice in terrorist acts;

(iii) Organises or directs others to commit terrorist acts; 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: "t~~T~~hose 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: "t~~T~~rustees"~~,~~ 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.

PART A

AML/CFT/PF INSTITUTIONAL POLICY FRAMEWORK

This part offers general guidelines on AML institutional framework

1. Development of a Risk Assessment Framework and Report in conformance with FATF's Recommendation 1 and its interpretative notes.

Each ***CMO*** shall develop a board-approved risk assessment framework and risk assessment report. The framework should include the risk assessment methodology applied in developing

the risk assessment report. The risk assessment process shall cover an evaluation of the risks posed by clients, products, channels of distribution of products and geographical risk. The results of the risk assessment shall be used to prepare the CMO's Compliance program. See section 40 of Act 749 as amended by section 19 Act 874 and expanded in Reg. I of LI 1987.

The Risk-based approach to managing risks should be the underlying principle.

The levels of risk categorizations shall be:

i. Prohibited business
i. High risk business
ii. Medium risk business
iii. Low risk business

2i. Development of AML Compliance Program

Refer to section 40 of Act 749 as amended by section 19 Act 874 and expanded in Reg. I of LI 1987

Every CMO shall develop, document and implement AML/CFT/PF Compliance programmes, policies, and internal control systems that will deter criminals from using its facilities for ML and ensure that its obligations under the ML Legislation are always met. The document should also state the CMOs commitment to comply with AML legislation and to actively prevent any transaction(s) that will facilitate criminal activity.

2ii. Checklist for Reviewing CMO's AML/CFT Compliance Program

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

1. Policy statement on money laundering and terrorist financing compliance
2. Designation of the AMLRO and responsibilities
3. Staff training requirements
4. PEP and other high risk procedures
5. Obligation to report STRs
6. Obligation to submit CTRs
7. Prohibition against Tipping off or disclosing to unauthorized external persons that an STR is being filed
8. Record keeping requirements
9. Internal AML/CFT Risk Assessment Procedures
10. Risk management procedures
11. Requirements for assessing risks of new products, services and technologies
12. Procedures related to identifying potential terrorist financing
13. Customer Acceptance Policy (CAP)
14. Monitoring of clients transactions
15. Adequate screening procedures on hiring employees
16. Independent Audit Testing
17. Customer Identification Programme
    - **a.** Type of information the CMO must obtain from prospective customers
    - **b.** Methodologies employed to verify such information
    - **c.** How to deal with customers who refuse to provide information
    - **d.** How to handle situation where customer identity cannot be verified
    - **e.** When to rely on another institutions identity verification process is appropriate
    - **f.** PEP identification
    - **g.** Review of clients against an appropriate sanction list
    - **h.** Customer notification of the CMOs identification and verification procedures:

1. Customer Due Diligence(CDD) : This involves collecting of sufficient additional information to understand the customer
2. Enhanced Due Diligence(EDD)
3. 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
4. Display of public notices issued by SEC and FIC

Comment [PMY6]: Check the numbering. A b
confusing.

The development of the AML Compliance Program in itself is not adequate to satisfy the regulatory requirements. Rather implementing and adhering to it, as well as communicating it to the staff of the CMO to set the tone for an AML compliance culture is required.

2iii. Testing for the adequacy of the Compliance Program

Every CMO shall make a policy commitment to subject its AML Compliance Program to independent-testing to determine its adequacy, completeness and effectiveness. A report of the test is required to be submitted to ***SEC*** and **FIC** by 31st December every financial year. Any identified weaknesses or inadequacies shall be promptly addressed by the ***CMO***.

~~the~~The independent test must not be conducted by the AMLRO.

2iv. Formal board approval of the AML Compliance Program

The ultimate responsibility for AML/CFT/PF compliance is placed on the Board of Directors of every ***CMO*** in Ghana. It is, therefore, required that the Board ensures that a comprehensive operational AML/CFT/PF Compliance Manual is formulated by Management and presented to the Board for consideration and formal approval. The Manual shall be forwarded to ***SEC*** and FIC within six months of its release. Quarterly reports on the AML/CFT/PF-compliance status of the ***CMO*** are to be presented to the Board for its information and necessary action.

3i. Designation and Duties of AML/CFT/PF Compliance Officer (AMLRO) Section 20 (1) (b) of Act 874 and (Reg. 5 of LI 1987)

Each ***CMO shall*** formerly appoint its AMLRO at the managerial level. The AMLRO so appointed shall possess the relevant competence, qualification, experience, authority and independence to implement the institution's AML/CFT/PF compliance programme.

Each designated AMLRO should have at least two (2) years' experience at management level in the financial industry and must report to either the CEO or the Board of Directors of his or her Company in that capacity.

3ii. Qualification of the AMLRO

The AMLRO shall have:

a. A working knowledge of ML Legislation,

b. A first degree in Accounting, Economics, Finance, Law or any other relevant field

c. At least two years' experience at a managerial position in the financial industry or must show evidence of performing a relevant function in another field.

d. Evidence of AML training.

e. Additional training in risk, compliance, audit, forensics or investigations (will be an added advantage).

The SEC may require AMLROs to pass an approved exam before accepting his or her designation as an AMLRO.

3iii. The duties of the Anti-Money Laundering Reporting Officer (AMLRO), among others shall include:

a. Oversight of CMOs compliance with AML Legislation

b. Guidance on best practise reports issued by SEC, FIC, FATF, IOSCO and other standard setting bodies

c. Update the board, senior management, audit, legal and staff on any adequacy of CMOs AML compliance, risks etc.

d. Implement findings of AML reviews such as the independent testing of the Compliance Program

e. Conducting Money Laundering and Terrorist Risk Assessment of his/her firm's products, services, customers, delivery channels and geographical areas

f. Developing, implementing and updating AML/CFT/PF Compliance Programme;

g. Receiving and vetting suspicious transaction reports from staff;

h. Regular monitoring of clients' transactions and filing suspicious transaction and currency transactions reports with the FIC;

i. Rendering "nil" reports with the FIC, where necessary to ensure compliance;

j. Coordinating the training of staff in AML awareness, detection of suspicious transaction red flags and reporting requirements;

k. Serving both as liaison officer between his or her institution, the ***SEC*** and FIC and a point-of contact for all employees on issues relating to money laundering, terrorist financing and proliferation financing.

l. Recording keeping including training records

m. Implementation of auditor's recommendation

n. Not conducting transactions to avoid reporting to SEC/FIC

5. Cooperation with Competent Authorities

Each ***CMO*** is required to state its commitment that it will comply promptly with all requests made pursuant to AML legislation and shall provide information to the **SEC**, FIC and other relevant government agencies on AML matters upon request per Section 30 of Act 749 amended by section 9 of Act 874.

Where there is a request for Information on Money Ll~~l~~aundering and Terrorist Financing, each CMO shall do the following (Reg. 42 of LI 1987):

a) 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 organisation named in the request;
b) Report promptly to the requesting authority the outcome of the search; and
c) Protect the security and confidentiality of such requests.

6. Secrecy and Confidentiality

Sections 24 to 32 of the SIA, requires CMOs to provide information or produce books on request. Secrecy and confidentiality laws shall not in any way, inhibit the implementation of the requirements in these guidelines, giving the relevant authorities the power to access information to properly perform their functions in combating money laundering, financing of terrorism and proliferation financing. This includes the sharing of information between relevant authorities, either domestically or internationally; and the sharing of information between CMOs, where this is required or necessary. CMOs shall also disclose information in conformance to FATF Recommendations 21, 24 and 25.

Comment [PMY7]: Let's be consistent with capitalisation and lower case.

7. Scope of Offensive Proceeds

In conformity with section 1 of Act 874 and FATF Recommendation 3, ***CMOs shall*** identify and report to the FIC,

the proceeds of crime derived from but not limited to the following:

1. **Participation in an organized crime group and racketeering;**
2. **Terrorism, including terrorist financing;**
    a. **Trafficking in human beings and migrant smuggling;**
    b. **Sexual exploitation, including sexual exploitation of children;**
    c. **Illicit trafficking in narcotic drugs and psychotropic substances;**
    d. **Illicit arms trafficking;**
    e. **Illicit trafficking in stolen and other goods;**
    f. **Corruption and Bribery;**
    g. **Fraud;**
    h. **Counterfeiting currency**
    i. **Counterfeiting and piracy of products;**
    j. **Environmental crime;**
    k. **Murder, grievous bodily injury;**
    l. **Kidnapping, illegal restraint and hostage taking;**
    m. **Robbery or theft;**
    n. **Smuggling (including in relation to customs and excise duties and taxes);**
    o. **Extortion;**
    p. **Forgery;**
    q. **Piracy; and**

r. **Insider trading and market manipulation.**

s. **Tax crimes (related to direct taxes and indirect taxes);**

t. **Any other predicate offence pursuant to the AML/CFT legislation**

Note that:

a. ML is a derivative offence which means that an initial crime (predicate offence) would have been committed and proceeds obtained therefrom.

b. Third party ML is the laundering of proceeds of crime by a person who was not involved in the commission of the predicate offense.

c. Self-laundering is the laundering of proceeds of crime by a person who was involved in the commission of the predicate offence.

PART B

1. Customer Due Diligence *(CDD)*

This section should be read in conjunction with section 23 of Act 749 as amended by section 6 of Act 874 and FATF's Recommendation 10.

CMOs shall identify and verify the identities of clients and beneficiary owners of their accounts. No anonymous accounts or accounts in fictitious names shall be opened or operated by the CMO.

i. CMOs shall undertake clients' due diligence (CDD) measures where:

a. A business relationship is established. ***CMOs*** shall not establish a business relationship until all relevant parties to the relationship have been identified and verified, and the nature of the business they intend to conduct ascertained. Once an on-going business relationship is established, any inconsistent activity can then be examined to determine whether or not there is an element of money laundering for suspicion.

b. Carrying out occasional (and/or one-off) transactions above the threshold of $10,000 or its equivalent (or as may be determined by ***SEC/FIC*** from time to time whichever is lower), including where the transaction is carried out in a single operation or several operations that appear to be linked within operators (even when different accounts are used), between operators or over a period of time.

The procedures above shall not apply to payments in respect of CMO-to-CMO 9 (or other financial institutions') transfers and settlements where both the originator and the beneficiary are CMOs or other financial institutions acting on their own behalf.

c. There is a suspicion of ML, regardless of any exemptions or any other thresholds referred to in this Manual; or
d. There are doubts about the veracity or adequacy of previously obtained clients' identification data.

ii. A CMO shall not be required (after obtaining all the necessary documents and verifying them), to repeatedly perform an identification and verification exercise every time a client conducts a transaction unless there is a basis to do so.

iii. Linked transactions

Where a number of single applications or instalment payments under different identities appear to be linked, identification evidence must be obtained in respect of parties involved in each single transaction. This should be investigated and an STR submitted to the FIC if the results sustain the suspicion.

iv. On the commencement of a business relationship, the following information on the nature of the business the client intends to undertake shall be documented among others:

a. Purpose for establishing the business relationship

b. Nature of activity to be undertaken

c. Expected origin of funds to be used during the relationship

d. Details of occupation or business activities and sources of income

2. Customer due diligence (CDD) processes

2.1. CMOs shall:

a. Carry out the full range of the CDD measure on all clients.

b. Identify all their clients and verify their identities using reliable, independently sourced documents, data or information.

c. CMOs shall identify beneficiary-owner(s) and take reasonable measures to verify their identity using relevant information or data obtained from a reliable source to be certain that they know who the beneficiary-owner is.

d. CMOs shall in respect of all clients determine whether or not a client is acting on his or her own behalf or on behalf of another person. Where the client is acting on behalf of another person, the ***CMO*** is required to take

reasonable steps to obtain sufficient identification-data and to verify the identity of that other person.

e. ***CMOs*** shall obtain information on the purpose and intended nature of the business relationship of their potential clients.

f. ***CMOs*** shall conduct ongoing due diligence on the business relationship as stated by the clients.

g. The ongoing due diligence shall include scrutinizing the transactions undertaken by the client throughout the course of the CMO/client relationship to ensure that the transactions being conducted are consistent with the CMO's knowledge of the client, its business, risk profiles, and the source of funds.

h. CMOs shall ensure that documents, data and 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 higher-risk business-relationships or client categories.

i. For clients that may require additional caution to be exercised when transacting with them, activities in the client's accounts shall be monitored on a regular basis for suspicious transactions.

j. While extra care shall be exercised in such cases, the CMO shall de-risk *(*refuse to do business with) such clients or automatically classify them as high risk and subject them to an enhanced due diligence process. In this regard, CMOs shall weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML,TF or PF.

k. A CMO shall consider reclassifying a client as higher risk if following initial acceptance of the client, the pattern of account activity of the client does not fit in with the

CMO's knowledge of the clients. A Suspicious Transaction Report (STR) shall also be considered.

1. A CMO shall not commence a business relation or perform any transaction, or in the case of existing business relation, terminate such business relation if the client fails to comply with the due diligence requirements. A CMO shall also consider lodging a suspicious transaction report with the FIC under those circumstances.

2.2. CDD measures for individuals

The type of individual/natural clients' information to be obtained and identification data to be used to verify the information shall include the following for individuals:

1. Date of birth: birth certificate, passport, national identity cards and social security records
2. Permanent address: utility bills, tax assessment, bank statement, and a letter from a public authority.
3. Contact information: Telephone numbers, email and postal addresses.

Natural persons– include those persons who exercise ultimate ownership, management and/or control over the legal person. Examples of types of measures needed to satisfactorily perform this function include:

a. **For companies** -The natural persons are those who own the controlling interests and comprise the mind and management of the company;

b. For **trusts** – The natural persons are the settlor, the trustee and person exercising effective control over the trust and the beneficiaries.

c. Where the client or the owner of the controlling interest is a **public company** subject to regulatory disclosure requirements (i.e. a public company listed on a recognized securities market) it is not necessary to identify and verify the identity of the shareholders of such a public company.

2.3. CDD measures for legal persons:

a. CMOs shall take reasonable measures in respect of clients that are legal persons/arrangements to:

b. Understand the ownership and control structure of such a client; and

c. Determine the natural persons that ultimately own, control and/or manage the client.

d. Types of information required shall include:

1. Name of institution
2. Principal place of business operations
3. Mailing address
4. Telephone and fax numbers
5. Website address
6. Identification numbers e.g. Tax Identification number, license number etc.
7. Regulations
8. Resolution of the board to open an account
9. Identification and verification of the identity of persons authorized to operate the account
10. Nature and purpose of business
11. Review of latest audited annual report
12. Enquiry by a business information service or an undertaking by a reputable firm of lawyers and accountants acceptable to the Commission
13. Undertaking a company search to determine its state as to whether the institution has not been or is not in the process of being dissolved, struck off wound up or terminated

14. Utilizing an independent verification process, such as assessing public and private data bases
15. Obtaining prior bank references
16. Visiting the corporate entity
17. Contacting the corporate entity by telephone mail or email.

Comment [PMY8]: Format the numbering

2.4. Further CDD measures for legal persons:

Furthermore, in respect of clients that are legal persons or legal arrangements, CMOs Shall:

i. Verify any person purporting to have been authorized to act on behalf of such a client by obtaining evidence of his/her identity and verifying the identity of such a person; and

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

2.5. CDD measures for lower risk clients, transactions or products

i. Where clients are determined as low risk, CMOs shall apply reduced or simplified CDD measures when identifying and verifying the identity of their clients and the beneficial-owners.

ii. There are low risks in circumstances where;

a. The risk of ML, TF or PF is lower.

b. Information on the identity of the clients and the beneficial owner of a client is publicly available.

c. Adequate checks and controls exist elsewhere in public institutions.

iii. The following may be considered to be low risk clients:

a. *Financial Institutions, including CMOs***,** provided they are subject to requirements for the combat of ML, TF and PF which are consistent with the provisions of this Manual and are supervised for compliance with them;
b. Public companies listed on a securities market or similar situations that are subject to regulatory disclosure requirements;
c. Government ministries, departments, agencies and parastatals or state enterprises;
d. Life insurance policies where the annual premium and single monthly premium are within the threshold determined by NIC;
e. Insurance policies for pension schemes if there is no surrender-value clause and the policy cannot be used as collateral;
f. 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
g. Beneficial-owners of pooled-accounts held by Designated Non-Financial Businesses and Professions (DNFBPs) provided that they are subject to requirements to combat ML, TF and PF.

iv. ***CMOs*** that apply simplified or reduced CDD measures to clients' resident abroad are required to limit such to clients in countries that have effectively implemented the FATF Recommendations.

v. Simplified CDD procedures are not acceptable, and therefore cannot apply to a customer whenever there is

suspicion of ML or specific higher risk scenarios. In such a circumstance, EDD is mandatory.

vi. CMOs shall adopt CDD measures on a risk sensitive-basis as provided for in this manual. **CMO*s*** shall determine in each case whether the risks are lower or not, having regard to the type of clients, product, delivery channels or the location of the clients.

2.6. CDD measures for higher risk categories of clients

i. CMOs shall perform EDD for higher risk categories of customers, business relationships or transactions. The basic principle of a risk based approach is that CMOs adopt an enhanced CDD process for higher risk categories of clients, business relationships or transactions. Similarly, simplified CDD process is adopted for lower risk categories of clients, business relationships or transactions.

ii. For determining a client's risk profile, the following are examples of high risk clients that a reporting institution shall consider exercising greater caution when approving the opening of account or when conducting transactions:

a. Non-resident clients

b. On-line accounts

c. Off-shore clients

d. Public company insiders

e. Discretionary accounts

f. Legal entities that obscure ownership or beneficial interests

g. Hedge funds

h. Charities, NGOs, FBOs

i. Other CMOs and FIs

j. Private banking customers

k. Legal persons, arrangements such as Trusts that are personal asset holding vehicles

l. Companies that have nominee-shareholders or shareholders in bearer shares

m. Politically exposed persons

n. Cross-border transactions and business relationships

o. Clients from locations known for its high crime rate (e.g. drug production, trafficking, smuggling);

p. Clients from or in countries or jurisdictions which do not or insufficiently apply the FATF Recommendations (such as jurisdictions designated as Non Cooperative Countries and Territories (NCCT) by the FATF or those known to the reporting institution to have inadequate AML/CFT/PF laws and regulations);

q. Politically Exposed Persons (PEPs) and persons/ companies related to them;

r. Complex legal arrangements such as unregulated investment vehicles/special purpose vehicles (SPV); including correspondent banking and Shell Banks; or

s. Companies that have nominee-shareholders;

iii. Upon determining clients as "high-risk", the reporting CMO shall undertake enhanced CDD processes on the clients which shall include enquiries on:

a. the purpose for opening an account;
b. the level and nature of trading activities intended;

c. the ultimate beneficial owners;
d. the source of funds;
e. senior management's approval for opening the account;

iv. The ***CMO*** shall continue to undertake enhanced monitoring of the business relationship.

2.7. Attention to higher risk countries

i. ***CMOs shall*** give special attention to business relationships and transactions with persons (including legal persons and other CMOs) from or in countries which do not or insufficiently apply the FATF recommendations.

ii. ***CMOs 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 documented findings made available to assist competent authorities such as **SEC**, FIC, auditors and law enforcement agencies (LEAs) to carry out their duties.

iii. ***CMOs*** that conduct business with foreign institutions which, do not continue to apply or insufficiently apply the provisions of FATF Recommendations, are required to take measures such as the following:

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

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

c. In considering requests for approving the establishment in countries applying the countermeasure of subsidiaries or branches or representative offices of financial institutions,

taking into account the fact that the relevant ***CMO*** is from a country that does not have adequate AML/CFT/PF systems;
d. Warning non-financial sector businesses that transactions with natural or legal persons within that country might run the risk of ML. Limiting business relationships or financial transactions with the identified country or persons in that country to those that are verified.

2.8. CDD on higher risk businesses

The principal control of business relationships rests on those who are mandated to manage the funds, account or investment without requiring authorization and who will be in a position to override internal control mechanisms. Identification evidence should be obtained for the principal beneficiary owner(s) of the company and any other person with principal control over the company's assets. The veil must be lifted in this case.

Where a higher risk business applicant is seeking to enter into a business relationship where third party funding and transactions are permitted, the following evidence shall be obtained:

3. The company must be an established company incorporated for 18 months or more
4. A search report at the RGD
5. A formal enquiry via an information service or
6. Undertaking from a recognised firm of accountants or lawyers
7. Certified true copy of the resolution of the board of directors to open the account and confer authority on those who will operate
8. Regulations of the company

2.8.1. Guidance on Know Your Customer (KYC) Procedures

Information relating to the implementation of the Customer Identification Process (CIP), Customer Acceptance Process and the CDD process must be designed to permit the CMO to

objectively determine the client's investment goal, investment strategies, risk appetite, source of income and other information. Based on the information collected in the KYC, the CMO shall determine whether the activity on the client's account is consistent with the information provided. The following shall be noted:

i. ***CMOs shall*** be satisfied that a prospective client is who he/she claims to be.

ii. If the client is acting on behalf of another, the funds are supplied by someone else or the investment is to be held in the name of someone else, then the ***CMO shall*** verify the identity of both the clients and the agent/trustee unless the ***client*** is itself a Ghanaian regulated ***CMO***.

iii. ***CMOs shall*** obtain evidence in respect of their ***clients,*** unless it is otherwise stated in ***this manual.***

CMOs shall identify all relevant parties to the relationship from the onset by obtaining satisfactory identification evidence as provided in this manual.

2.8.2. Nature and Level of the Business

i. ***CMOs*** shall obtain sufficient information on the nature of the business that their ***client*** is taking or intends to undertake, including the expected and/or predictable pattern of transactions.

The information collected at the outset for this purpose shall include:

a. 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.

2.8.3. CMOs shall take reasonable steps to keep the information up to date as the situation arises, such as when an existing client opens a new account.

2.8.4. Apply Commercial Judgment

i. CMOs shall take a risk-based approach to the 'Know Your client' requirement and decide the number of times to verify the clients' records during the relationship, the identification evidence required and when additional checks are necessary.

ii. For personal account relationships, all joint-account holders need to be verified.

iii. In respect of private company or partnership, focus shall be on the principal owners/controllers and their identities shall also be verified.

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

2.9. CDD on existing clients

i. ***CMOs shall*** apply CDD requirements to existing clients on the basis of materiality and risk and continue to conduct due diligence on such existing relationships at appropriate times.

ii. The appropriate time to conduct CDD by CMOs shall include when:

a. A transaction of significant value takes place,

b. Clients documentation standards change substantially,

c. There is a material change in the way that the account is operated, for example due to frequency of operation and change in the type(s) of products

d. The institution becomes aware that it lacks sufficient information about an existing client.

iii. The ***CMOs shall*** properly identify the clients in accordance with these criteria. The clients' identification records shall be made available to the AML/CFT/PF compliance officer, other appropriate staff and relevant authorities.

2.10. CDD on Politically Exposed Persons (PEP)

i. CMOs shall perform CDD on PEPs. Act 874 defines Politically Exposed Persons (PEPs) to include a Head of State or Head of government etc.

An artificial politically exposed person and members of the family of the politically exposed person and close partners and associates of the politically exposed person are all classified as PEPs.

ii. ***CMOs shall*** in addition to performing CDD measures, put in place appropriate risk management systems to determine whether a potential client or existing clients or the beneficial-owner is a politically exposed person.

iii. ***CMOs shall*** obtain senior management approval before they establish business relationships with PEPs and to render quarterly returns on their transactions with PEPs to the FIC.

iv. Where a client has been accepted or has an ongoing relationship with the ***CMO*** and the client or beneficial-owner is subsequently found to be or becomes a PEP, the ***CMO*** is required to obtain senior management approval in order to continue the business relationship.

v. CMOs ***shall*** take reasonable measures to establish the source of wealth and the sources of funds of clients and beneficial-owners identified as PEPs and report all anomalies immediately to the ***SEC*** and FIC.

vi. ***CMOs*** in a business relationship with PEPs shall conduct enhanced ongoing monitoring of that relationship. In the event of any transaction that is abnormal, ***CMOs shall*** flag the account and report immediately to the FIC.

2.11. Attention to Complex and unusually Large Transactions

Section 6(6) of Act 874 requires CMOs to pay attention to complex and unusually large transactions in that respect:

a. **CMOs shall** pay special attention to all complex, unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. ***Such*** transactions or patterns of transactions include:
   i. Significant transactions relative to a relationship,
   ii. Transactions that exceed certain limits,
   iii. Very high account turnover inconsistent with the size of the account balance or
   iv. Transactions which fall out of the regular pattern of the account's activity.

b. ***CMOs shall*** examine as far as possible the background and purpose for such transactions and set forth their findings in writing to the FIC; ***such finding shall be kept*** available for ***SEC***, FIC, and other relevant authorities and auditors for at least seven years.

2.12. Failure to Complete CDD

i. ***Every CMO*** that does not comply with the foregoing provisions shall:

a. not be permitted to open the account, commence business relations or perform the transaction; and

b. Be required to render a suspicious transaction report to the *FIC*.

ii. The ***CMO*** that has already commenced the business relationship shall terminate the business relationship and render suspicious transaction reports to the FIC.

2.13. Establishing Identity

a. Identification Evidence

The CMO shall establish the identity of the client with a view to obtaining the satisfaction that the prospective client is who she/he claims to be. The information obtained shall be updated when necessary. A risk-based approach shall be adopted in this exercise. Elements of perceived risks includes, source of funds, mode of payment, whether application is in or by a remote medium like telephone, fax, post or internet.

i. The ***client's*** identification process shall not start and end at the point of establishing the relationship but 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 will however differ from one type of ***client*** to another.

ii. The general principles for establishing the identity of both legal and natural persons and obtaining satisfactory identification evidence set out in this Manual are by no means exhaustive.

b. What is Identity?

i. Identity generally means a set of attributes such as names used, physical features, date of birth, and place of birth,

nNationality and the residential address at which the clients can be located. These are features which can uniquely identify a natural or legal person.

ii. In the case of a natural person, the date of birth is required to 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 clients.

iii. Where an international passport or national identity card is taken as evidence of identity, the number, date and place/country of issue (as well as expiring date in the case of international passport) are required to be recorded.

c. When Must Identity be verified?

i. Identity shall be verified whenever a business relationship is to be established, on account opening or during a one-off transaction or when a series of linked transactions take place. "Transaction" in this Manual is defined to include the giving of advice. The "advice" here does not apply when information is provided about the availability of products or services nor applies when a first interview/discussion prior to establishing a relationship takes place.

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

d. Whose Identity Must Be Verified?

i. ***Clients*** - sufficient evidence of the identity must be obtained to ascertain that the ***client*** is the very person he/she claims to be.

ii. A person acting on behalf of others - The obligation is to obtain sufficient evidence of identities of the **two** persons involved.

iii. There is no obligation to look beyond the ***client*** where:

a. The client is acting on his/her own account (rather than for a specific client or group of ***clients***);
b. A client is a bank, broker-dealer, fund manager or any other regulated ***CMO****, or* financial institutions; and
c. All the businesses are to be undertaken in the name of a regulated **CMO** or financial institution.

iv. In other circumstances, unless the ***client*** is a regulated ***CMO*** or financial institution acting as agent on behalf of one or more underlying ***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:

1. The named account holder/person in whose name an investment is registered;
2. Any principal beneficial owner of funds being invested who is not the account holder or named investor;
3. The principal controller(s) of an account or business relationship (i.e. those who regularly provide instructions); and
4. Any intermediate parties (e.g. where an account is managed or owned by an intermediary).

v. ***CMOs shall*** take appropriate steps to identify directors and all the signatories to an account.

vi. Joint applicants/account holders - identification evidence shall be obtained for all the account holders.

vii. For higher risk businesses undertaken for private companies (i.e. those not listed on the stock exchange) sufficient evidence of identity and address shall be verified in respect of:

1. The principal underlying beneficial owner(s) of the company with 10% interest and above; and
2. Persons with controlling interest in the company either as shareholders, directors or senior management.

viii. ***CMOs 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 higher risk categories of clients in this Manual.

ix. **Trusts** – ***CMOs 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.

e. Savings Schemes and Investments in Third Parties' Names (or accounts for banks): When an investor sets up a savings accounts or a regular savings 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 savings scheme shall be regarded as the applicant for business for whom identification evidence must be obtained in addition to the legal owner/beneficiary.

f. Personal pension advisors

These are charged with the responsibility to obtain the identification evidence on behalf of the Pension Fund Provider. CMOs shall demand confirmation of identification evidence given on the transfer of a pension to another provider.

Comment [PMY9]: Formatting. Look up the entire document

g. Timing of Identification Requirements

i. The appropriate time frame for obtaining satisfactory evidence of identity depends on the nature of the business, the geographical location of the parties and whether it is possible to obtain and verify the evidence of identity before commitments are entered into or money changes hands. However, any occasion when business is conducted before satisfactory evidence of identity has been obtained shall be exceptional and can only be those circumstances justified with regard to the risk.

ii. To this end, ***CMOs shall****:*

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

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

iii. ***CMOs shall*** observe the provisions in the Timing of Verification section of this Manual.

iv. ***A CMO*** may however start processing the transaction or application immediately, provided that it:

1. promptly takes appropriate steps to obtain identification evidence;

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

v. The failure or refusal by an applicant to provide satisfactory identification evidence within a reasonable time-frame without adequate explanation may lead to a suspicion that the depositor or investor is engaged in

money laundering. The ***CMO shall*** therefore make a Suspicious Transaction Report to the FIC based on the information in its possession before the funds involved are returned to the potential client or sent where they came from.

vi. ***CMOs shall*** include in its Compliance Program written and consistent policies of closing an account or unwinding a transaction where satisfactory evidence of identity cannot be obtained.

vii. ***CMOs shall*** respond promptly to inquiries made by competent authorities relating to the identity of their clients.

h. Cancellation & Cooling-Off Rights

Where an investor exercises cancellation rights or cooling-off rights, the sum invested must be repaid subject to deductions, where applicable. Since cancellation/or cooling-off rights could offer a readily available route for laundering money, **CMOs 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 FIC.

i. Redemptions/Surrenders

a) When an investor finally realizes his investment (wholly or partially), if the amount payable is $10,000 (or its equivalent) for an individual or $25,000 (or its equivalent) for a body corporate, or such other monetary amounts as may, from time to time, be stipulated by any applicable money laundering legislation or regulation, the identity of the investor must be verified and recorded if it had not been done previously.

b) In the case of redemption or surrender of an investment (wholly or partially), a ***CMO shall*** take reasonable measures to establish the identity of the investor where payment is made to:

1. The legal owner of the investment by means of a cheque crossed "account payee"; or
2. A bank account held (solely or jointly) in the name of the legal owner of the investment by any electronic means effective for transfer funds.

2.14. Identification Procedures

a. General Principles of identification procedures include:

i. A ***CMO shall*** ensure that it is dealing with a real person or organization (natural, artificial or legal) by obtaining sufficient identification evidence. When 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 ***CMO***.

ii. 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.

iii. Since no single form of identification can be fully guaranteed as genuine or representing correct identity, the identification process***es*** shall ***be*** cumulative.

Comment [PMY10]: ????????

Comment [PMY11]: ???????

iv. The procedures adopted to verify the identity of private individuals and whether or not

identification was done face to face or remotely are ***required to be stated in the client's file***. The reasonable steps taken to avoid single, multiple fictitious applications or substitution (impersonation) fraud shall be stated by the ***CMO*** in the ***client's*** file.

v. An introduction from a respected ***client,*** a person personally known to a Director or Manager or a senior member of staff often provides comfort but must not replace the need for identification evidence requirements to be complied with as set out in this Manual.

vi. Details of the person who initiated and authorized the introduction shall be kept in the ***client'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.

b. Identification procedures for clients resident in Ghana

1. New Business for Existing Clients

i. When an existing ***client*** 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 of such a client unless the name or the address provided does not tally with the information in the ***CMO's*** file. However, procedures ***shall*** be put in place to guard against impersonation and fraud. The opportunity of opening the new account shall also be taken to ask the ***client*** to confirm the relevant details and to provide any missing KYC information. This is particularly important:

- If there was an existing business relationship with the ***client*** and identification evidence had not previously been obtained; or

- If there had been no recent contact or correspondence with the ***client*** within the past twelve months; or

- When a previously dormant account is re-activated.

- 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 this Manual.

2. Certification of Identification Documents

i. In order to guard against the dangers of postal-interception and fraud, prospective ***client*** shall not be asked to send by post originals of their valuable personal identity documents such as international passport, identity card, driving licence, etc.

ii. Where there is no face to face contact with the ***client*** and documentary evidence is required, copies certified by a lawyer, notary public/court of competent jurisdiction, senior civil or public servant, a commissioned officer of the Ghana Armed Forces; captain and above or persons of equivalent rank in the other security services, a registered medical practitioner, a solicitor or barrister or other recognised professionals registered with their respective regulating bodies shall be obtained. The person undertaking the

certification must be known and capable of being contacted if necessary.

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

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

v. Senior official within the account opening institution or;

vi. Notary public/court of competent jurisdiction

vii. Certified copies of identification evidence are to be stamped, dated and signed "original sighted by me" by a senior officer of the ***CMO. CMOs shall*** always ensure that a good production of the photographic evidence of identity is obtained. Where this is not possible, a copy of evidence certified as providing a good likeness of the applicant could only be acceptable in the interim, which shall not exceed the period of 30 working days.

3. Recording Identification Evidence

i. Records of the supporting evidence and methods used to verify identity are required to be retained for a minimum period of seven years after the account is closed or the business relationship ended.

ii. Where the supporting evidence could not be copied at the time it was presented, the reference numbers and other relevant details of the identification evidence are required to be recorded to enable the documents to be obtained later. Confirmation is required to be provided that the original documents

were seen by certifying either on the photocopies or on the record that the details were taken down as evidence.

iii. Where checks are made electronically, a record of the actual information obtained or of where it can be re-obtained must be retained as part of the identification evidence. Such records will make the reproduction of the actual information that would have been obtained before, less cumbersome.

iv. An accountable institution may appoint a person to keep records on behalf of the institution in conformity with section 8(4, 5and 6) of Act 874.

4. Concession in respect of Payment Made by Post.

i. Concession may be granted for product or services (where the money laundering risk is considered to be low) in respect of long-term life insurance business or purchase of personal investment products. If payment is to be made from an account held in the clients' name (or jointly with one or more other persons) at a regulated ***CMO***, no further evidence of identity is necessary.

ii. **Investment Funds**:
In circumstances where the balance in an investment funds account is transferred from one Funds Manager to another and the value at that time is above US$10,000 or its equivalent for an individual and $25,000 or its equivalent for a body corporate and identification evidence has neither been taken nor confirmation obtained from the original Fund Manager, then such evidence shall be obtained at the time of the transfer.

5. Documenting Evidence of Identity

In order to guard against forged or counterfeit-documents, care shall be taken to ensure that

documents offered are originals. Copies that are dated and signed 'original seen' by a senior public servant or equivalent in a reputable private organization could be accepted in the interim, pending presentation of the original documents. Hereunder are examples of suitable documentary evidence for Ghanaian resident individuals:

(i) **Personal Identity Documents**

1. Valid International Passport
2. Residence Permit issued by the Immigration Authorities
3. Current Driving Licence issued by the Driver and Vehicle Licensing Authority (DVLA)
4. Tax Clearance Certificate issued by Ghana Revenue Authority
5. Birth Certificate/Sworn Declaration of Age
6. National Identity card
7. National Health Insurance ID

(ii) **Documentary Evidence of Address**

1. Record of home visit in respect of non-Ghanaians
2. Confirmation from the electoral register that a person of that name lives at that address
3. Recent utility bill (e.g. ECG, GWCL, telephone etc.)
4. Current driving licence issued by DVLA
5. Bank statement or passbook containing current address
6. State/local government rates
7. Solicitor's letter confirming recent house purchase or search report from the Land Registry
8. Tenancy Agreement
9. Search reports on prospective client's place of employment and residence signed by a senior officer of the ***CMO***.

(iii) **Checking Telephone Directory**

Checking of a local or national telephone directory can be used as additional corroborative evidence ***but*** not as a primary check.

6. Physical checks on private individuals resident in Ghana

i. It shall be mandatory for a ***CMO*** to establish the true identities and addresses of its clients and for effective checks to be carried out to ***guard*** against substitution of identities by client.

ii. Additional confirmation of the clients' identity and the fact that the application was made by the person identified shall be obtained through one or more of the following procedures:

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

2. An initial deposit cheque drawn on a personal account in the clients name by another CMO in Ghana;

3. Telephone contact with the client prior to opening the account on an independently verified home or business number or a "welcome call" to the clients 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;

4. Internet sign-on following verification procedures where the client 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;

5. ATM card or account activation procedures.

iii. ***CMOs 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 within the relationship are also obtained from the clients.

7. Electronic Checks

i. As an alternative or supplementary to documentary evidence of identity and address, the clients' identity, address and other available information may be checked electronically by accessing other data-bases or sources. Each source may be used separately as an alternative to one or more documentary checks.

ii. ***CMOs shall*** use a combination of electronic and documentary checks to confirm different sources of the same information provided by the clients.

iii. In respect of electronic checks, confidence as to the reliability of information supplied will be established by the cumulative nature of checking across a range of sources, preferably covering a period of time or through qualitative checks that assess the validity of the information supplied. The number or quality of checks to be undertaken will vary depending on the diversity as well as the breadth and depth of information available from each source. Verification that the client is the data-subject also needs to be conducted within the checking process.

iv. Some examples of suitable electronic sources of information are ***as follows:***

1. An electronic search of the Electoral Register (is not to be used as a sole identity and address check);

2. Access to internal or external account database; and

3. An electronic search of public records, where available.

v. CMOs shall put in place internal procedures for the identification of socially but financially disadvantaged persons.

vi. CMOs should apply procedures to guard against impersonation, invented identities and the use of false address. When dealing with non-face-to-face persons extra measures shall be undertaken for reassurance.

vii. Where a ***CMO*** has reasonable grounds to conclude that an individual client is not able to produce the detailed evidence of his identity and cannot reasonably be expected to do so, the ***Operator*** may accept as identification evidence of a letter or statement from a person in a position of responsibility such as solicitors, doctors, ministers of religion and teachers who know the client, confirming that the client is who he says he is, and his permanent address.

viii. When a ***CMO*** has decided to treat a client as "financially excluded", it is required to record the reasons for doing so along with the account opening documents and returns rendered to the ***SEC*** and FIC quarterly.

ix. Where a letter/statement is accepted from a professional person, it shall include a telephone number where the person can be contacted for verification. The ***CMO shall*** verify from an independent source the information provided by the professional person.

x. In order to guard against "financial exclusion" and to minimize the use of the exception procedure, ***CMOs shall*** include in their internal procedures the "alternative documentary evidence of personal identity and address" that can be accepted.

xi. ***CMOs shall*** put in place additional monitoring for accounts opened under the financial exclusion exception procedures to ensure that such accounts are not misused.

8. Identification procedures for clients not resident in Ghana

1. Private Individuals not resident in Ghana

i. For those prospective clients who are not resident in Ghana but who make face-to-face contact, international passports or national identity cards ***shall*** generally be available as evidence of the name of the clients.

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

ii. ***CMOs shall*** obtain separate evidence of the applicant's permanent residential address from the best available evidence, preferably from an official source. A "P.O. Box number" alone is not accepted as evidence of address. The applicant's residential address ***shall*** be such that it can be physically located.

iii. Relevant evidence ***shall*** be obtained by the ***CMO*** directly from the clients or through a reputable credit or **CMO** in the applicant's home country or country of residence. However, particular care shall be taken when relying on identification evidence provided from other countries. ***CMOs shall*** ensure that the client's true identity and current permanent address are actually confirmed. In such cases, copies of relevant identity documents shall be sought and retained.

iv. Where a foreign national has recently arrived in Ghana, reference might be made to his/her employer, university, evidence of travelling documents, etc. to verify the applicant's identity and residential address.

2. Private Individuals not Resident in Ghana: Supply of Information

i. For a private individual not resident in Ghana, who wishes to supply documentary information by post, telephone or electronic means, a risk-based approach shall be taken. The ***CMO shall*** obtain one separate item of evidence of identity in respect of the name of the clients and one separate item for the address.

ii. Documentary evidence of name and address can be obtained:

a. By way of original documentary evidence supplied by the clients;

b. By way of a certified copy of the client's passport or national identity card and a separate certified document verifying address e.g. a driving licence, utility bill, etc.; or

c. Through a branch, subsidiary or head office of a correspondent bank.

ii. Where the client does not already have a business relationship with the foreign ***CMO*** that is supplying the information, certified copies of relevant underlying documentary evidence must be sought, obtained and retained by the institutions.

iii. Where necessary, an additional comfort must be obtained by confirming the client's true name,

address and date of birth from a reputable approved institution in the client's home country.

2.15. Information to establish identity

Establishing the identity of natural persons

A. Obtaining information on natural persons

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

1. Legal name and any other names used (such as maiden name);
2. Correct permanent address (full address shall be obtained and a Post Office box number is not sufficient);
3. Telephone number, fax number, and e-mail address;
4. Date and place of birth;
5. Nationality;
6. Occupation, public position held and name of employer;
7. An official personal identification number or other unique identifier contained in an unexpired official document such as passport, identification card, residence permit, social security records or driving licence that bears a photograph of the clients;
8. Signature.

B. Verification of information on natural persons

A ***CMO shall*** verify this information by at least one of the following methods:

1. Confirming the date of birth from an official document (e.g. birth certificate, passport, identity card, social security records);

2. Confirming the permanent address (e.g. utility bill, tax assessment, bank statement, a letter from a public authority);

3. Contacting the clients by telephone, by letter or e-mail to confirm the information supplied after an account has been

opened (e.g. a disconnected phone, returned mail, or incorrect e-mail address ***shall*** warrant further investigation);

4.Confirming the validity of the official documentation provided through certification by an authorized person (e.g. embassy official, notary public).

5. Such other documents of an equivalent nature may be produced as satisfactory evidence of clients' identity.

6. ***The CMOs*** shall apply effective client identification procedures for non-face-to-face client as for those available ***physically.***

C. Assessment of risk profile of natural persons

From the information provided, ***CMOs*** shall be able to make an initial assessment of a client's risk profile. Particular attention needs to be focused on those clients identified as having a higher risk profile. Additional inquiries made or information obtained in respect of those clients ***shall*** include the following:

1. Evidence of an individual's permanent address sought through a credit reference agency search, or through independent verification by home visits;
2. Personal reference (i.e. by an existing ***client*** of the same institution);
3. Prior client bank reference and contact with the bank regarding the ***client;***
4. Source of wealth;
5. Verification of employment, public position held (where appropriate).

The ***client*** acceptance policy shall not be so restrictive to amount to a denial of access by the general public to Securities transactions, especially for people who are financially or socially disadvantaged.

D. Obtaining information on Institutions

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

E. Corporate Entities

For corporate entities (i.e. corporations and partnerships), the following information ***shall*** be obtained:

1. Registered name of institution and registered number;
2. Registered address and any separate principal place of institution's business operations;
3. Mailing address of institution;
4. Contact telephone and fax numbers;
5. Some form of official identification number, if available (e.g. Tax identification number);
6. The original or certified copy of the Certificate of Incorporation, Certificate to commence business and the Regulations;
7. The resolution of the Board of Directors to open an account and identification of those who have authority to operate the account;
8. Nature and purpose of business and its legitimacy;
9. Particulars of shareholders (20% or more) and at least two resident directors;

F. A ***CMO shall*** verify this information by at least one of the following methods:

1. For established corporate entities -reviewing a copy of the latest annual report and financial statements (audited, if available);

2. Conducting an enquiry by a business information service or an undertaking from a reputable and known firm of lawyers or accountants in good standing confirming the documents submitted;

3. Undertaking a company search and/or other commercial enquiries to see that the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated;

4. Utilizing an independent information verification process, such as accessing public and private databases established under law;

5. Obtaining prior bank references;

6. Visiting the corporate entity; and

7. Contacting the corporate entity by telephone, mail or e-mail;

G. The ***CMOs shall*** also take reasonable steps to verify the identity and reputation of any agent that opens an account on behalf of corporate clients, if that agent is not an officer of the corporate ***client.***

H. Obtaining and verifying information on Corporations/Partnerships

1. For corporations/partnerships, the principal guidance is to look behind the ***Operator*** to identify those who have control over the business and the company's/partnership's assets, including those who have ultimate control.

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

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

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

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

I. Obtaining information on Other Types of Operators

The following information ***shall*** be obtained in addition to that required to verify the identity of the principals in respect of Retirement Benefit Programmes, Mutual/Friendly Societies, Cooperatives and Provident Societies, Charities, Clubs and Associations, Trusts and Foundations and Professional Intermediaries:

- Name of account;
- Mailing address;
- Contact telephone and fax numbers;
- Some form of official identification number, such as tax identification number;
- Description of the purpose/activities of the account holder as stated in a formal constitution; and
- Copy of documentation confirming the legal existence of the account holder such as an extract or an official search report from the appropriate regulatory institution.

J. Verification of information of other types of operations

A ***CMO shall*** verify this information by at least one of the following:

1. Obtaining an independent undertaking from a ***legal practitioner*** or ***chartered*** Accountant confirming the documents submitted;
2. Obtaining prior bank references; and
3. Accessing public and private databases or official sources.

K. Obtaining information on Retirement Benefit Programmes

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 the ***CMO shall*** take steps to verify their identities.

L. Obtaining information on Mutual/Friendly, Cooperative and Provident Societies

Where these entities are clients, the principals to be identified ***shall*** be considered to be those persons exercising control or significant influence over the organisation's assets. This often includes Board members, executives and account signatories.

M. Obtaining information on Charities, Clubs and Associations

In the case of accounts to be opened for charities, clubs, and societies, the ***CMOs shall*** take reasonable steps to identify and verify at least two signatories along with the ***operator*** itself. The principals who shall be identified ***shall*** be considered to be those persons exercising control or significant influence over the organization’s assets.

This includes members of the governing body or committee, the President, Board members, the Treasurer, and all signatories.

In all cases, independent verification shall be obtained that the persons involved are true representatives of the ***operators***.

N. Obtaining information on Trusts and Foundations

When opening an account for a Trust, the ***capital Market Operator shall*** take reasonable steps to verify the trustees, the settlor (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, steps ***shall*** be taken to verify the founder, the managers/directors and the beneficiaries.

O. Obtaining information on 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. Where the funds are co-mingled, the ***CMO shall*** look through to the beneficial-owners. However, there may be circumstances that ***CMO*** may not look beyond the intermediary (e.g. when the intermediary is subject to the same due diligence standards in respect of its client base as the ***CMO***).

P. Obtaining information on Collective Investment Schemes and Limited Partnerships

Where such circumstances apply and an account is opened for an open or closed ended investment company (unit trust or limited partnership) also subject to the same due diligence standards in respect of its client base as the ***CMO,*** the following

shall be considered as principals and the ***CMO shall*** take steps to identify them:

1. The fund itself;
2. Its directors or any controlling board (where it is a company)
3. Its Trustee (where it is a Unit Trust)
4. Its managing (general) partner (where it is a limited partnership)
5. Account signatories;
6. Any other person who has control over the relationship such as fund administrator or manager.

Q. Obtaining information on other investment vehicles

Where other investment vehicles are involved, the same steps ***shall*** be taken as in above (where it is appropriate to do so). 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.

R. Intermediaries shall be treated as individual clients of the ***CMO*** and the standing of the intermediary ***shall*** be separately verified by obtaining the appropriate information itemized above.

2.16. Non face-to-face identification

i. In view of possible false identities and impersonations that ***may*** arise with non-face-to-face clients, additional measures/checks ***shall*** be undertaken to supplement the documentary or electronic evidence.

These additional measures/***checks*** will apply whether the applicant is resident in Ghana or elsewhere and ***shall*** be

particularly robust where the applicant is requiring a margin facility or other product/service that offers money transmission or third party payments.

ii. Procedures to identify and authenticate the ***client shall be put in place*** to ensure that there is sufficient evidence either documentary or electronic to confirm his address and personal identity and to undertake at least one additional check to guard against impersonation ***and*** fraud.

iii. The extent of the identification evidence required will depend on the nature and characteristics of the product or service and the assessed risk.

iv. If reliance is being placed on intermediaries to undertake the processing of applications on the ***client's*** behalf, checks ***shall*** be undertaken to ensure that the intermediaries are regulated for money laundering 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.

v. ***CMOs shall*** conduct regular monitoring of internet-based businesses/clients. If 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. AMLRO officers are required to review these solutions, record exemptions and report same quarterly to the ***SEC*** and FIC.

2.17. Establishing identity for refugees and asylum seekers

i. A refugee and asylum seeker may require a basic account without being able to provide evidence of identity. In such circumstances, authentic references from the Ministry of Interior or an appropriate government agency shall be used in conjunction with other readily available evidence.

ii. Additional monitoring procedures shall however be undertaken to ensure that the use of the account is consistent with the client's circumstances and returns rendered half yearly to SEC and FIC.

2.18. Establishing Identity for Students and Minors

i. When opening accounts for students or other young persons, the normal identification procedures set out in this Manual ***shall*** *be* followed as far as possible. Where such procedures would not be relevant or do not provide satisfactory identification evidence, verification could be obtained:

a. Via the home address of the parent(s); or

b. By obtaining confirmation of the applicant's address from his/her institution of learning; or

c. By seeking evidence of a tenancy agreement or student accommodation contract.

ii. Often, an account for a minor will be opened by a family member or guardian. In cases where the adult opening the account does not already have an account with the ***CMO,*** the identification evidence for that adult, or of any other person who will operate the account shall be obtained in addition to obtaining the birth certificate or passport of the child. It shall be noted that this type of account could be open to abuse and therefore strict monitoring shall be undertaken, and reports submitted half yearly to SEC and FIC.

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

2.19. Quasi Corporate Clients

A. Establishing Identity - Trust, Nominees and Fiduciaries

i. Trusts, nominee companies and fiduciaries are popular vehicles for criminals wishing to avoid the identification procedures and mask the origin of the proceeds of criminal activity they wish to launder. The particular characteristics of Trusts that attract the genuine clients, the anonymity and complexity of structures that they can provide are also highly attractive to money launderers.

ii. Identification and "Know Your Business" procedures ***shall*** be set and managed according to the perceived risk, in trust, nominees and fiduciaries accounts.

iii. The principal objective for money laundering prevention via trusts, nominees and fiduciaries is to verify the identity of the provider of funds such as the settlor, those who have control over the funds (the trustees and any controller who has the power to remove the trustees). For discretionary or offshore Trust, the nature and purpose of the Trust and the original source of funding must be ascertained.

iv. Whilst reliance can often be placed on other ***CMOs*** that are to undertake the checks or confirm identity, the responsibility to ensure that this is undertaken rests with the ***CMO***. The underlying evidence of identity must be made available to law enforcement agencies in the event of an investigation.

v. Identification requirements must 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.

B. Offshore Trusts

i. Offshore Trusts present a higher money laundering risk and therefore additional measures are needed for Special Purpose Vehicles (SPVs) or International Business Companies connected to Trusts, particularly when Trusts are set up in offshore locations with strict bank secrecy or confidentiality rules. Those created in jurisdictions without

equivalent money laundering procedures in place ***shall*** warrant additional enquiries.

ii. Unless the ***client*** for business is itself a regulated ***CMO,*** measures ***shall*** be taken to identify the Trust company or the corporate service provider in line with the requirements for professional intermediaries or companies generally.

iii. Certified copies of the documentary evidence of identity for the underlying principals such as settlors, controllers, etc. on whose behalf the ***client*** for business is acting, ***shall*** also be obtained.

iv. For overseas Trusts, nominee and fiduciary accounts, where the ***client*** is itself a ***CMO*** that is regulated for money laundering purposes:

a. Reliance can be placed on an introductory letter, certificate or licence stating that evidence of identity exists for all underlying principals and confirming that there are no anonymous principals;
b. The trustees/nominees shall be asked to state from the outset the capacity in which they are operating or making the application;
c. Documentary evidence of the appointment of the current Trustees shall also be obtained.

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

vi. Any application to open an account or undertake a transaction on behalf of another without the ***client*** identifying their Trust or Nominee capacity shall be regarded as suspicious and shall lead to further enquiries and submission of reports to ***SEC*** and FIC.

vii. Where a CMO in Ghana is itself the ***client*** to an offshore Trust on behalf of ***its*** **clients,** if the corporate Trustees are not regulated, then the Ghanaian ***CMO shall*** undertake the due diligence on the Trust itself.

viii. If the funds have been drawn upon an account that is not under the control of the Trustees, the identity of two of the authorized signatories and their authority to operate the account shall also be verified. When the identities of beneficiaries have not previously been verified, verification shall be undertaken when payments are made to them.

C. Conventional Family and Absolute Ghanaian Trusts

i. In the case of conventional Ghanaian Trusts, identification evidence shall be obtained for:

a. Those who have control over the funds (the principal trustees who may include the settlor);
b. The providers of the funds (the settlors, except where they are deceased);
c. Where the settlor is deceased, a written confirmation shall be obtained for the source of funds (grant of probate or copy of the Will or other document(s) creating the Trust).

ii. Where a corporate Trustee such as a bank 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 procedures contained in this Manual for verifying the identity of persons, institutions or companies shall be followed.

iii. Although a ***CMO*** may not review any existing Trust, confirmation of the settlor and the appointment of any additional Trustees ***shall*** be obtained.

iv. Copies of any underlying documentary evidence ***shall*** be certified as true copies. In addition, a check shall be carried out to ensure that any bank account on which the Trustees have drawn funds is in their names. Taking a risk based approach; the

identity of any additional authorised signatories shall be verified when required.

D. Receipt and Payment of Funds

i. Where money is received on behalf of a Trust, reasonable steps ***shall*** be taken to ensure that:

a. The source of the funds is properly identified; and

b. The nature of the transaction or instruction is understood.

ii. It is also important to ensure that payments are properly authorized in writing by the Trustees.

E. 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. This also applies to life proceeds.

F. Powers of Attorney and Third Party Mandates

a. The authority to deal with assets under a Power of Attorney and Third Party Mandates constitutes a business relationship. Consequently, at the start of the relationship, identification evidence ***shall*** be obtained from the holders of powers of attorney and third party mandates in addition to the ***clients*** or subsequently on a later appointment of a new attorney, if advised, particularly within one year of the start of the business relationship. New attorney for corporate or Trust business shall always be verified. The most important requirement is for ***CMO*** to ascertain the reason for the grant of the power of attorney.

b. Records of all transactions undertaken in accordance with the Power of Attorney ***shall*** be maintained as part of the client's record. This should conform to FATF Recommendation 17.

G. Executorships accounts

i. When an account is opened for the purpose of winding up the estate of a deceased person, the identity of the executor /administrator of the estate ***shall*** be verified.

ii. However, identification evidence would not normally be required for the executors/administrators when payment is being made from an established bank or mortgage institution's account in the deceased's name, solely for the purpose of winding up the estate in accordance with the Grant of Probate or Letters of Administration. Similarly, where a life policy pays out on death, there shall be no need to obtain identification evidence for the legal representatives.

iii. Payments to the underlying named beneficiaries on the instructions of the executor or administrator may also be made without additional verification requirements. However, if a beneficiary wishes to transact business in his/her own name, then identification evidence shall be required.

iv. In the event that suspicion ***is*** aroused concerning the nature or origin of assets comprising an estate that is being wound up, a report is required to be submitted to FIC.

H. Unincorporated Business/Partnerships

i. Where the ***client*** is an un-incorporated business or a partnership whose principal partners/controllers do not already have a business relationship with the ***CMOs***, identification evidence shall be obtained for the principal beneficial owners/controllers. This would also entail identifying one or more signatories in whom significant control has been vested by the principal beneficial owners/controllers.

ii. Evidence of the trading address of the business or partnership ***shall*** be obtained.

iii. The nature of the business or partnership ***shall*** be ascertained (but not necessarily verified from a partnership

deed) to ensure that it has a legitimate purpose. Where a formal partnership arrangement exists, a mandate from the partnership authorizing the opening of an account or undertaking the transaction and conferring authority on those who will undertake transactions ***shall*** be obtained.

2.20. Client Accounts Opened by Professional Intermediaries

Stock-brokers, fund managers, and DNFBPs such as solicitors, accountants, estate agents and other intermediaries frequently hold funds on behalf of their clients in client's accounts opened with CMOs. In such cases the customer is the professional and is different when the professional introduces a client.

2.21. Limited Liability Partnerships

These should be treated as corporate customers for verification of identity and KYC purposes.

1. PURE CORPORATE CLIENTS

A. General Principles

i. Complex organizations and their structures, other corporate and legal entities are the most likely vehicles for money laundering. Those that usually are privately owned are being fronted by legitimate trading companies. Care shall be taken to verify the legal existence of the client company from official documents or sources and to ensure that persons purporting to act on its behalf are fully authorized.

Enquiries shall be made to confirm that the legal person is not merely a "brass-plate company" where the controlling principals cannot be identified.

ii. The identity of a corporate company comprises:

i. Registration number;

ii. Registered corporate name and any trading names used;

iii. Registered address and any separate principal trading addresses;

iv. Particulars of directors;

v. Owners and shareholders; and

vi. The nature of the company's business.

vii. Company regulations

iii. The extent of identification measures required validating this information or the documentary evidence to be obtained depends on the nature of the business or service that the company requires from the ***CMO***. A risk-based approach shall be taken. In all cases, information as to the nature of the normal business activities that the company expects to undertake with the **CMO shall** be obtained. Before a business relationship is established, measures shall be taken by way of company search at the Registrar General's Department and other regulatory authorities and other commercial enquiries undertaken to check that the clients-company's legal existence has not been or is not in the process of being dissolved, struck off, wound up or terminated.

B. Non Face-to-Face Business

i. As with the requirements for private individuals, because of the additional risks with non-face-to-face business, additional procedures ***shall*** be undertaken to ensure that the ***client's*** business, company or society exists at the address provided and it is for a legitimate purpose.

ii. Where the characteristics of the product or service permit, care ***shall*** be taken to ensure that relevant evidence is obtained to confirm that any individual representing the company has the necessary authority to do so.

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

C. Low Risk Corporate Business

i. Public Quoted Companies

a. Corporate ***clients*** that are listed on the ***securities*** exchange are considered to be publicly owned and generally accountable. Consequently, there is no need to verify the identity of the individual shareholders.

b. It is not necessary to identify the directors of a quoted company.

c. ***CMOs*** shall ensure that the individual officer or employee (past or present) is not using the name of the company or its relationship with the ***CMO*** for criminal purposes. The Board Resolution or other authority for any representative to act on behalf of the company in its dealings with the ***CMO shall*** be obtained to confirm that the individual has the authority to act. Phone calls can be made to the Chief Executive Officer or his designated representative of such a company to intimate him of the application to open the account ***with the CMO***.

d. No further steps ***shall*** be taken to verify identity over and above the usual commercial checks where the applicant company is:

i. Listed on a securities market; or

ii. There is independent evidence to show that it is a wholly owned subsidiary or a subsidiary under the control of such a company.

e. Due diligence shall be conducted where the account or service required falls within the category of higher risk business.

D. Private /Public unquoted Companies

i. Where the ***client*** is ***a private/public unquoted company*** and none of the principal directors or shareholders already has an account with the ***CMO***, the following documents shall be

obtained from an official or recognized independent source to verify the business itself:

a. A copy of the certificate of incorporation/registration, evidence of the company's registered address and the list of shareholders and directors;

b. A search at the RGD or an enquiry via a business information service to obtain the information in (a) above; and

c. An undertaking from a reputable and recognized firm of lawyers or accountants confirming the documents submitted to the CMO.

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

E. Higher Risk Businesses relating to Private/Public unquoted Companies

i. For private **/public unquoted Companies** undertaking higher risk business (in addition to verifying the legal existence of the business) the principal requirement is to look behind the corporate entity to identify those who have ultimate control over the business and the company's assets. What constitutes significant shareholding or control for this purpose will depend on the nature of the company. Identification evidence is required to be obtained for those shareholders with interests of 10% or more.

ii. The principal control rests with those who are mandated to manage the funds, accounts or investments without requiring authorization and who would be in a position to override internal procedures and control mechanisms.

iii. Identification evidence ***shall*** be obtained for the principal-beneficial 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 objective is to undertake measures that look behind that company or vehicle and verify the identity of the beneficial-owner(s) or settlors. When **a CMO** becomes aware that the principal-beneficial owners/controllers have changed, they ***shall*** ensure that the identities of the new ones are verified.

iv. ***CMOs shall*** identify directors who are not principal controllers and signatories to an account for risk based approach purposes.

v. Where there is suspicion as a result of change in the nature of the business transacted or investment account, further checks ***shall*** be made to ascertain the reason for the changes.

vi. Particular care shall be taken to ensure that full identification and "Know Your Clients" requirements are met if the company is an International Business Company (IBC) registered in an offshore jurisdiction.

viii. A visit to the place of business shall be undertaken to confirm the existence of business premises and the nature of business activities conducted. This should be done periodically and an STR submitted to the FIC where necessary.

F. Foreign *CMO*

i. For foreign ***CMOs***, the confirmation of existence and regulated status shall be checked by one of the following means:

a. Checking with the home country's ***Securities Market Regulator*** or relevant supervisory body;

b. Checking with another office, subsidiary ***or*** branch in the same country;

c. Checking with the Ghanaian regulated correspondent ***CMO*** of the overseas ***Operator***;

d. Obtaining evidence of its license or authorization to conduct ***Securities*** business from the ***Operator*** itself.

ii. In addition to the identity of the Principal Employer, the source of funding information from various international publications and directorates or any of the international business information services. Information from these sources shall be verified and recorded to ensure that a complete audit trail exists if the employer is dissolved or wound up.

iii. For the 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 Registrars or references from Professional Advisers or Investment Managers.

iv. Any payment of benefits by or on behalf of the Trustees of an Occupational Pension Scheme shall require verification of identity of the recipient.

v. Where individual members of an Occupational Pension Scheme are to be given personal investment advice, their identities shall be verified.

vi. 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.

G. Other Institutions

1. Charities in Ghana

a. Adherence to the identification procedures required for money laundering prevention purpose would remove the opportunities for opening unauthorised accounts with false identities on behalf of charities. Confirmation of the authority to act in the name of the charity is mandatory**.**

b. The practice of opening unauthorised accounts of this type under sole control is strongly discouraged. Accounts for charities in Ghana are required to be operated by a minimum of two signatories duly verified and documentation evidence obtained.

2. Registered Charities

a. When dealing with an application from a registered charity, the *CMO shall* obtain and confirm the name and address of the charity concerned.

b. To guard against the laundering of fraudulently obtained funds (where the person making the application or undertaking the transaction is not the official correspondent or the recorded alternate) a ***CMO*** is required to send a letter to the official correspondence, informing him of the schemes application before it. The official correspondence shall be requested to respond as a matter of urgency especially where there is any reason to suggest that the application has been made without authority.

c. Applications on behalf of unregistered charities ***shall*** be dealt with in accordance with procedures for clubs and societies set out in ***these Rules***.

3. Clubs and Societies

a. In the case of applications made on behalf of clubs or societies, a ***CMO shall*** take reasonable steps to satisfy itself as to the legitimate purpose of the organisation by sighting its constitution. The identity of at least two of the principal contact persons or signatories shall be verified initially in line with the requirements for private individuals. The signing authorities ***shall*** be structured to ensure that at least two of the signatories that authorize any transaction have been verified. When signatories change, ***CMOs shall*** ensure that the identities of at least two of the current signatories are verified.

b. 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 clients.

c. ***CMOs*** are required to look at each situation on a case –by case basis.

4. Occupational Pension Schemes

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 are required to be verified.

5. Religious Organizations (ROs) or Faith Based Organization (FBO)

A religious organisation is expected by law to be registered and shall therefore have a registered number. Its identity can be verified by reference to the appropriate registration body, headquarters or regional office. As a Registered organisation, the identity of at least two signatories to its account ***shall*** be verified.

6. Three-Tiers of Government/Parastatals (Ministries, departments and agencies)

Where the client for business is any of the above, the ***CMO shall*** verify the legal standing of the applicant, including its principal ownership and the address. A certified copy of the Resolution or other 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*** also be made with the Chief Executive Officer or his designate of the organisation/parastatals concerned, intimating him of the application to open the account with the ***CMO.***

7. Foreign Consulates

The authenticity of clients that request to undertake transactions with **CMOs** in the name of Ghanaian-resident foreign consulates and any documents of authorization presented in support of the

application ***shall*** be checked with the Ministry of Foreign Affairs or the relevant authorities in the Consulate's home country.

2.22. Intermediaries or Other Third Parties to Verify Identity or to Introduce Business

A. Who to rely upon and the circumstances

Whilst the responsibility to obtain satisfactory identification evidence rests with the ***CMO*** that is entering into the relationship with a client, it is reasonable, in a number of circumstances, for reliance to be placed on another ***CMO to****:*

i. Undertake the identification procedure when introducing a client and to obtain any additional KYC information from the client; or

ii. Confirm the identification details if the clients 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 Authorised Financial Intermediaries

i. Where an intermediary introduces a client and then withdraws from the ensuing relationship altogether, then the underlying client has become the applicant for the business. He ***shall*** be identified in line with the requirements for personal, corporate or business clients as appropriate.

ii. An introduction letter ***shall*** be issued by the introducing ***CMO*** or person in respect of each applicant for business. To ensure that product-providers meet their obligations that satisfactory identification evidence has been obtained and will be retained for the necessary statutory period, each introduction letter ***shall*** either be accompanied by certified copies of the identification evidence that has been obtained in line with the usual practice of certification of identification documents or by sufficient

details/reference numbers etc., that will permit the actual evidence obtained to be re-obtained at a later stage.

C. Written Applications

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

D. Non-Written Application

Unit Trust Managers and other product providers receiving non-written applications from financial intermediaries (where a deal is placed over the telephone or by other electronic means) have an obligation to verify the identity of clients and ensure that the intermediary provides specific confirmation that identity has been verified. A record ***shall*** be made of the answers given by the intermediary and retained for a minimum period of seven years.

E. Introductions from Foreign Intermediaries

Where introduced business is received from a regulated financial intermediary who is outside Ghana, the reliance that can be placed on that intermediary to undertake the verification of identity-check ***shall*** be assessed by the ***AMLRO*** or some other competent persons within the ***CMO*** on a case by case basis based on the knowledge of the intermediary.

F. Corporate Group Introductions

i. Where a client is introduced by one part of a financial sector group to another, it is not necessary for identity to be re-verified or for the records to be duplicated provided that:

a. The identity of the client has been verified by the introducing parent company, branch, subsidiary or associate in line with the AML Legislation to equivalent standards and taking account of any specific requirements such as separate address verification;

b. No exemptions or concessions have been applied in the original verification procedures that would not be available to the new relationship;

c. A group introduction letter is obtained and placed with the clients' account opening records; and

d. In respect of group introducers from outside Ghana, arrangements shall be put in place to ensure that identity is verified in accordance with requirements and that the underlying records of identity in respect of introduced clients are retained for the necessary period.

ii. Where ***a CMO*** has day-to-day access to all the Group's "Know Your ***Client"*** information and records, there is no need to identify an introduced client or obtain a group introduction letter if the identity of that ***client*** has been verified previously. However, if the identity of the client has not previously been verified, then any missing identification evidence will need to be obtained and a risk-based approach taken on the extent of KYC information that is available on whether or not additional information shall be obtained.

ii. ***CMOs shall*** ensure that there is no secrecy or data protection legislation that would restrict free access to the records on request by law enforcement agencies under court order or relevant mutual assistance procedures. If it is found that such restrictions apply, copies of the underlying records of identity ***shall,*** wherever possible, be sought and retained.

iii. Where identification records are held outside Ghana, it ***shall be*** the responsibility of the ***CMOs*** to ensure that the records available do, in fact, meet the requirements in this Manual.

G. Business Conducted by Agents

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

ii. A ***CMO*** may regard evidence as sufficient if it has established that the client:

a. Is bound by and has observed this Manual or the provisions of AML Legislation*;* and

b. As 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.

iii. Consequently, where another ***CMO*** deals with its own client (regardless of whether or not the underlying ***client*** is disclosed to the ***CMO***) then:

a. Where the agent is a ***CMO***, 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

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

c. In circumstances where an agent is either unregulated or is not covered by the relevant AML Legislation, then each case ***shall*** be treated on its own merits. The knowledge of the agent will inform the type of the due diligence standards to apply.

H. Correspondent Relationship

i. Transactions conducted through correspondent relationships need to be managed, taking a risk-based approach. "Know Your Correspondent" procedures are required to be established to ascertain whether or not the correspondent ***CMO*** or the counter-party is itself regulated for money laundering prevention. If regulated, the correspondent, ***CMO is*** required to verify the

identity of its ***clients*** in accordance with FATF standards. Where this is not the case, additional due diligence will be required to ascertain and assess the correspondent's ***CMO's internal*** policy on money laundering prevention and know your clients procedures.

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

iii. ***CMOs shall*** maintain records of having ensured that sufficient due diligence has been undertaken by the remitting CMO on the underlying client and the origin of the funds in respect of the funds passed through their accounts.

iv. ***CMOs shall*** guard against establishing correspondent relationships with high risk foreign CMOs (e.g. shell CMOs with no physical presence in any country) or with correspondent CMOs that permit their accounts to be used by such banks.

I. Acquisition of One *CMO*/Business by Another

i. When one ***CMO*** acquires the business and accounts of another ***CMO***, it is not necessary for the identity of all the existing clients to be re-identified, provided that all the underlying clients' records are acquired with the business. It is, however, important to carry out due diligence enquiries to confirm that the acquired ***operator*** had conformed to the requirements in this Manual.

ii. Verification of identity shall be undertaken as soon as it is practicable for all the transferred clients who were not verified by the transferor in line with the requirements for existing ***clients*** that open new accounts, where:

a. The money laundering procedures previously undertaken have not been in accordance with the requirements of this Manual;

b. The procedures cannot be checked; or

c. The clients-records are not available to the acquiring ***CMO***.

2.23. Receiving CMOS and Agents

A. Vulnerability of Receiving Bankers and Agents to Money Laundering

Receiving ***CMOs*** may be used by money launderers in respect of offers for sale where new issues are over-subscribed and their allocation is scaled down. In addition, the money launderer is not concerned if there is a cost involved in laundering proceeds of crime. New issues that trade at a discount will, therefore, still prove acceptable to the money launderer. Criminal funds can be laundered by way of the true beneficial-owner of the funds providing the payment for an application in another person's name, specifically to avoid the verification process and to break the audit trail with the underlying crime from which the funds are derived.

B. Who shall be identified?

i. ***Receiving CMOs*** shall obtain satisfactory identification evidence of new applicants, including such applicants in a rights issue where the value of a single transaction or a series of linked transactions is US$10,000 or its equivalent for foreign transfers or $10,000 or its equivalent for individuals and $25,000 for corporate body or more.

ii. If funds to be invested are being supplied by or on behalf of a third party, it is important that the identification evidence for both the applicant and the provider of the funds are obtained to ensure that the audit trail for the funds is preserved.

C. Applications Received via Brokers

i. Where the application is submitted (payment made) by a broker or an intermediary acting as agent, no steps need to be taken to verify the identity of the underlying applicants. However, the following standard procedures apply:

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

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

ii. The terms and conditions of the issue ***shall*** state that any requirements to obtain identification evidence are the responsibility of the broker lodging the application and not the receiving ***CMO***.

iii. 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.

D. Applications Received from Foreign Brokers

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

E. Multiple Family Applications

i. Where multiple family applications are received supported by one cheque and the aggregate subscription price is US$10,000 or its equivalent for foreign transfers; and $10,000 or more or its equivalent for an individual person, then identification evidence will not be required for:

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

b. A joint account holder; or

c. An application in the name of a child where the relevant company's Regulations prohibit the registration in the names of minors and 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.

ii. However, identification evidence of the signatory of the financial instrument will be required for any multiple family application for more than US$1,000 or its equivalent for foreign transfers; or more than $5, 000 or its equivalent for an individual; or more than $25, 000 or its equivalent for a body corporate where such is supported by a cheque signed by someone whose name differs from that of the applicant. Other monetary amounts or more may, from time to time, be stipulated by any applicable money laundering legislation/guidelines.

iii. Where an application is supported by a ***financial institution's*** branch cheque or bankers' draft, the applicant shall state the name and account number from which the funds were drawn:

a. On the front of the cheque; or

b. On the back of the cheque together with a branch stamp; or

c. Providing other supporting documents.

F. Linked Transactions

i. If it appears to a person handling applications that a number of single applications under US$10,000 or its equivalent and **$10, 000** or its equivalent in different names are linked (e.g. payments from the same ***CMO*** account) apart from the multiple family applications above, identification evidence ***shall*** be obtained in respect of parties involved in each single transaction.

ii. Instalment payment issues ***shall*** be treated as linked transactions where it is known that total payments will amount to US$10,000 or its equivalent for foreign transfers or

$10,000 or its equivalent for an individual; or $25,000 or its equivalent for body corporate or such other monetary amounts as may, from time to time, be stipulated by any applicable money laundering legislation or guidelines. Either at the outset or when a particular point has been reached, identification evidence ***shall*** be obtained.

iii. Applications that are believed to be linked and money laundering is suspected ***shall*** be processed on a separate batch for investigation after allotment and registration has been completed. Returns with the documentary evidence are to be rendered to the FIC accordingly. Copies of the supporting cheques, application forms and any repayment cheques shall be retained to provide an audit trail until the receiving ***CMO*** is informed by FIC or the investigating officer that the records are of no further interest.

2.24. Exemption from Identification Procedures

Where a client's identity was not properly obtained as contained in this Manual and Requirements for Account Opening Procedure, ***CMO****s* ***shall*** re-establish the client's identity in line with the contents of this Manual, except where it concerns:

i. **Ghanaian *CMOs***

Identification evidence is not required where the client for business is a Ghanaian ***CMO*** or person covered and regulated by the requirements of this Manual.

ii. **One-off Cash Transaction (Remittances, Wire Transfers, etc.)**

Cash remittances and wire transfers (either inward or outward) or other monetary instruments that are undertaken against payment in cash for clients who do not have an account or other established relationship with the ***CMO*** (i.e. walk–in clients) present a high risk for money laundering purposes. It is therefore required that adequate

procedures are established to record the transaction and relevant identification evidence taken, where necessary. Where such transactions form a regular part of the ***CMO's*** business, the limits for requiring identification evidence of US $1,000 or its equivalent for foreign transfers; $10,000 or its equivalent for individuals and $25,000 or its equivalent for a corporate body must, however, be observed.

iii. **Re-investment of Income**

The proceeds of a one-off transaction can be paid to a client or be further re-invested where records of his identification requirements were obtained and kept. In the absence of this, his/her identification requirements ***shall*** be obtained before the proceeds are paid to him or be re-invested on his behalf in accordance with the relevant provision of this Manual.

2.25. Timing of Verification

i. ***The CMO*** is to obtain satisfactory evidence that it is dealing with the real client (natural, corporate or legal), by obtaining and verifying adequate identification evidence. Where reliance is being placed on a third party to identify or verify the identity of the applicant, the overall legal responsibility for obtaining satisfactory identification evidence rests with the ***CMO***. ***CMOs shall*** insist on normal identification procedures for every client.

ii. ***CMOs shall*** verify the identity of the clients, beneficial-owner and occasional clients before or during the course of establishing a business relationship or conducting transactions for them.

ii. ***CMOs*** *shall* complete the verification of the identity of the clients and beneficial owner following the establishment of the business relationship, only when:

a. This can take place as soon as reasonably practicable;
b. It is essential not to interrupt the normal business conduct of the clients; and

c. The money laundering risks can be effectively managed.

iv. Examples of situations where it may be essential not to interrupt the normal conduct of business are:

a. ***Securities transactions****:* In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the client is contacting them and the performance of the transaction may be required before verification of identity is completed.

b. Non face-to-face business.

v. Where a client is permitted to utilize the business relationship prior to verification, CMOs shall adopt risk management procedures concerning the conditions under which this may occur. These procedures include a set of measures such as 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.

PART C

1. New Technologies and Non-Face-To-Face Transactions

In line with FATF's Recommendation 15, CMOs shall put in place:

a. Policies or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing and proliferation financing schemes such as internationally accepted Credit or Debit Cards and mobile phone banking and wire transfers.

b. Policies and procedures to address any specific risks associated with non -face to face business relationships or transactions. These policies and procedures shall be applied automatically when establishing clients relationships and conducting ongoing due diligence.

c. A ***CMO*** that relies upon a third party shall immediately obtain the necessary information concerning property which has been laundered or which constitutes proceeds from, instrumentalities used in and intended for use in the commission of money laundering, financing of terrorism and proliferation of financing or other predicate offences. Such CMO shall satisfy itself that copies of identification data and other relevant documentation

relating to the CDD requirements are made available by the third party upon request without delay.

d. The ***CMO shall*** be satisfied that the third party is a regulated institution with measures in place to comply with requirements of CDD. Accounts or transactions between CMOs for their clients shall perform some of the elements of the CDD process on the introduced business. The following criteria shall be met:

i. Immediately obtain from the third party the necessary information concerning certain elements of the CDD process;
ii. Take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available by the third party upon request without delay;
iii. Satisfy themselves that the third party is regulated in accordance with Core Principles of AML/CFT/PF and has measures in place to comply with the CDD requirements set out in this Manual; and
iv. Make sure that adequate KYC provisions are applied to the third party in order to get account information for competent authorities.

e. The ultimate responsibility for clients' identification and verification remains with the ***CMOs*** relying on the third party.

2. Maintenance of Records on Transactions

Section 30 of the SIA Act 929, section 8 of Act 874 and FATF's Recommendation 11, requires that CMOs shall;

a. Maintain all necessary records of transactions, both domestic and international, for at least seven years following completion of the transaction (or longer if requested by the ***SEC*** and FIC in specific cases). This requirement applies regardless of whether the account or business relationship is ongoing or has been terminated.

b. Maintain records of the identification data, account files and business correspondence for at least seven years following the termination of an account or business relationship (or longer if requested by the ***SEC*** and FIC in specific cases).
c. Ensure that all clients-transaction records and information are available on a timely basis to the ***SEC*** and FIC.

d. ***Some*** of the necessary components of transaction-records ***to be kept*** include clients' and beneficiary's names, addresses (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the type and amount of currency involved, the type and identifying number of any account involved in the transaction.

3. Compliance, Monitoring and Response to Suspicious Transactions

a. Section 30 of Act 874 and FATF's Recommendation 20 and 21 require that every CMO shall;

1. Have a written policy framework approved by the board that would guide and enable its staff to monitor, recognize and respond appropriately to suspicious transactions.
2. Designate an officer appropriately as the AML/CFT/PF Compliance Officer to supervise the monitoring and reporting of suspicious transactions.
3. Be alert to the various patterns of conduct that have been known to be suggestive of money laundering and maintain a checklist of such transactions which shall be disseminated to the relevant staff.
4. When any staff of a ***CMO*** detects any "red flag" or suspicious money laundering activity, the operator is required to promptly institute a "Review Panel" under the supervision of the AMLRO. Every action taken must be recorded. The operator and its staff shall maintain confidentiality in respect of such investigation and any suspicious transaction report that may be filed with the relevant authority.

5. This action is, however, in compliance with the provisions of the money laundering law that criminalizes "tipping off" (i.e. doing or saying anything that might tip off someone else that he is under suspicion of money laundering).

6. A ***CMO*** that suspects or has reason to suspect that funds are the Proceeds of a criminal activity or are related to terrorist financing shall report promptly its suspicions to the FIC. All suspicious transactions, including attempted transactions are to be reported regardless of the amount involved. This requirement applies regardless of whether the transactions involve tax crimes or other things.

7. ***CMOs,*** their directors, officers and employees (permanent and temporary) are prohibited from disclosing the fact that a report is required to be filed with the relevant authorities.

b. Internal controls, compliance and audit

i. ***CMOs shall*** establish and maintain internal procedures, policies and controls to prevent money laundering, financing of terrorism and proliferation financing and to communicate these to their employees.

These procedures, policies and controls ***shall*** cover the CDD, record retention, the detection of unusual and suspicious transactions, the reporting obligation, among other things.

ii. The AMLRO and appropriate staff shall have timely access to clients' identification data, CDD information, transaction records and other relevant information.

iii. ***CMOs shall*** develop programs against money laundering and terrorist financing which shall include:

a. The development of internal policies, procedures and controls, including appropriate compliance management arrangements and adequate screening procedures to ensure high standards when hiring employees;

b. An on-going employee training program to ensure that employees are kept informed of new developments, including information on current ML, FT and PF techniques, methods and trends; and that there is a clear explanation of all aspects of AML/CFT/PF laws and obligations, and in particular, requirements concerning CDD and suspicious transaction reporting; and

c. Adequately resourced and independent audit function to test compliance with the procedures, policies and controls.

d. The formation of control policy concerned with issues of timing, degree of control, areas to be controlled responsibilities and follow ups to combat ML and FT.

iv. **A *CMO shall*** also put in place a structure that ensures the operational independence of the AMLRO).

4. Suspicious Transactions "Red Flags"

Important suspicious transaction red flags include:

(a) **Potential Transactions Perceived or Identified as Suspicious**

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

ii. Transactions involving shell companies.

iii. Transactions with correspondents that have been identified as higher risk.

iv. Large transaction activity involving monetary instruments such as traveller's cheques, bank drafts, money order, particularly those that are serially numbered.

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

(b) **Terrorist Financing "Red Flags" occurs when:**

i. Persons involved in a transaction 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).

ii. Securities transaction by a non-profit or charitable organisation, 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 organisation and other parties in the transaction.

iii. Large ***volume of securities transactions through*** a business account, ***where*** there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves designated high-risk locations.

iv. The stated occupation of the clients is inconsistent with the type and level of account activity.

v. Multiple personal and business accounts or the accounts of non-profit organisations or charities ***that*** are used to collect and ***channel securities*** to a small number of foreign beneficiaries.

(c) **Other Unusual or Suspicious Activities**

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

ii. Employee ***failure*** to comply with approved operating guidelines.

iii. Employee is reluctant to take a vacation.

(d) **Other forms of reporting**

CMOs shall report all securities transactions in any currency above a threshold of $10, 000 (or its equivalent) for individual and $25,000(or its equivalent) for corporate person to the FIC.

5. AML/CFT/PF Employee-Education and Training Programme

Section 20 of Act 874 requires that:

a. ***CMOs shall*** design a comprehensive employee education and training program not only to make employees fully aware of their obligations but also to equip them with relevant skills required for the effective discharge of their AML/CFT/PF tasks.

b. The timing, coverage and content of the employee training program ***shall*** be tailored to meet the perceived needs of the ***CMOs***. ***CMOs shall*** render annual returns on their level of compliance to the ***SEC*** and FIC.

c. The employee training programs are required to be developed under the guidance of the AMLROs in collaboration with the top Management. The basic elements of the employee training program are expected to include:

i. AML Legislation and offences
ii. The nature of money laundering
iii. Money laundering 'red flags' and suspicious transactions, including trade-based money laundering typologies
iv. Reporting requirements
vi. Clients due diligence
vii. Risk-based approach to AML/CFT/PF
viii. Record keeping and retention policy.

d. ***CMOs shall*** submit their Annual AML/CFT/PF Employee training program to the SEC and FIC not later than the 31st of December every financial year against the next year.

6. Monitoring of Employee Conduct

CMOs shall monitor their employees' accounts for potential signs of money laundering. They are also required to subject employees' accounts to the same AML/CFT/PF procedures as applicable to other clients' accounts. This is required to be performed under the supervision of the AMLROs. The latter's own account is to be reviewed by the Internal Auditor or a person of adequate/similar seniority. Compliance reports including findings are to be rendered to the ***SEC*** /FIC.

Training shall form part of employees' appraisal.

7. Protection of Staff who Report Violations

a. ***CMOs shall*** direct their employees in writing to always co-operate fully with the Regulators and law enforcement agencies and to promptly report suspicious transactions to them. They are also required to make it possible for employees to report any violations of the institution's AML/CFT/PF compliance program to the AMLRO. Where the violations involve the AMLRO, employees are required to report such to a designated higher authority such as the Internal Auditor.

b. ***CMOs shall*** inform their employees in writing to make such reports confidential and that they will be protected from victimization for making them.

PART D

1. Additional Areas of AML/CFT/PF Risks

a. ***CMOs shall*** review, identify and record other areas of potential money laundering risks not covered by this Compliance Manual and report same quarterly to the SEC and FIC.

b. ***CMOs*** shall review their AML/CFT/PF frameworks from time to time with a view to determining their adequacy and identifying other areas of potential risks not covered by the AML/CFT/PF Compliance Manual.

2. Additional Procedures

Having reviewed the AML/CFT/PF framework and identified new areas of potential money laundering vulnerabilities and risks, ***CMOs shall*** design additional procedures as a contingency plan in their AML/CFT/PF Operational Manuals. These will provide how such potential risks will be appropriately managed if they crystallize. Details of the contingency plan are to be submitted to ***SEC*** and FIC by 31st December every financial year.

3. Terrorist Financing Offences

This extends to any person who wilfully provides or collects funds by any means, directly or indirectly, with the intention that they should 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 an individual terrorist.

a. Terrorist financing offences extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful 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.

b. Terrorist financing offences are extended to any funds whether from a legitimate or illegitimate source. Terrorist

financing offences therefore do not necessarily require that the funds are actually used to carry out or attempt a terrorist-act or be linked to a specific terrorist-act. Attempt to finance terrorist/terrorism and to engage in any of the types of conduct as set out above is also an offence.

c. Terrorist financing offences are predicate offences for money laundering and therefore apply, regardless of whether the person alleged to have committed the offence is in the same country or a different country from the one in which the terrorist/ terrorist organization is located or the terrorist act occurred or is expected to occur.

d. Terrorist financing offences extends to any funds whether from a legitimate or illegitimate source.

4. Acquisition of one Financial Institution by another

When a financial institution acquires a CMO, it is not necessary for the identity of all the existing customers to be re-identified and verified provided that those customer records are acquired with the business. CDD should be conducted to ensure that the acquired institution has fully complied with AML Legislation.

5. Receiving CMOS and Agents

CMOs who act as receivers or agents in respect of new issues of securities shall:

a. identify all applicants including applicants of a rights issue

b. identify and verify the identity of third parties who provide funds

c. Identify and verify of all beneficiary owners.

6. Culture of Compliance

CMO shall have a comprehensive AML/CFT/PF compliance program to guide its compliance efforts and to ensure the diligent implementation of its Manual. All staff shall be involved in the

implementation of the program and there shall be evidence of access to the program and training in it for all staff.

7. Financial Exclusion

Persons who are socially and financially disadvantaged should not be precluded from undertaking financial transactions or obtaining financial services especially due to their inability to show evidence to identify themselves. Internal procedures of CMOs shall make allowances for such persons on how to confirm and verify the identity of such persons. For example a CMO may accept a letter or statement from a person in a position of responsibility such as solicitors, doctors, ministers of religion and teachers who know the client, to confirm that the client is who he says he is. The document should include the contact information of the provider. All records of the reasons on this case should be maintained. Procedures on Financial Inclusion should be contained in the CMOs compliance program.

8. Important AML Documentation

The following documents and information shall be reviewed as part of any SEC's AML/CFT supervisory oversight and inspection process:

- AML/CFT program
- Risk assessment framework and report
- New account opening and KYC related documents;
- Documents evidencing proof of client identity verification
- Risk categorization of clients
- Suspicious Transaction Reports (STRs), and underlying investigatory working papers;
- All documents reflecting investigation of possible suspicious transactions that did not result in the filling of a STRs;
- All documents relating to the CMO's independent AML/CFT testing program including, but not limited to, the latest testing reports, the scope and methodology of testing

performed, underlying test work papers, and related AMLRO reviews, memoranda and correspondence;

- Board of Directors and/or Internal Audit Committee documents reflecting discussions of any aspect of the CMO's AML/CFT program, including, but not limited to: (i) meeting minutes; (ii) CMO independent AML/CFT testing reports; (iii) decisions to file or not file STRs with the FIC, etc.;
- All AMLRO documents relating to the execution of the CMO's AML/CFT program;
- Wire and other transfers;
- Client and CMO proprietary account statements;
- List of training topics, dates of training, dates AML training was given, the nature of the training, the names of the staff who received training, list of attendees and the results of the test undertaken by staff, where appropriate;
- Verification of employees receiving written copies of the firm's AML procedures.
- Financial statements, budgets
- Operational reports

9. Sanctions

Section 206 of the SIA, Act 929, imposes a penalty on CMOs for non-compliance. Furthermore, Act 874 imposes sanctions for breach of AML Legislation which is in line with FATF Recommendation 35.

a. In addition to the regulatory sanctions that may be imposed by the Commission, particulars of the breaches of these Guidelines by financial institutions or individual(s) shall be referred to the appropriate law enforcement agency for further action.

b. For the purpose of emphasis, financial institutions are particularly reminded to take note of the following:

Section 39 of Act 749, amended by section 18 of Act 874

Section 42 of Act 749

Section 43 of Act 749
Section 44 of Act 749
Section 50(2) of Act 749
Regulation 44 of L.I.1987:

c. Refer to SEC/FIC administrative sanctions list issued on……for further guidance on ML sanctions.