BANK OF GHANA
AND
FINANCIAL INTELLIGENCE CENTRE

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

FOR BANKS AND NON-BANK FINANCIAL INSTITUTIONS IN GHANA

JULY, 2018

Contents

FOREWORD vii

LIST OF ACRONYMS & ABBREVIATION viii

INTRODUCTION ix

PURPOSE AND OVERVIEW OF THE GUIDELINE ix

THE OBJECTIVE x

1.0 PART A 1

AML/CFT& P DIRECTIVES 1

GENERAL GUIDELINES ON INSTITUTIONAL POLICY 1

ASSESSING AML/CFT RISK AND APPLYING A RISK –BASED APPROACH 1

APPOINTMENT OF ANTI – MONEY LAUNDERING REPORTING OFFICER AND DUTIES 2

COOPERATION WITH COMPETENT AUTHORITIES 3

1.1 SCOPE OF UNLAWFUL ACTIVITIES 3

1.2 MEASURES TO BE TAKEN AGAINST ML/TF 4

1.3 CUSTOMER DUE DILIGENCE (CDD) 5

1.4 CONDUCTING CDD 5

1.5 CDD PROCEDURES 5

1.6 HIGHER-RISK CATEGORIES OF CUSTOMERS 7

1.7 LOWER RISK CUSTOMERS, TRANSACTIONS OR PRODUCTS 8

1.8 TIMING OF VERIFICATION 9

1.9 FAILURE TO COMPLETE CDD 10

1.10 EXISTING CUSTOMERS 11

1.11 POLITICALLY EXPOSED PERSONS (PEPs) 11

1.12 CROSS-BORDER CORRESPONDENT BANKING 13

1.13 NEW TECHNOLOGIES AND NON-FACE-TO-FACE TRANSACTIONS 14

1.14 RELIANCE ON INTERMEDIARIES AND THIRD PARTIES ON CDD FUNCTION 14
1.15 MAINTENANCE OF RECORDS ON TRANSACTIONS 16
1.16 ATTENTION ON COMPLEX AND UNUSUAL LARGE TRANSACTIONS 16
1.17 SUSPICIOUS TRANSACTIONS, COMPLIANCE MONITORING AND RESPONSE TO SUSPICIOUS TRANSACTIONS 17
1.18 INTERNAL CONTROLS, COMPLIANCE AND AUDIT 18
1.19 OTHER MEASURES 19
1.20 SANCTIONS 19
1.21 SHELL BANKS 20
1.22 OTHER FORMS OF REPORTING 20
1.23 ATTENTION TO HIGHER RISK COUNTRIES 20
1.24 FOREIGN BRANCHES AND SUBSIDIARIES 21
1.25 AML/CFT EMPLOYEE-EDUCATION AND TRAINING PROGRAMME 22
1.26 MONITORING OF EMPLOYEE CONDUCT 23
1.27 PROTECTION OF STAFF WHO REPORT VIOLATIONS 24
1.28 ADDITIONAL PROCEDURES AND MITIGANTS 24
1.29 RISK ASSESSMENT FOR NEW PRODUCTS 24
1.30 TESTING FOR THE ADEQUACY OF THE AML/CFT COMPLIANCE PROGRAMME 25
1.31 FORMAL BOARD APPROVAL OF THE AML/CFT COMPLIANCE MANUAL 25
1.32 CULTURE OF COMPLIANCE 25
1.33 TERRORIST FINANCING&FINANCING OF PROLIFERATION 25
1.34 MONEY OR VALUE TRANSFER (MVT) SERVICES 26
1.35 WIRE TRANSFERS 27
2.0 Part B 30
KNOW YOUR CUSTOMER (KYC) PROCEDURES 30
2.1 DUTY TO OBTAIN IDENTIFICATION EVIDENCE 30

2.2 NATURE AND LEVEL OF THE BUSINESS 31
2.3 APPLY COMMERCIAL JUDGEMENT 31
2.4 ESTABLISHMENT OF IDENTITY 32
2.5 WHAT IS IDENTITY 32
2.6 WHEN MUST IDENTITY BE VERIFIED 32
2.7 REDEMPTIONS/SURRENDERS 33
2.8 WHOSE IDENTITY MUST BE VERIFIED 33
2.9 SAVINGS SCHEMES AND INVESTMENTS IN THIRD PARTIES' NAMES 35
2.10 PERSONAL PENSION SCHEMES 35
2.11 TIMING OF IDENTIFICATION REQUIREMENTS 35
2.12 CANCELLATION & COOLING-OFF RIGHTS 36
2.13 IDENTIFICATION PROCEDURES 37
2.14 GENRAL PRINCIPLES 37
2.15 NEW BUSINESS FOR EXISTING CUSTOMERS 38
2.16 CERTIFICATION OF IDENTIFICATION DOCUMENTS 38
2.17 RECORDING IDENTIFICATION EVIDENCE 39
2.18 CONCESSION IN RESPECT OF PAYMENT MADE BY POST 40
2.19 TERM DEPOSIT ACCOUNT (TDA) AND INDIVIDUAL SAVINGS ACCOUNTS (ISA) 41
2.20 INVESTMENT FUNDS 42
2.21 ESTABLISHING IDENTITY 42
2.22 PRIVATE INDIVIDUALS 42
2.23 PRIVATE INDIVIDUALS RESIDENT IN GHANA 43
2.24 DOCUMENTING EVIDENCE OF IDENTITY 43
2.25 PERSONAL IDENTITY DOCUMENTS 44
2.26 DOCUMENTARY EVIDENCE OF ADDRESS 44
2.27 PHYSICAL CHECKS ON PRIVATE INDIVIDUALS RESIDENT IN GHANA 45

2.28 ELECTRONIC CHECKS 45
2.29 PRIVATE INDIVIDUALS NOT RESIDENT IN GHANA 46
2.30 PRIVATE INDIVIDUALS NOT RESIDENT IN GHANA: SUPPLY OF INFORMATION 47
2.31 NON FACE-TO-FACE IDENTIFICATION 48
2.32 ESTABLISHING IDENTITY FOR REFUGEES AND ASYLUM SEEKERS 49
2.33 ESTABLISHING IDENTITY FOR STUDENTS AND MINORS 50
2.34 QUASI CORPORATE CUSTOMERS 50
2.35 EXECUTORSHIP ACCOUNTS 54
2.36 CORPORATE CUSTOMERS 56
2.37 HIGHER RISK BUSINESS 59
2.38 OTHER INSTITUTIONS 61
2.39 CHARITIES IN GHANA 62
2.40 REGISTERED CHARITIES 63
2.41 RELIGIOUS ORGANIZATIONS (ROs) 63
2.42 MINISTRIES, DEPARTMENTS AND AGENCIES MDAs) AND OTHER PUBLIC INSTITUTIONS 64
2.43 FOREIGN CONSULATES 64
2.44 INTERMEDIARIES OR OTHER THIRD PARTIES TO VERIFY IDENTITY OR TO INTRODUCE BUSINESS 64
2.45 ACQUISITION OF ONE FINANCIAL INSTITUTION/ BUSINESS BY ANOTHER 69
2.46 RECEIVING FINANCIAL INSTITUTIONS AND AGENTS 70
2.47 APPLICATIONS RECEIVED THROUGH BROKERS 70
2.48 APPLICATIONS RECEIVED FROM FOREIGN BROKERS 71
2.49 MULTIPLE FAMILY APPLICATIONS 71
2.50 LINKED TRANSACTIONS 72
2.51 DOMICILIARY ACCOUNT (DA) 72
2.52 PROVISION OF SAFE CUSTODY AND SAFE DEPOSIT BOXES 73

2.53 EXEMPTION FROM IDENTIFICATION PROCEDURES 73
2.54 FINANCIAL INCLUSION 74
2.55 SANCTIONS FOR NON-COMPLIANCE WITH KYC 75
APPENDIX A 75
INFORMATION TO ESTABLISH IDENTITY 76
APPENDIX B 82
DEFINITION OF TERMS 82
APPENDIX C 95
MONEY LAUNDERING AND TERRORIST FINANCING "RED FLAGS" 95
APPENDIX D 102
Further Guidance on Accountable Institutions' Risk Assessment and Business/Customer Risk Rating 102
APPENDIX E 105
GUIDANCE ON ENHANCED DUE DILIGENCE 105

FOREWORD

The world has experienced phenomenal growth of financial services over the last couple of decades. This globalization has led to increased cross-border activities enhancing global financial intermediation. Unfortunately, this development has been accompanied by a spate of transnational organized crime including Money Laundering and Terrorist Financing (ML/TF) perpetuated by underground economies.

Money Laundering and Terrorist Financing affect whole economies, and therefore impact negatively on the economic, political and social development, posing serious challenges to all countries.

The need for countries to have strong anti-money laundering mechanisms, coupled with the enhancement of transparent financial integrity cannot therefore be over-emphasized. Ghana is determined to maintain a sound financial system and to join global efforts to minimize the scourge of Money Laundering and Terrorist Financing.

In pursuit of the above goal and in order to avoid the risk of under-regulation, the Financial Intelligence Centre (FIC) and the Bank of Ghana (BOG) is providing this Guideline to assist licensed banks and non-bank financial institutions design and implement their respective AML/CFT compliance programmes.

This Guideline is issued consistent with the Banks & Specialized Deposit Taking Institutions, Act 2016, (Act 930),and Anti-Money Laundering Act, 2008 (Act 749) as Amended.

GOVERNOR
BANK OF GHANA

CHIEF EXECUTIVE OFFICER
FINANCIAL INTELLIGENCE CENTRE

LIST OF ACRONYMS & ABBREVIATION

AI	-	Accountable Institution
AML	-	Anti-Money Laundering
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
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 Organisation
NIC	-	National Insurance Commission
PEP	-	Politically Exposed Person
RO	-	Religious Organisation
SEC	-	Securities & Exchange Commission
STR	-	Suspicious Transaction Report
TF	-	Terrorist Financing

INTRODUCTION

Following the enactment of the Anti-Money Laundering Act, 2008 (Act 749), the Anti-Terrorism Act, 2008 (Act 762) and the subsequent passage of the Anti-Money Laundering Regulations, 2011 (L.I.1987), Ghana has intensified its efforts towards the fight against money laundering and terrorist financing. The benefit of the Anti-Money Laundering Act will not be realized unless there is effective implementation of the collaborative measures being adopted by the Bank of Ghana (BOG) and the Financial Intelligence Centre (FIC) as well as compliance by licensed financial institutions. It is against this background that the BOG and FIC in accordance with section 6(d) of Act 749 and Regulation 38 of L.I.1987 developed the Guideline for financial institutions licensed by the Bank of Ghana.

The Guideline has incorporated essential elements of the AML Act and Regulations, relevant FATF-Recommendations, the sound practices of the Basle Committee on Banking Supervision and other international best practices on Anti-Money Laundering and the Combating of the Financing of Terrorism (AML/CFT).

To provide a further guide and to avoid ambiguity, the Guideline on KYC is also provided to assist financial institutions in their implementation of the Guideline.

PURPOSE AND OVERVIEW OF THE GUIDELINE

Money laundering (ML) has been defined as the process whereby criminals attempt to conceal the illegal origin and/or illegitimate ownership of property and assets that are the fruits or proceeds of their criminal activities. It is, thus, a derivative crime. Financing of Terrorism (FT) is defined here to include both legitimate and illegitimate money characterized by concealment of the origin or intended criminal use of the funds.

Money laundering and terrorist financing are global phenomena and there has been growing recognition in recent times, and indeed well-documented evidence, that both money laundering and terrorist financing pose major threats to international peace and security which could seriously undermine Ghana's development and progress.

Consequently, concerted global efforts have been made to check these crimes. Financial Institutions, in particular, have come under sustained regulatory pressure to improve their monitoring and surveillance systems with a view to preventing, detecting and responding effectively to the threat of money laundering and terrorist financing.

The Guideline covers among others the following key areas of AML/CFT policy: Reporting Officer designation and duties; the need to co-operate with the supervisory authority; customer due diligence; monitoring and responding to suspicious transactions; reporting requirements; record keeping; and AML/CFT employee training program.

Financial institutions are exposed to varying money laundering risks and serious financial and reputational damage if they fail to manage these risks adequately. Diligent implementation of the provisions of this Guideline would not only minimize the risk faced by licensed financial institutions of being used to launder the proceeds of crime but also provide protection against fraud and reputational and financial risks. In this connection, the affected institutions are directed to adopt a risk-based approach in the identification and management of their AML/CFT risks.

Ghanaian financial institutions are also reminded that AML/CFT laws in all the jurisdictions in which they operate should not only designate money laundering and predicate offences but should also prescribe sanctions for non-compliance with the relevant laws and regulations on customer due diligence, non-rendition of prescribed reports and not keeping of appropriate records. It is, therefore, in the best interest the accountable institutions to entrench a culture of compliance which would be facilitated by the Guideline.

The Guideline is structured in two, Part A made up of the new AML/CFT Directives while Part B provides guidance on KYC.

THE OBJECTIVE

The AML/CFT Guideline:

(a) is formulated in accordance with the provisions of the Anti-Money Laundering Act, 2008(Act 749) as amended, and Anti-Terrorism Act 2008, (Act 762) as amended, other relevant laws and the FATF Revised Recommendations. The Guideline is also intended to ensure that all accountable institutions (reporting entities) understand and comply with the requirements of the law and obligations imposed on them.

(b) mandates the Bank of Ghana and Financial Intelligence Centre to effectively enforce AML/CFT requirements and ensure compliance by AIs.

(c) provides guidance on KYC measure to assist ALs in the implementation of the Guideline

1.0 PART A

AML/CFT& P DIRECTIVES

AML/CFT INSTITUTIONAL POLICY FRAMEWORK

GENERAL GUIDELINES ON INSTITUTIONAL POLICY

Every financial institution licensed by Bank of Ghana shall adopt policies indicating its commitment to comply with AML/CFT & P obligations under the relevant Acts and regulations to prevent any transaction that facilitates ML/TF activities.

Every financial institution shall formulate and implement internal rules, procedures and other controls that will deter criminals from using its facilities for money laundering and terrorist financing and shall ensure that its obligations under the relevant laws and regulations are always met.

ASSESSING AML/CFT RISK AND APPLYING A RISK –BASED APPROACH

The reporting institutions' AML/CFT risk management function must be aligned and integrated with their overall risk management control function. Accountable institutions licensed by Bank of Ghana are required to take appropriate steps to identify, assess and understand their ML/TF risks in relation to their customers, countries or geographical areas, products and services, transactions or delivery channels in a form of a framework to guide the staff in the organization.

In assessing ML/TF risks, Accountable Institutions are required to have the following processes in place:

(a) Document their risk assessments and findings in the form of a framework;

(b) Consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

(c) Keep the assessment up-to-date through a periodic review; and

(d) Provide periodic risk assessment information to BOG and FIC any time there is a review.

Accountable Institutions are required to conduct additional risk assessment as and when required by the BOG.

Accountable Institutions shall be guided by the results of National Risk Assessment Reports in conducting their respective risk assessments.

Accountable Institutions shall provide timely reporting of the AML/CFT risk assessment, ML/TF risk profile and the effectiveness of risk control and mitigation measures to their respective Boards of Directors. The frequency of reporting shall be determined by their Boards.

Further Guidance on AIs Risk Assessment and Business/Customer Risk Rating is provided in Appendix D

APPOINTMENT OF ANTI – MONEY LAUNDERING REPORTING OFFICER AND DUTIES

Each financial institution shall appoint a responsible official as an Anti-Money Laundering Reporting Officer (AMLRO) who shall be a key management personnel of the accountable institution and who will operationally report to the Board in accordance with section 41(1)(b) of the Anti-Money Laundering Act, 2008 (Act 749) as amended and Regulation 5(1) of L.I. 1987.

The duties of the AML Reporting Officer shall include but not limited to the following:

i. Develop an AML/CFT Compliance Programme;
ii. Receive and vet suspicious (unusual) transaction reports from the staff;
iii. File suspicious and cash transaction reports with the FIC;
iv. Ensure that the financial institution's compliance programme is implemented;
v. Coordinate the training of the staff in AML/CFT awareness, detection methods and reporting requirements; and
vi. Serve both as a liaison officer with the BOG and the FIC and a point-of-contact for all employees on issues relating to money laundering and financing terrorism & proliferation.

Each anti-money laundering reporting officer shall be equipped with the relevant competence, authority and independence to implement the institution's AML/CFT

compliance programme. He or she should be encouraged by the institution to acquire professional qualification in anti-money laundering and financial crime.

Every financial institution shall ensure that the AMLRO has access to other information that may be of assistance to him/her in consideration of a suspicious or unusual transaction report.

COOPERATION WITH COMPETENT AUTHORITIES

Each financial institution shall declare its commitment to comply promptly with all requests made pursuant to the law and regulations and provide information to the BOG, FIC and other relevant competent authorities.

Each financial institution's procedures for responding to authorized requests for information on money laundering and terrorist financing shall meet the following requirements such that it shall be able to:

i. search immediately the institution's records to determine whether it maintains or has maintained any account for or has engaged in any transaction with each individual, entity, or organization named in the request;

ii. report promptly to the requesting authority the outcome of the search; and

iii. protect the security and confidentiality of such requests.

1.1 SCOPE OF UNLAWFUL ACTIVITIES

(a) Financial institutions shall identify and report to the BOG and the FIC, the proceeds of crime derived from unlawful activities including but not limited to the following:

i. Participation in an organized criminal group and racketeering;

ii. Terrorism, including terrorist financing;

iii. Trafficking in human beings and migrant smuggling;

iv. Sexual exploitation, including sexual exploitation of children;

v. Illicit trafficking in narcotic drugs and psychotropic substances;

vi. Illicit arms trafficking;

vii. Illicit trafficking in stolen and other goods;

viii. Corruption and bribery;

ix. Fraud;

x. Counterfeiting currency;

xi. Counterfeiting and piracy of products;

xii. Environmental crime;

xiii. Murder, grievous bodily injury;

xiv. Kidnapping, illegal restraint and hostage-taking;

xv. Robbery or theft;

xvi. Smuggling;

xvii. Tax Evasion;

xviii. Extortion;

xix. Forgery;

xx. Piracy; and

xxi. Insider trading and market manipulation.

xxii. Any other predicate offence under the Anti-Money Laundering Act, 2008 Act 749 as amended and Anti-Terrorism Act 2008, Act 762 as amended.

1.2 MEASURES TO BE TAKEN AGAINST ML/TF

Notwithstanding an accountable institution's internal policies relating to customer confidentiality and particularly in accordance with the provisions in the Banks and SDI Act, 2016 (Act 930), Non-Deposit Taking Institutions Act 2008 (Act 774) and the AML Act, 2008 (Act 749) as amended, competent authorities shall have access to information in order to perform their functions in combating money laundering and financing of terrorism; the sharing of information between competent authorities, either domestically or internationally; and the sharing of information between financial institutions, where this is required or necessary.

1.3 CUSTOMER DUE DILIGENCE (CDD)

CDD is the identification and verification of both the client and beneficiary including but not limited to continuous monitoring of the business relationship with the financial institution. Financial institutions are not permitted to operate anonymous accounts or accounts in fictitious names.

1.4 CONDUCTING CDD

Financial institutions shall undertake customer due diligence (CDD) measures when:

(a) business relationships are established;

(b) carrying out occasional transactions. This may include transactions carried out in a single operation or several operations that appear to be linked. It may also involve carrying out occasional transactions such as money transfers, including those applicable to cross-border and domestic transfers between financial institutions by means of credit or debit cards to effect the transaction. The following transactions are however, exempted:

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

ii. Financial institution-to-financial institution transfers and settlements where both the originator-person and the beneficial-person are financial institutions acting on their own behalf.

(c) There is a suspicion of money laundering or terrorist financing, regardless of any exemptions or any other thresholds referred to in the Guideline; or

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

1.5 CDD PROCEDURES

(a) Financial institutions shall identify their customers (whether permanent or occasional; natural or legal persons; or legal arrangements) and verify the customers' identities using reliable, independently sourced documents, data or

information. All financial institutions are required to carry out the full range of the CDD procedures in the Guideline. However, in reasonable circumstances, financial institutions can apply the CDD procedures on a risk-based approach.

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

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

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

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

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

(d) Financial institutions shall in respect of all customers determine whether or not a customer is acting on behalf of another person. Where the customer or any other third party is acting on behalf of another person or making deposits and withdrawals, the financial institution shall take reasonable steps to obtain sufficient identification data and to verify the identity of that other person as pertains in (a) above.

(e) Financial institutions shall take reasonable measures in respect of customers that are legal persons or legal arrangements to:

i. understand the ownership and control structure of such a customer; and

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

The natural persons include those persons who exercise ultimate and effective control over the legal person or arrangement. Examples of types of measures needed to satisfactorily perform this function include:

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

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

Where the customer 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 stock exchange) it is not necessary to identify and verify the identity of the shareholders of such a public company.

(f) Financial institutions shall obtain information on the purpose and intended nature of the business relationship of their potential customers.

(g) Financial institutions shall conduct ongoing due diligence on the business relationship as stated by the customers above.

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

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

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

1.6 HIGHER-RISK CATEGORIES OF CUSTOMERS

(a) Accountable institutions shall perform enhanced due diligence for higher-risk categories of customers, business relationship or transaction. Financial institutions are to adopt CDD procedures on a risk sensitive-basis.

Accountable institutions are required to determine in each case whether the risks are lower or not, having regard to the type of customer, product, transaction or the

location of the customer. Where there is doubt, financial institutions are directed to seek clearance from the Bank of Ghana.

Examples of higher-risk customer categories include:

i. Non-resident customers;

ii. Private banking customers;

iii. Legal persons or legal arrangements such as trusts that are personal-assets holding vehicles;

iv. Companies that have nominee-shareholders or shares in bearer form; and

v. Politically exposed persons (PEPs)

vi. Cross-border banking and business relationships,

vii. Designated Non-Financial Businesses and Professions, and

viii. Any customer deemed high risk by the AI.

1.7 LOWER RISK CUSTOMERS, TRANSACTIONS OR PRODUCTS

These include:

(a) Financial institutions – provided they are subject to requirements for the combat of money laundering and financing of terrorism & proliferation which are consistent with the provisions of this Guideline and are supervised for compliance with them;

(b) Public companies (listed on a stock exchange) that are subject to regulatory disclosure requirements;

(c) Ministries, Department and Agencies (MDAs) and other public institutions;

(d) Life insurance policies where the annual premium and single monthly premium are within the threshold determined by National Insurance Commission (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 money laundering and the financing of terrorism & proliferation of weapons of mass destruction consistent with the provisions of Anti-Money Laundering Act as amended.

Financial institutions that apply simplified or reduced CDD procedures to customers resident abroad are required to limit such to customers in countries that have effectively implemented the FATF Recommendations.

Simplified CDD procedures are not acceptable and therefore cannot apply to a customer whenever there is suspicion of money laundering or financing terrorism & proliferation or specific higher-risk scenarios. In such a circumstance, enhanced due diligence is mandatory.

Where there are low risks, financial institutions shall apply reduced or simplified measures. There are low risks in circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available or where adequate checks and controls exist elsewhere in other public institutions. In circumstances of low-risk, financial institutions shall apply the simplified or reduced CDD procedures when identifying and verifying the identity of their customers and the beneficial owners.

AIs shall prepare an internal risk assessment framework to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

1.8 TIMING OF VERIFICATION

(a) Financial institutions shall verify the identity of the customer, beneficial-owner and occasional customers before or during the course of establishing a business relationship or conducting transactions for them.

(b) Financial institutions are permitted to complete the verification of the identity of the customer and beneficial owner following the establishment of the business relationship, only when:

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

ii. it is essential not to interrupt the normal business conduct of the customer; and the money laundering risks can be effectively managed.

(c) Examples of situations where it may be essential not to interrupt the normal conduct of business are:

i. Non face-to-face business

ii. 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 customer is contacting them and the performance of the transaction may be required before verification of identity is completed.

Life insurance business in relation to identification and verification of the beneficiary under the policy. This may take place after the business relationship with the policyholder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

(d) Where a customer is permitted to utilize the business relationship prior to verification, financial institutions are required to 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 and have no apparent or visible economic or lawful purpose.

1.9 FAILURE TO COMPLETE CDD

(a) The financial institution which does not comply with item 1.4 above:

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

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

(b) The financial institution that has already commenced the business relationship (eg items 1.3 - 1.7 above) shall terminate the business relationship and submit a Suspicious Transaction Report (STR) to the Financial Intelligence Centre (FIC) within twenty four hours.

1.10 EXISTING CUSTOMERS

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

(b) The appropriate time to conduct CDD by financial institutions is when:

i. a transaction of significant value takes place,

ii. customer documentation standards change substantially,

iii. there is a material change in the way that the account is operated, and

iv. the institution becomes aware that it lacks sufficient information about an existing customer.

The financial institution shall properly identify the customer in accordance with these criteria. The customer identification records should be made available to the AML/CFT Reporting Officer, other appropriate staff and competent authorities.

1.11 POLITICALLY EXPOSED PERSONS (PEPs)

(a) PEPs are individuals who are or have been entrusted with prominent public functions both in Ghana or in foreign countries and people or entities associated with them. PEPs also include person who are or have been trusted with a prominent functions by international organization.

Examples of PEPs include, but are not limited to;

i. Heads of State or government;

ii. Ministers of State;

iii. Politicians;

iv. High ranking political party officials; and

v. An artificial politically exposed person (an unnatural legal entity. belonging to a PEP);

vi. Senior public officials;

vii. Senior Judicial officials

viii. Senior military officials;

ix. Chief executives of state owned companies/corporations;

x. Family members or close associates of PEPs.

xi. Traditional Rulers

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

(c) Financial institutions shall obtain senior management approval before they establish a business relationship with PEP.

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

(e) Financial institutions shall take reasonable measures to establish the source of wealth and the sources of funds of customers and beneficial-owners identified as PEPs and report all anomalies immediately to the FIC and other relevant authorities.

(f) Financial institutions in business relationships with PEPs are required to conduct enhanced ongoing monitoring of that relationship. In the event of any transaction that is abnormal, financial institutions are required to flag the account and to report immediately to the FIC and other relevant authorities.

1.12 CROSS-BORDER CORRESPONDENT BANKING

Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Large international banks typically act as correspondents for several other banks around the world.

Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international transfers of funds, cheque clearing, payable-through-accounts and foreign exchange services.

(a) In relation to cross-border and correspondent banking and other similar relationships, financial institutions shall, in addition to performing the normal CDD procedures, take the following measures:

i. Gather sufficient information about a respondent institution to understand fully the nature of its business; and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether or not it has been subject to a money laundering or terrorist financing investigation or regulatory action.

ii. Assess the respondent institution‘s AML/CFT controls and ascertain that the latter are in compliance with FATF standards.

iii. Obtain approval from senior management before establishing correspondent relationships.

iv. Document the respective AML/CFT responsibilities of such institution.

(b) Where a correspondent relationship involves the maintenance of payable through-accounts, the financial institution should be satisfied that:

i. its customer (the respondent bank or financial institution) has performed the normal CDD obligations on its customers that have direct access to the accounts of the correspondent financial institution; and

ii. the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.

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

(a) Financial institutions shall have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes such as internationally accepted credit or debit cards and mobile telephone banking.

(b) Financial institutions shall have policies and procedures in place 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 customer relationships and conducting ongoing due diligence. Measures for managing the risks should include specific and effective CDD procedures that apply to non-face to face customers.

(c) The Financial Institution should satisfy itself that the third party is a regulated and supervised institution and has measures in place to comply with requirements of CDD and reliance on intermediaries and other third parties on CDD as contained in the Guideline.

(d) A financial institution that relies on a third party should immediately obtain the necessary information concerning property which has been laundered or which constitutes proceeds of, or means used to or intended for use in the commission of money laundering and financing of terrorist or any other unlawful act. Such financial institution should satisfy itself that copies of identification data and other relevant documentation relating the CDD requirements will be made available from the third party upon request without delay.

1.14 RELIANCE ON INTERMEDIARIES AND THIRD PARTIES ON CDD FUNCTION

(a) Financial institutions relying on intermediaries or other third parties which have no outsourcing or agency relationships, business relationships, accounts or transactions between financial institutions for their clients are required to perform some of the elements of the CDD process on the introduced business. The following criteria should also 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 from the third party upon request without delay;

iii. Satisfy themselves that the third party is regulated and supervised in accordance with Core Principles of AML/CFT and has measures in place to comply with the CDD and Record Keeping requirements set out in the Guideline;

iv. When determining in which countries the third party that meets the conditions are based, the Accountable Institution (AI) should have regard to information available on the level of country risk; and

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

(b) For financial institutions that rely on a third party that is part of the same financial group, relevant competent authorities may also consider that the requirements of the criteria above are met in the following circumstances:

i. the group applies CDD and record-keeping requirements, in line with Recommendations 10 to 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18;

ii. the implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority; and

iii. any higher country risk is adequately mitigated by the group's AML/CFT policies.

(c) The ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

1.15 MAINTENANCE OF RECORDS ON TRANSACTIONS

(a) Financial institutions are required to maintain all necessary records of transactions, both domestic and international, for at least five (5) years following completion of the transaction (or longer if requested by the BOG and FIC in specific cases). This requirement applies regardless of whether the account or business relationship is ongoing or has been terminated.

(b) Examples of the necessary components of transaction-records include customer's 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 identification number of any account involved in the transaction.

(c) Financial institutions shall maintain records of the identification data, account files and business correspondence for at least five (5) years following the termination of an account or business relationship (or longer if requested by the BOG and FIC in specific cases).

(d) Financial institutions shall ensure that all customer-transaction records and information are available on a timely basis to the BOG and FIC.

1.16 COMPLEX AND UNUSUAL LARGE TRANSACTIONS

(a) Financial institutions shall pay special attention to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. Examples of such transactions or patterns of transactions include significant transactions relative to a relationship, transactions that exceed prescribed limits, very high account turnover inconsistent with the size of the balance or transactions which fall out of the regular pattern of the account's activity.

(b) Financial institutions are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing. They are required to report such findings to the FIC within 24 hours; and keep them available for BOG, FIC, other competent authorities and auditors for at least five (5) years.

1.17 SUSPICIOUS TRANSACTIONS, COMPLIANCE MONITORING AND RESPONSE TO SUSPICIOUS TRANSACTIONS

Definition of a Suspicious Transaction

(a) For the purpose of the Guideline, 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 customer's known legitimate business or personal activities or normal business for that type of account or that the transaction lacks an obvious economic rationale.

Institutional Policy

(b) Every financial institution shall have a written policy framework that would guide and enable its staff to monitor, recognize and respond appropriately to suspicious transactions. A list of Money Laundering "Red Flags" is provided in Appendix C to the Guideline**.**

(c) Every accountable institution shall designate an officer appropriately as the AML/CFT Reporting Officer to; inter alia supervise the monitoring and reporting of suspicious transactions.

(d) Every accountable institution should be alert to the various patterns of conduct that have been known to be suggestive of money laundering and maintain a check list of such transactions which should be disseminated to the relevant staff.

(e) When any staff of a financial institution detects any "red flag" or suspicious money laundering activity, the staff is required to promptly report to the AML/CFT Reporting Officer. Every action taken shall be recorded. The institution and its staff shall maintain confidentiality in respect of such investigation and any suspicious transaction report that may be filed with the competent authority. This action is, however, in compliance with the provisions of the Anti-Money Laundering Act which criminalize "tipping off" (i.e. doing or saying anything that might alert or give information to someone else that he is under suspicion of money laundering).

(f) A financial institution that suspects or has reason to suspect that funds or the proceeds of unlawful activity or are related to terrorist financing, shall report within 24 hours, its suspicions to the FIC. All suspicious transactions, including attempted transactions are to be reported regardless of the amount involved. This requirement to report suspicious transactions should apply regardless of whether they are thought, among other things, to involve tax matters.

(g) Financial institutions, their directors and employees (permanent and temporary) are prohibited from disclosing the fact that a report is required to be filed or has been filed with the competent authorities.

1.18 INTERNAL CONTROLS, COMPLIANCE AND AUDIT

(a) Financial institutions shall establish and maintain internal procedures, policies and controls to prevent money laundering and financing of terrorism and to communicate these to their employees. These procedures, policies and controls should cover the CDD, record retention, the detection of unusual and suspicious transactions, the reporting obligation, among other things.

(b) The AML/CFT Reporting Officer and appropriate staff are to have timely access to customer identification data, CDD information, transaction records and other relevant information.

(c) Accountable institutions are therefore required to develop programs against money laundering and terrorist financing to include:

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

ii. Ongoing employee training programs to ensure that employees are kept informed of new developments, including:

a. Information on current ML and FT techniques, methods and trends;

b. Clear explanation of all aspects of AML/CFT laws and obligations, and,

c. Requirements concerning CDD and suspicious transaction reporting.

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

Accountable Institutions shall put in place a structure that ensures the operational independence of the AML/CFT Reporting Officer.

1.19 OTHER MEASURES

These measures are meant to deter money laundering and financing of terrorism & proliferation.

They include measures on sanctions, shell banks, other forms of reporting, special attention for higher-risk countries and foreign branches and subsidiaries of Ghanaian financial institutions.

1.20 SANCTIONS

(a) In addition to the regulatory sanctions that may be imposed by BOG as indicated in section 92 (8) and (9) of the Banks and SDI Act 2016, Act 930, particulars of the breaches of the Guideline by accountable institutions or individual(s) shall be referred to the appropriate law enforcement agency for further action.

(b) For the purpose of emphasis, accountable institutions are particularly reminded to take note of the following:

Section 39 of Act 749 as amended.

Section 42 of Act 749 as amended

Section 43 of Act 749 as amended

Section 44 of Act 749 as amended

Section 50(2) of Act 749 as amended

Regulation 44 of L.I.1987

Section 92 (8) of Banks and Specialized Deposit- taking institution Act 2016, (Act 930)

(c) An accountable institution shall preserve the funds, other assets and instrumentalities of crime for a period of one year or as may be determined by Bank of Ghana to facilitate investigations.

1.21 SHELL BANKS

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

(b) Financial institutions shall take all necessary measures to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

1.22 OTHER FORMS OF REPORTING

Financial institutions shall report to the FIC all cash transactions within Ghana in any currency and with a threshold of GHS50, 000.00 for banks GHS20,000.00 for specialized deposit-taking institutions (or its foreign currency equivalent) and Electronic Transactions with a threshold of $1,000.00 or its equivalent for both individuals and business entities or amounts as may be determined by the FIC from time to time.

1.23 HIGHER RISK COUNTRIES

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

(b) Accountable institutions shall report, as stated below, transactions that have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined and written findings made available to assist competent authorities such as BOG, FIC, auditors and law enforcement agencies (LEAs) to carry out their duties.

Accountable institutions are also required to report suspicious transactions relating to financing of terrorism & proliferation to the FIC.

(c) Accountable institutions that do 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:

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

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

iii. 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 financial institution is from a country that does not have adequate AML/CFT systems;

iv. Warning non-financial sector businesses that transactions with natural or legal persons within that country might run the risk of money laundering; limiting business relationships or financial transactions with the identified country or persons in that country.

1.24 FOREIGN BRANCHES AND SUBSIDIARIES

(a) Accountable institutions shall ensure that their foreign branches and subsidiaries or parent observe group AML/CFT procedures consistent with the provisions of the Guideline and to apply them to the extent that the local/host country's laws and regulations permit.

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

(c) Financial groups shall implement group-wide programmes against ML/TF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group. These measures include:

i. compliance management arrangements (including the appointment of a compliance officer at the management level);

ii. screening procedures to ensure high standards when hiring employees;

iii. an ongoing employee training programme;

iv. an independent audit function to test the system;

v. policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

vi. the provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and

vii. adequate safeguards on the confidentiality and use of information exchanged.

(d) Accountable institutions shall inform the BOG in writing when their foreign branches or subsidiaries or parent are unable to observe the appropriate AML/CFT procedures because they are prohibited by the host country's laws, regulations or other measures.

(e) Accountable institutions are subject to these AML/CFT principles, and shall therefore apply consistently the CDD procedures at their group level, taking into account the activity of the customer with the various branches and subsidiaries.

1.25 AML/CFT EMPLOYEE-EDUCATION AND TRAINING PROGRAMME

Institutional Policy

(a) Accountable institutions shall design comprehensive employee education and training programs 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 tasks. Indeed, the establishment of such an employee training program is not only considered as best practice but also a statutory requirement.

(b) The timing, coverage and content of the employee training program should be tailored to meet the perceived needs of the financial institutions. A comprehensive

training program is however required to encompass staff/areas such as reporting officers; new staff (as part of the orientation program for those posted to the front office); banking operations/branch office staff (particularly cashiers, account opening, mandate, and marketing staff); internal control/audit staff and managers.

Accountable Institutions are required to submit their annual AML/CFT employee training program for the ensuing year to the BOG and FIC not later than the 31st of December every financial year.

(c) The employee training program is required to be developed under the guidance of the AML/CFT Reporting Officer in collaboration with the Executive Management.

The basic elements of the employee training program are expected to include:

i. AML regulations 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

v. Customer due diligence

vi. Risk-based approach to AML/CFT regime

vii. Record keeping and retention policy.

Financial institutions shall submit half yearly report on their level of compliance to the BOG and FIC.

(d) Accountable Institutions shall fully participate in all AML/CFT interactive programmes organized by BOG or FIC. Failure shall attract sanctions from BOG.

1.26 MONITORING OF EMPLOYEE CONDUCT

(a) Accountable institutions shall monitor their employees' accounts for potential signs of money laundering. They are also required to subject employees' accounts, including accounts of key management personnel, to the same AML/CFT procedures as applicable to other customers' accounts. This is required to be performed under the supervision of the AML/CFT Reporting Officer. The AML.CFT reporting officer's

account is to be reviewed by the Chief Internal Auditor or a person of adequate/similar seniority. Compliance reports including findings on the AMLRO's account shall be submitted to the BOG and FIC at the end of June and December every year.

(b) The AML/CFT performance review of staff shall be part of employees' annual performance appraisals.

1.27 PROTECTION OF STAFF WHO REPORT VIOLATIONS

(a) Accountable institutions shall direct their employees in writing and ensure that they always co-operate fully with the Regulators and law enforcement agencies. They are also required to make it possible for directors, officials and employees to report any violations of the institution's AML/CFT compliance program to the AML/CFT Reporting Officer. Where the violations involve the Reporting Officer, employees are required to report such to a designated higher authority such as the Chief Internal Auditor.

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

1.28 ADDITIONAL PROCEDURES AND MITIGANTS

Having reviewed the AML/CFT framework and identified new areas of potential money laundering vulnerabilities and risks, financial institutions shall design additional procedures and mitigants as contingency plan in their AML/CFT Operational Guidelines. These will provide how such potential risks will be appropriately managed if they crystallize. Details of the contingency plan shall be submitted to the BOG and FIC not later than 31st December of every financial year.

1.29 RISK ASSESSMENT FOR NEW PRODUCTS

(a) Accountable institutions shall review, identify and record areas of potential money laundering risks not covered and submit to BOG approval before they are launched

(b) Accountable institutions are therefore required to review their AML/CFT frameworks from time to time with a view to determining their adequacy and identifying other areas of potential risks when introducing new products.

1.30 ADEQUACY OF THE AML/CFTCOMPLIANCE PROGRAMME

Every accountable institution shall make a policy commitment and to subject its AML/CFT compliance program to independent-testing or require its internal audit function to determine its adequacy, completeness and effectiveness. Report of compliance Program is required to be submitted to the BOG and FIC not later than 31st December of every financial year. Any identified weaknesses or inadequacies should be promptly addressed by the accountable institution.

1.31 BOARD APPROVAL OF THE AML/CFT COMPLIANCE MANUAL

The ultimate responsibility for AML/CFT compliance is placed on the Board of every accountable institution in Ghana. It is, therefore, required that the Board ensures that a comprehensive operational AML/CFT compliance manual is formulated by Management and presented to the Board for consideration and formal approval. Copies of the approved manual above are to be forwarded to the BOG within one (1) months of the release of the manual. Quarterly reports on the AML/CFT compliance status of the institution shall be presented to the Board for its information and necessary action.

1.32 CULTURE OF COMPLIANCE

Every accountable institution shall have a comprehensive AML/CFT- compliance program to guide its compliance efforts and to ensure the diligent implementation of its guidelines. Indeed, entrenching a culture of compliance would not only minimize the risks of being used to launder the proceeds of crime but also provide protection against fraud as well as reputational and financial risks.

1.33 TERRORIST FINANCING & FINANCING OF PROLIFERATION

(a) Terrorist financing offences should extend to any person who willfully provides or collects funds by any means, directly or indirectly, with the unlawful 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 by an individual terrorist.

(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. Terrorist financing offences 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 or terrorist organization is located or the terrorist act occurred or will occur.

1.34 MONEY OR VALUE TRANSFER SERVICES (MVTS)

(a) All natural and legal persons that offer Money or Value Transfer Services (MVTS) are required to be licensed by the BOG. The operators are therefore subject to the provisions of Part 1.35 of the Guideline.

(b) MVTS operators shall maintain a current list of its agents and quarterly returns of such be submitted to the BOG. They are required to gather and maintain sufficient information about their agents and correspondent operators or any other operators or institutions they may do business with and maintain records for a minimum of 5 years after the termination of a contractual relationship or completion of a transaction.

(c) MVTS operators shall assess their agents' and correspondent operators' AML/CFT controls and ascertain that they are adequate and effective. They shall obtain approval from the BOG before establishing new correspondent relationships. They shall also document and maintain a checklist of the respective AML/CFT responsibilities of each of its agents and correspondent operators.

(d) In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider should be required to:

i. take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

ii. file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

1.35 WIRE TRANSFERS

(a) For all wire transfers, the ordering financial institutions shall obtain and maintain the following information relating to the originator and beneficiary of the wire transfer:

i. Required and accurate originator information:
- the name of the originator;
- the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and the originator's address, or national identity number, or customer identification number, or date and place of birth.

ii. Required beneficiary information:
- the name of the beneficiary; and
- the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(b) For all wire transfers, the ordering financial institutions shall verify the identity of the originator and beneficiary in accordance with the CDD requirements contained in the Guideline. The receiving financial institution shall also verify the identity of the beneficiary.

(c) For cross-border wire transfers, the ordering financial institutions shall include the full originator and Beneficiary information above in the message or the payment form accompanying the wire transfer.

(d) Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file should contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and the financial institution should be required to include the originator's account number or unique transaction reference number.

(e) For domestic wire transfers, the ordering financial institution shall either:

i. include the full originator and beneficiary information in the message or the payment form accompanying the wire transfer; or

ii. include only the originator‘s and beneficiary’s account number or a unique transaction reference number within the message or payment form provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

(f) The second option should be permitted by the ordering financial institution only if full originator information can be made available to the beneficiary financial institution and to the appropriate authorities within three (3) business days of receiving the request.

(g) The ordering financial institution shall maintain all originator and beneficiary information collected, in accordance with Recommendation 11.

(h) Each intermediary and beneficiary financial institution in the payment chain shall ensure that all originator and beneficiary information that accompanies a wire transfer is transmitted with the transfer.

(i) Where technical limitations prevent the full originator and beneficiary information accompanying a cross-border wire transfer from being transmitted with a related domestic wire transfer (during the necessary time to adapt payment systems), a record must be kept for a minimum of five (5) years by the receiving intermediary financial institution of all the information received from the ordering financial institution. The same applies to beneficial financial institutions.

(j) The ordering financial institution shall not execute the wire transfer if it does not include both the originator and beneficiary information.

(k) Beneficiary financial Institutions shall adopt a risk based approach in determining when to execute, reject or suspend wire transfers lacking the required originator and beneficiary information and the appropriate follow-up action.

(l) Beneficiary financial institutions shall adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator and beneficiary information. The lack of complete originator and

beneficiary information is considered as a factor in assessing whether a wire transfer or related transactions are suspicious. They are therefore required to be reported to the FIC.

(m) The beneficiary financial institution shall restrict or even terminate its business relationship with the financial institutions that fail to meet the above standards.

(n) Cross-border and domestic transfers between financial institutions are, however, not intended to cover the following types of payments:

i. Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction, such as withdrawals from a bank account through an ATM machine, cash advances from a credit card or payments for goods and services. However, when credit or debit cards are used as a payment system to effect a money transfer the necessary information should be included in the message; and

ii. Financial institution-to-financial institution transfers and settlements where both the originator and the beneficiary are financial institutions acting on their own behalf

iii. Money or value transfer service (MVTS) providers are required to comply with all of the relevant requirements in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider:(a) are required to take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

iv. should file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the FIC.

(o) Financial Institutions shall verify the identity of beneficiary of all wire transfers.

(p) Financial Institutions shall ensure that, they take freezing action and comply with prohibitions from conducting transactions with designated persons and entities in the context of processing wire transfers, as per obligations set out in the relevant

UNSCRs relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCRs 1267 and 1373, and their successor resolutions.

2.0 Part B

KNOW YOUR CUSTOMER (KYC) PROCEDURES

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

2.1 DUTY TO OBTAIN IDENTIFICATION EVIDENCE

(a) The first requirement of knowing your customer for money laundering purposes is for the accountable institution to be satisfied that a prospective customer is who he/she is or claims to be.

(b) Accountable institutions shall not carry out or agree to carry out financial business or provide advice to a customer or potential customer unless they are certain as to who that person actually is. If the customer 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 accountable institution has the obligation to verify the identity of both the customer and the agent/trustee unless the customer is itself a Ghanaian regulated financial institution.

(c) Financial institutions have the duty to obtain evidence in respect of their customers. There are certain exceptions to this duty as set out in Section 2.9 of the Guideline. Since exemptions are difficult to apply, accountable institutions are required to identify all relevant parties to the relationship from the outset.

2.2 NATURE AND LEVEL OF THE BUSINESS

The general principles and means of obtaining satisfactory identification evidence are also set out below:

(a) Accountable institutions shall obtain sufficient information on the nature of the business that their customer intends to undertake, including the expected or predictable pattern of transactions.

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

i. purpose and reason for opening the account or establishing the relationship;

ii. nature of the activity that is to be undertaken;

iii. expected origin of the funds to be used during the relationship; and

iv. details of occupation/employment/business activities and sources of wealth or income.

(b) Accountable institutions shall take reasonable steps to keep the information up to date as the opportunities arise, such as when an existing customer opens a new account. Information obtained during any meeting, discussion or other communication with the customer shall be recorded and kept in the customer's file to ensure, as far as practicable, that current customer information is readily accessible to the Anti-Money Laundering Reporting Officer (AMLRO) or relevant regulatory bodies.

2.3 APPLY COMMERCIAL JUDGEMENT

(a) Accountable institutions shall take a risk-based approach to the 'Know Your Customer 'requirements. Institutions shall also decide on the number of times to verify the customers' records during the relationship, the identification evidence required and when additional checks are necessary. These decisions shall equally be recorded. For personal account relationships, all joint-account holders need to be

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

(b) The identification evidence collected at the outset should be viewed against the inherent risks in the business or service.

2.4 ESTABLISHMENT OF IDENTITY IDENTIFICATION EVIDENCE

(a) The customer identification process shall not 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 institution to another.

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

2.5 WHAT IS IDENTITY

(a) Identity generally means a set of attributes such as name(s) used, date of birth and the residential address including the code and digital address at which the customer can be located. These are features which can uniquely identify a natural or legal person.

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

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

2.6 WHEN MUST IDENTITY BE VERIFIED

(a) Identity shall be verified whenever a business relationship is to be established, on account opening or during one-off transaction or when series of linked transactions take place. “Transaction” in the Guideline is defined to include the giving of advice.

The “advice” here does not apply to when information is provided about the availability of products or services nor applies to when a first interview/discussion prior to establishing a relationship takes place.

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

2.7 REDEMPTIONS/SURRENDERS

(a) When an investor realizes his investment (wholly or partially), 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), an accountable institution shall take reasonable measures to establish the identity of the investor where payment is made to:

i. the legal owner of the investment by means of a cheque crossed “account payee”; or

ii. 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.

2.8 WHOSE IDENTITY MUST BE VERIFIED

(a) Clients - sufficient evidence of the identity shall be obtained to ascertain that the client is the very person he/she claims to be.

(b) the person acting on behalf of another - The obligation is to obtain sufficient evidence of identities of the two persons involved. In consortium lending, the lead manager/agent shall supply a confirmation letter as evidence that he has obtained the required identity.

This rule is however, subject to some exceptions;

(c) There is no obligation to look beyond the client where:

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

ii. the client is a bank, broker, fund manager or other regulated financial institutions; and

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

(d) In other circumstances, unless the client is a regulated 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:

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

ii. any principal beneficial owner of funds being invested who is not the accountholder or named investor;

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

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

(e) Financial institutions shall take appropriate steps to identify directors and all the signatories to an account.

(f) Joint applicants/account holders - identification evidence shall be obtained for all the account holders.

(g) For higher risk business 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:

i. the principal underlying beneficial owner(s) of the company with 5% interest and above; and

ii. persons with controlling interest in the company.

(h) Financial institutions 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 Customers as provided in the Guideline.

(i) Trusts – Financial institutions 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.

2.9 SAVINGS SCHEMES AND INVESTMENTS IN THIRD PARTIES' NAMES

When an investor sets up a savings account 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 should be regarded as the applicant for business for whom identification evidence must be obtained in addition to the beneficiary.

2.10 PERSONAL PENSION SCHEMES

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

(b) Personal pension advisers are charged with the responsibility of obtaining the identification evidence on behalf of the pension fund provider. Financial institutions shall demand confirmation of identification evidence given on the transfer of a pension to another provider.

2.11 TIMING OF IDENTIFICATION REQUIREMENTS

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

(b) To this end, financial institutions shall:

i. obtain identification evidence as soon as reasonably practicable after it has contact with a client with a view to agreeing with the client to carry out an initial

transaction; or reaching an understanding (whether binding or not) with the client that it may carry out future transactions; and

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

(c) Financial institutions shall also observe the provision in the Timing of Verification under the AML/CFT Directive of the Guideline.

(d) A financial institution may however start processing the business or application immediately, provided that it:

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

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

(e) The failure or refusal by an applicant to provide satisfactory identification evidence within a reasonable time-frame without adequate explanation may lead to a suspicion that the depositor or investor is engaged in money laundering. The financial institution shall therefore make a suspicious transaction report to the FIC based on the information in its possession.

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

(g) Financial institutions shall respond promptly to inquiries made by competent authorities.

2.12 CANCELLATION & COOLING-OFF RIGHTS

Where an investor exercises cancellation rights or cooling-off rights, the sum invested must be repaid. Since cancellation/cooling-off rights could offer a readily available route for laundering money, financial institutions should 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 should be treated as suspicious and reported to the FIC.

2.13 IDENTIFICATION PROCEDURES

2.14 GENRAL PRINCIPLES

(a) A financial institution shall ensure that it is dealing with a “real” person or organization (natural or business entity) 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 financial institution.

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

(c) No single form of identification can be fully guaranteed as genuine or representing correct identity; the identification process should therefore be cumulative.

(d) The procedures adopted to verify the identity of private individuals and whether or not identification was done face to face or remotely are required to be stated in the customer’s file. The reasonable steps taken to avoid single, multiple fictitious applications, impersonation or fraud are required to be stated also by the financial institution.

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

2.15 NEW BUSINESS FOR EXISTING CUSTOMERS

(a) When an existing customer closes one account and opens another or enters into a new agreement to purchase products or services, there is no need to verify the identity or address for such a customer unless the name or the address provided does not tally with the information in the financial institution's records. However, procedures shall be put in place to guard against impersonation or fraud. The opportunity of opening the new account should also be taken to ask the customer to confirm the relevant details and to provide any missing KYC information. This is particularly important:

i. if there was an existing business relationship with the customer and identification evidence had not previously been obtained; or if there had been no recent contact or correspondence with the customer within the past twelve (12) months; or

ii. when a previously dormant account is re-activated.

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

2.16 CERTIFICATION OF IDENTIFICATION DOCUMENTS

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

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

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

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

ii. a senior official within the account opening institution; or

iii. a lawyer, attorney or notary public.

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

2.17 RECORDING IDENTIFICATION EVIDENCE

(a) Records of the supporting evidence and methods used to verify identity are required to be retained for a minimum period of five (5) years after the account is closed or the business relationship ended.

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

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

(d) An AI may appoint a person to keep records on its behalf.

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

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

(g) An AI that appoints a person to keep records on its behalf shall within seven days, inform the FIC of the appointment in writing.

2.18 CONCESSION IN RESPECT OF PAYMENT MADE BY POST

(a) 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 customer's name (or jointly with one or more other persons) at a regulated financial institution, no further evidence of identity is necessary.

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

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

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

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

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

(d) In order to avoid proceeds of unlawful activity from being laundered by a customer who uses a third-party cheque, draft or electronic payment drawn on a bank, etc, financial institutions may rely upon the required documentary evidence of the third party, without further verification of the identity, where there is no apparent inconsistency between the name in which the application is made and the name on the payment instrument. Payments from joint accounts are considered acceptable for this purpose. The overriding requirement is that the name of the account-holder from where the funds have been provided must be clearly indicated on the record reflecting the payment/ receipt.

(e) In the case of a cheque issued by mortgage institution or banker's draft, it will only be possible to rely on this concession if the holder of the account from which the

money is drawn is confirmed to have met the KYC requirements by the mortgage institution or bank. Likewise, payments by direct debit or debit card cannot be relied upon unless the authentication procedure identifies the name of the accountholder from which the payment is drawn and confirms the customer's address.

(f) In respect of direct debits, it cannot be assumed that the account-holding bank/institution will carry out any form of validation of the account name and number or that the mandate will be rejected if they do not match. Consequently, where payment for the product is to be made by direct debit or debit card/notes, and the applicant's account details have not previously been verified through sighting of a bank statement or cheque drawn on the account, repayment proceeds should only be returned to the account from which the debits were drawn.

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

(h) The concession can apply both where an application is made directly to the financial institution and where a payment is passed through a regulated intermediary.

(i) A financial institution that has relied on the postal concession to avoid additional verification requirements (which must be so indicated on the customer's file) cannot introduce that customer to another financial institution for the purpose of offering bank accounts or other products that provide cheque or money transmission facilities.

(j) If such a customer wishes to migrate to an account that provides cheque or third party transfer facilities, then additional identification checks must be undertaken before the transfer. Where these circumstances occur on a regular basis, financial institutions shall identify all the parties to the relationship at the outset.

2.19 TERM DEPOSIT ACCOUNT (TDA) AND INDIVIDUAL SAVINGS ACCOUNTS (ISA)

TDA can be broadly classified as a one-off transaction. However, financial institutions should note that concession is not available for TDAs opened with cash where there is no audit trail of the source of funds or where payments to or from third

parties are allowed into the account. The identity verification requirements will therefore differ depending on the nature and terms of the TDA and ISA.

2.20 INVESTMENT FUNDS

In circumstances where the balance in an investment funds account is transferred from one Fund Manager to another and identification evidence has neither been taken nor confirmation obtained from the original fund manager, then such evidence should be obtained before the transfer.

2.21 ESTABLISHING IDENTITY

Establishing identity under the Guideline is divided into four broad categories:

i. Private individual customers;

ii. Quasi corporate customers;

iii. Unincorporated businesses/partnerships; and

iv. Corporate customers.

2.22 PRIVATE INDIVIDUALS

(a) General Information

(b) The following information is to be established and independently validated for all private individuals whose identities need to be verified:

i. the full name(s) used; and

ii. the permanent home address, including landmarks and postcode, where available.

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

(d) It is important to obtain the date of birth as it may be required to confirm identity.

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

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

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

(h) For lower-risk accounts or simple investment products such as deposit or savings accounts without cheque-books or automated money transmission facilities, there is an overriding requirement for the financial institution to satisfy itself as to the identity and address of the customer.

2.23 PRIVATE INDIVIDUALS RESIDENT IN GHANA

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

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

2.24 DOCUMENTING EVIDENCE OF IDENTITY

In order to guard against forged or counterfeit-documents, care should be taken to ensure that documents offered are originals. Copies that are dated and signed ‘original sighted by me’ by a senior public servant or equivalent in a reputable private organization could be accepted in the interim, pending presentation of the original documents within six (6) months. Hereunder are examples of acceptable documentary evidence for Ghanaian resident private individuals:

2.25 PERSONAL IDENTITY DOCUMENTS

a. Valid Passport

b. Resident Permit issued by the Ghana Immigration Service

c. Current Driving License issued by the Driver and Vehicle Licensing Authority(DVLA)

d. National Identity card

e. Tax Clearance Certificate(TIN)

f. Birth Certificate

g. Voters ID

h. SSNIT Biometric Card

2.26 DOCUMENTARY EVIDENCE OF ADDRESS

a. Record of home visit

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

c. Recent utility bill (e.g. Water, Electricity and Telephone bills, etc.)

d. State/Local Government Rates documents

e. Bank statement or passbook containing current address

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

g. Tenancy Agreement

h. Search reports on prospective customer's place of employment and residence signed by a senior officer of the financial institution.

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

2.27 PHYSICAL CHECKS ON PRIVATE INDIVIDUALS RESIDENT IN GHANA

(a) It is mandatory for financial institutions to establish the true identities and addresses of their customers and for effective checks to be carried out to protect the institutions against substitution of identities by applicants.

(b) Additional confirmation of the customer's identity and the fact that the application was made by the person identified should be obtained through one or more of the following procedures:

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

ii. an initial deposit cheque drawn on a personal account in the applicant's name in another financial institution in Ghana;

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

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

v. card or account activation procedures.

(c) Financial institutions 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 customer.

2.28 ELECTRONIC CHECKS

(a) As an alternative or supplementary to documentary evidence of identity and address, the applicant's 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.

(b) Accountable institutions shall use a combination of electronic and physical checks to confirm different sources of the same information provided by the customers. Physical and electronic checks of the same statement of account are the different sources.

(c) 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 applicant is the data subject also needs to be conducted within the checking process to ensure that the physical person being verified is the same as or consistent with attributes of the person (eg name, age, gender etc.) in the data base.

(d) Some examples of suitable electronic sources of information are set out below:

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

ii. Access to internal or external account database; and

iii. An electronic search of public records where available.

(e) Applying the above process and procedures will assist financial institutions to guard against impersonation, invented-identities and the use of false address. However, if the applicant is a non-face to face person, one or more additional measures must be undertaken for re-assurance.

2.29 PRIVATE INDIVIDUALS NOT RESIDENT IN GHANA

(a) For prospective customers who are not resident in Ghana but who make face-to-face contact, international passports or national identity cards should generally be available as evidence of the name of the customer. Reference numbers, date and country of issue should be obtained and the information recorded in the customer's file as part of the identification evidence.

(b) Financial institutions shall obtain separate evidence of the applicant's permanent residential address from the best available evidence, preferably from an official source. A postal address in the form of "P.O. Box number" alone is not acceptable as evidence of address. The applicant's residential address should be such that it can be physically located by way of a recorded description or other means.

(c) Relevant evidence should be obtained by the financial institution directly from the customer or through a reputable credit or financial institution in the applicant's home country or country of residence. However, particular care must be taken when relying on identification evidence provided from other countries. Financial institutions are required to ensure that the customer's true identity and current permanent address are actually confirmed. In such cases, copies of relevant identity documents should be sought and retained.

(d) Where a foreign national has recently arrived in Ghana, reference might be made to his/her employer, educational institutions, evidence of traveling documents, etc. to verify the applicant's identity and residential address.

2.30 PRIVATE INDIVIDUALS NOT RESIDENT IN GHANA: SUPPLY OF INFORMATION

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

(b) Documentary evidence of name and address can be obtained:

i. by way of original documentary evidence supplied by the customer; or

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

iii. through a branch, subsidiary, head office of a correspondent bank.

(c) Where the applicant does not already have a business relationship with the financial institution that is supplying the information or the financial institution is not within

Ghana, certified true copies of relevant underlying documentary evidence must be sought, obtained and retained by the institutions.

(d) Where necessary, an additional comfort must be obtained by confirming the customer's true name, address and date of birth from a reputable credit institution in the customer's home country.

Financial institutions are requested to use these requirements in conjunction with Appendix A to the Guideline.

2.31 NON FACE-TO-FACE IDENTIFICATION

(a) In keeping with the requirements on non-face-to-face customers, or where customers are unable to provide original documentation, a financial institution should only accept customer information that has been certified by a qualified practicing notary public.

The absence of face-to-face contact may indicate a higher ML/TF risk situation. If customer identification and verification measures do not adequately address the risks associated with non-face-to-face contact, this may increase the risk of identity fraud or customers providing inaccurate information potentially to disguise illegal activity if effective measures to address this risk are not employed. However, this lack of face-to-face contact is often counter-balanced through the adoption of alternative identification mechanisms, which can provide adequate risk mitigation measures. Accordingly, at least one additional measure or check should be undertaken to supplement the documentary or electronic evidence. These additional measures will apply whether the applicant is resident in Ghana or elsewhere and must be particularly robust where the applicant is requiring a bank account or other product/service that offers money transmission or third party payments.

(b) Procedures to identify and authenticate the customer have 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 or fraud.

Non-face-to-face verification of customer identity often requires corroborating information received from the customer with information in third party databases or

other reliable sources, and potentially tracing the customer's Internet Protocol (IP) address, and even searching the Web for corroborating information, provided that the data collection is in line with national privacy legislation. It may be appropriate to use multiple techniques to effectively verify the identity of customers. In situations where higher ML/TF risk is identified, enhanced CDD should be carried out in proportion to that risk.

(c) The extent of the identification evidence required will depend on the nature and characteristics of the product or service and the assessed risk. However, care must be taken to ensure that the same level of information is obtained for internet customers and other postal/telephone customers.

(d) If reliance is being placed on intermediaries to undertake the processing of applications on the customer's behalf, checks should be undertaken to ensure that the intermediaries are regulated for anti-money laundering prevention and that the relevant identification procedures are applied. In all cases, evidence as to how identity has been verified should be obtained and retained with the account opening records.

(e) Financial institutions shall conduct regular monitoring of internet-based business/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 should be put in place to recognize suspicious transactions. AML/CFT Reporting Officers are required to review these systems/solutions, record exemptions and report same half yearly to the BOG and FIC.

2.32 ESTABLISHING IDENTITY FOR REFUGEES AND ASYLUM SEEKERS

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

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

2.33 ESTABLISHING IDENTITY FOR STUDENTS AND MINORS

(a) When opening accounts for students or minors, the normal identification procedures set out in the Guideline should be followed as far as possible. Where such procedures would not be relevant or do not provide satisfactory identification evidence, verification could be obtained:

i. via the home address of the parent(s); or

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

iii. by seeking evidence of a tenancy agreement or student accommodation contract.

(b) 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 financial institution, the identification evidence for that adult, or of any other person who will operate the account should be obtained in addition to obtaining the birth certificate or passport of the child. It should be noted that this type of account could be opened to abuse and therefore strict monitoring should then be undertaken and maintained.

(c) For accounts opened through a school-related scheme, the school should 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.

2.34 QUASI CORPORATE CUSTOMERS

Establishing Identity–Trusts, Nominees and Fiduciaries

(a) Trusts, nominee companies and fiduciaries are popular vehicles for criminals wishing to avoid the identification procedures and mask the origin of the proceeds of unlawful activity they wish to launder. The particular characteristics of trusts that attract the

genuine customer, the anonymity and complexity of structures that they can provide are also highly attractive to money launderers.

(b) Some trusts, nominees and fiduciary accounts present a higher money laundering risk than others. Identification and “Know Your Business” procedures need to be set and managed according to the perceived risk.

(c) 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 controllers who have 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.

(d) Whilst reliance can often be placed on other financial institutions that are regulated for money laundering prevention to undertake the checks or confirm identity, the responsibility to ensure that this is undertaken rests with the financial institution. The underlying evidence of identity must be made available to law enforcement agencies in the event of an investigation.

(e) 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.

Offshore Trusts

(f) 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 should warrant additional enquiries.

(g) Unless the applicant for business is itself a regulated financial institution, measures should be taken to identify the trust company or the corporate service provider in line with the requirements for professional intermediaries or companies generally.

(h) Certified true copies of the documentary evidence of identity for the underlying principals such as settlors, controllers, etc. on whose behalf the applicant for business is acting, should also be obtained.

(i) For overseas trusts, nominee and fiduciary accounts, where the applicant is itself a financial institution that is regulated for money laundering purposes:

i. reliance can be placed on an introduction or intermediary certificate letter stating that evidence of identity exists for all underlying principals and confirming that there are no anonymous principals;

ii. the trustees/nominees should be asked to state from the onset the capacity in which they are operating or making the application;

iii. documentary evidence of the appointment of the current trustees should also be obtained.

(j) Where the underlying evidence is not retained within Ghana, enquiries should 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, should it be needed in Ghana.

(k) Any application to open an account or undertake a transaction on behalf of another without the applicant identifying their trust or nominee capacity should be regarded as suspicious and should lead to further enquiries and submission of reports to the FIC.

(l) Where a bank in Ghana is itself the applicant to an offshore trust on behalf of a customer, if the corporate trustees are not regulated, then the Ghanaian bank should undertake the due diligence on the trust itself.

(m) If the funds have been drawn on an account that is not under the control of the trustees, the identity of the authorized signatories and their authority to operate the account should also be verified. When the identity of beneficiaries has not previously been verified, verification should be undertaken when payments are made to them.

Conventional Family and Absolute Ghanaian Trusts

(n) In the case of conventional Ghanaian trusts, identification evidence should be obtained for:

i. those who have control over the funds (the principal trustees who may include the settlor);

ii. the providers of the funds (the settlors, except where they are deceased); and

iii. where the settlor is deceased, written confirmation should be obtained for the source of funds (grant of probate or copy of the Will or other document creating the trust).

(o) 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 procedure contained in the Guideline for verifying the identity of persons, institutions or companies should be followed.

(p) Although a financial institution may not review any existing trust, confirmation of the settlor and the appointment of any additional trustees should be obtained.

(q) Copies of any underlying documentary evidence should be certified as true copies. In addition, a check should 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; consideration should be given as to whether the identity of any additional authorized signatories to the bank account should also be verified.

(r) It is a normal practice for payment of any trust property to be made to all the trustees. As a matter of practice, some life assurance companies make payments directly to beneficiaries on receiving a request from the trustees. In such circumstances, the payment should be made to the named beneficiary by way of a crossed cheque marked “account payee only” or a bank transfer direct to an account in the name of the beneficiary.

Receipt and Payment of Funds

(s) Where money is received on behalf of a trust, reasonable steps should be taken to ensure that:

i. the source of the funds is properly identified; and

ii. the nature of the transaction or instruction is understood**.**

(t) It is also important to ensure that payments are properly authorized in writing by the trustees.

Identification of New Trustees

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

Life Policies Placed in Trust

(v) Where a life policy is placed in trust, the applicant for the policy is also a trustee and where the trustees have no beneficial interest in the funds, it should only be necessary to verify the identity of the person applying for the policy. The remainder of the trustees would however need to be identified in a situation where policy proceeds were being paid to a third party not identified in the trust deed.

Powers of Attorney and Third Party Mandates

(w) 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 should be obtained from the holders of powers of attorney and third party mandates in addition to the customer 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 should always be verified. The most important requirement is for financial institutions to ascertain the reason for the granting of the power of attorney.

(x) Records of all transactions undertaken in accordance with the power of attorney should be maintained as part of the client's record.

2.35 EXECUTORSHIP ACCOUNTS

a. Where a bank 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.

b. However, identification evidence would not normally be required for the executors/administrators when payment is being made from an established financial institutions 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 is normally no need to obtain identification evidence for the legal representatives.

c. 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 will be required.

d. In the event that there is suspicion concerning the nature or origin of assets comprising an estate that is being wound up, then reports of the suspicions are required to be submitted to the FIC.

"Client Accounts" Opened By Professional Intermediaries

(e) Stockbrokers, fund managers, solicitors, accountants, estate agents and other intermediaries frequently hold funds on behalf of their clients in "client accounts "opened with financial institutions. Such accounts may be general omnibus accounts holding the funds of many clients or they may be opened specifically for a single client. In each case, it is the professional intermediary who is the financial institution's customer. These situations should be distinguished from those where an intermediary introduces a client who himself becomes a customer of the financial institution.

(f) Where the professional intermediary is itself covered and indeed is monitored under the Anti-Money Laundering Regulations and by AML/CFT supervisors respectively or their equivalent, identification can be waived on production of evidence.

(g) However, where the professional intermediary is not covered under the Anti-Money Laundering Regulations or their equivalent, the financial institution should not only verify the identity of the professional intermediary but should verify also the identity of the person on whose behalf the professional intermediary is acting.

(h) Where it is impossible for a financial institution to establish the identity of the person(s) for whom a solicitor or accountant is acting, it will need to take a

commercial decision based on its knowledge of the intermediary, as to the nature and extent of business that they are prepared to conduct if the professional firm is not itself covered by the Guideline. Financial institutions should be prepared to make reasonable enquiries about transactions passing through client-accounts that give cause for concern and should report any transaction where suspicions cannot be verified to the FIC.

Unincorporated Business /Partnership

(i) Where the applicant is an un-incorporated business or a partnership whose principal partners/controllers do not already have a business relationship with the financial institution, identification evidence should 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.

(j) Evidence of the trading address of the business or partnership should be obtained. Where a current account is being opened, a visit to the place of business might also be made to confirm the true nature of the business activities. For established businesses, a copy of the latest annual audited accounts should be obtained.

(k) The nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose. In cases where a formal partnership agreement 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 should be obtained.

Limited Liability Partnership

(l) Limited liability partnerships should be treated as corporate customers for verification of identity and Know Your Customer purposes.

2.36 CORPORATE CUSTOMERS

General Principles

(a) Complex organizations and their structures, other corporate and legal entities are the most likely vehicles for money laundering. Those that are privately owned are being fronted by legitimate trading companies. Care should be taken to verify the legal

existence of the applicant-company from official documents or sources and to ensure that persons purporting to act on its behalf are fully authorized. Enquiries should be made to confirm that the legal person is not merely a “brass-plate company” where the controlling principals cannot be identified.

(b) The identity of a corporate body comprises:

i. registration number;

ii. registered corporate name and any trading names used;

iii. registered address and any separate principal trading addresses;

iv. directors;

v. owners and shareholders; and

vi. the nature of the company’s business.

vii. regulations of the company

(c) The extent of identification measures required in 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 financial institution. A risk-based approach should be taken. In all cases, information as to the nature of normal business activities that the company expects to undertake with the financial institution should be obtained. Before a business relationship is established, measures should be taken by way of company search at the Registrar General’s Department/other regulatory authorities and other commercial enquiries undertaken to ensure that the applicant-company’s legal existence has not been or is not in the process of being dissolved, struck off, wound up or terminated.

Non Face -to -Face Business

(d) As with the requirements for private individuals, because of the additional risks with on-face-to-face business, additional procedures shall be undertaken to ensure that the applicant’s business, company or society exists at the address provided and it is for a legitimate purpose.

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

(f) Where the principal owners, controllers or signatories need to be identified within the relationship, the relevant requirements for the identification of personal customers should be followed.

Public Registered Companies

(g) Corporate customers that are listed on the stock exchange are considered to be publicly owned and generally more accountable. However, if the circumstances trigger suspicion, the identity of a shareholder may be verified

(h) Similarly, it is not necessary to identify the directors of a quoted company. However, financial institutions shall make appropriate arrangements to ensure that the individual officer or employee (past or present) is not using the name of the company or its relationship with the financial institution for unlawful activity. The Board resolution or other authority for any representative to act on behalf of the company in its dealings with the financial institution shall be obtained to confirm that the individual has the authority to act. Phone calls can be made to the Chief Executive Officer/or the designated officer of such a company to inform him of the application to open the account.

(i) No further steps should be taken to verify identity over and above the usual commercial checks where the applicant company is listed on the stock exchange; or there is independent evidence to show that it is a wholly owned subsidiary or a subsidiary under the control of such a company.

(j) Due diligence will normally be conducted where the account or service required falls within the category of higher risk business.

Private Companies

(k) Where the applicant is an unquoted company and none of the principal directors or shareholders already have an account with the financial institution, the following documents should be obtained from an official or recognized independent source to verify the business itself:

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

ii. a search at the Registrar General's Department or an enquiry via a business information service to obtain the information in (a) above; and

iii. an undertaking from a firm of lawyers or accountants confirming the documents submitted to the Registrar General's Department.

(l) Attention should 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 should be undertaken.

2.37 HIGHER RISK BUSINESS

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

i. For established companies (those incorporated for eighteen (18) months or more) a set of the latest annual report shall be produced;

ii. A search report at the Registrar General's Department or an enquiry via a business information service or an undertaking from a firm of lawyers or accountants confirming the documents submitted to the Registrar General's Department;

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

iv. The regulations of the company.

Higher Risk Business Relating to Private Companies

(b) For private 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 assets. What constitutes significant shareholding or control for this purpose

will depend on the nature of the company. Identification evidence shall be obtained for those shareholders with interests of 5% or more.

(c) 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.

(d) 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. 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 financial institutions become aware that the principal-beneficiary owners/controllers have changed, they are required to ensure that the identities of the new ones are verified.

(e) Financial institutions shall also identify directors who are not principal controllers and signatories to an account for risk based approach purpose.

(f) In respect of a full banking relationship (irrespective of whether or not the turnover is significant) a visit to the place of business shall be undertaken to confirm the existence of business premises and the nature of the business activities conducted.

(g) If suspicions are aroused by a change in the nature of the business transacted or the profile of payments through a bank or investment account, further checks shall be made to ascertain the reason for the changes.

(h) For full banking relationships, periodic enquiries shall be made to establish whether there have been any changes to controllers, shareholders or to the original nature of the business or activity.

(i) Particular care shall be taken to ensure that full identification and "Know Your Customer" requirements are met if the company is an International Business Company (IBC) registered in an offshore jurisdiction and operating out of a different jurisdiction.

Foreign Financial Institutions

(j) For foreign financial institutions, the confirmation of existence and regulatory status should be checked by one of the following means:

i. checking with the home country's central bank or relevant supervisory body; or

ii. checking with another office, subsidiary, branch, or correspondent bank in the same country;

iii. checking with Ghanaian regulated correspondent bank of the overseas institution;

iv. obtaining evidence of its licence or authorization to conduct financial and banking business from the institution itself.

(k) Additional information on banks all over the world can be obtained from various international publications and directories or any of the international business information services.

References made to these publications are not meant to replace the confirmation evidence required above.

Forex Bureaux

Although forex bureaux are subject to the regulations, they must be verified in accordance with the procedures for 'Other Financial Institutions'. Satisfactory evidence of identity must include receipt of a certified copy of the applicant's operating license.

2.38 OTHER INSTITUTIONS

(a) Clubs and Societies

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

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

(b) Occupational Pension Schemes

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

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

iii. 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 registers or references from professional advisers or investment managers.

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

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

2.39 CHARITIES IN GHANA

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

ii. The practice of opening unauthorized accounts of this type under sole control is strongly discouraged. For emphasis, accounts for charities in Ghana shall be operated by a minimum of two signatories, duly verified and documentation evidence obtained.

2.40 REGISTERED CHARITIES

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

ii. To guard against the laundering of proceeds from unlawful activity (where the person making the application or undertaking the transaction is not the official correspondent or the recorded alternate) a financial institution shall send a letter to the official correspondent, informing him of the charity's application before it. The official correspondent should be requested to respond as a matter of urgency especially where there is a reason to suggest that the application has been made without authority.

iii. Where a charity is opening a current account, the identity of all signatories should be verified initially and when the signatories change, care should be taken to ensure that the identity of any new signatory is verified.

iv. Applications on behalf of un-registered charities should be dealt with in accordance with procedures for clubs and societies set out in item 2.38 (a) of the Guideline.

2.41 RELIGIOUS ORGANIZATIONS (ROs)

A religious organization is expected by law to be registered by the Registrar General's Department and will therefore have a registered number. Its identity can be verified by reference to the Registrar General's Department, appropriate headquarters or regional area of the denomination. As a registered organization, the identity of at least two signatories to its account must be verified.

2.42 MINISTRIES, DEPARTMENTS AND AGENCIES, MDAs AND OTHER PUBLIC INSTITUTIONS

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

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

2.43 FOREIGN CONSULATES

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

2.44 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 financial institution that is entering into the relationship with a client, it is reasonable, in a number of circumstances, for reliance to be placed on another financial institution to:

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

ii. confirm the identification details if the customer is not resident in Ghana; or

iii. confirm that the verification of identity has been carried out (if an agent is acting for underlying principals).

(b) Introductions from Authorized Financial Intermediaries

Where an intermediary introduces a customer and then withdraws from the ensuing relationship altogether, then the underlying customer has become the applicant for the business. He must, therefore, be identified in line with the requirements for personal, corporate or business customers as appropriate. An introduction letter should therefore be issued by the introducing financial institution 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 must either be accompanied by certified true 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) a financial intermediary must provide along with each application, the customer's introduction letter together with certified true copies of the evidence of identity which should be placed in the customer's file. If these procedures are followed, the product provider, stockbroker or investment banker will be considered to have fulfilled its own identification obligations. However, if the letter is not forthcoming from the intermediary, or the letter indicates that the intermediary has not verified the identity of the applicant, the service provider is required to satisfy its obligation by applying its own direct identification procedures.

(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 customers and ensure that the intermediary provides specific confirmation that identity has been verified.

A record must be made of the answers given by the intermediary and retained for a minimum period of five (5) years. These answers constitute sufficient evidence of identity in the hands of the service provider.

(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 must be assessed by the Anti-Money Laundering Reporting Officer (AMLRO) or some other competent person within the financial institution on a case by case basis based on the knowledge of the intermediary.

(f) Corporate Group Introductions

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

i. the identity of the customer has been verified by the introducing parent company, branch, subsidiary or associate in line with the Anti-Money Laundering requirements to equivalent standards and taking account of any specific requirements such as separate address verification;

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

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

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

(g) Where financial institutions have day-to-day access to all the Group's "Know Your Customer" information and records, there is no need to identify an introduced customer or obtain a group introduction letter if the identity of that customer has been verified previously. However, if the identity of the customer 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 should be obtained.

(h) For financial institutions that rely on a third party that is part of the same financial group, relevant competent authorities may also consider the following circumstances:

i. the group applies CDD and record-keeping requirements, in line with Part 1.4, 1.5, 1.11 and 1.15, and programmes against money laundering and terrorist financing, in accordance with Part 1.24 of the Guideline;

ii. the implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority; and

iii. any higher country risk is adequately mitigated by the group's AML/CFT policies.

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

(j) Where identification records are held outside Ghana, it is still the responsibility of the financial institution to ensure that the records available do, in fact, meet the requirements in the Guideline.

(k) Business Conducted by Agents

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

A financial institution may regard evidence as sufficient if it has established that the client:

i. is bound by and has observed the Guidelines or the provisions of the Anti-Money Laundering Act, 2008 (Act 749); and

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

(l) Consequently, where another financial institution deals with its own client(regardless of whether or not the underlying client is disclosed to the financial institution) then:

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

ii. where a regulated agent from outside Ghana deals through a customer omnibus account or for a named customer through a designated account, the agent should provide a written assurance that the identity of all the underlying clients has been verified in accordance with their local requirements.

Where such an assurance cannot be obtained, then the business should not be undertaken.

(m) In circumstances where an agent is either unregulated or is not covered by the relevant Anti-Money Laundering Legislation, then each case should be treated on its own merits. The knowledge of the agent will inform the type of the diligence standards to apply. The Risk-based approach must also be observed by the financial institution.

(n) Syndicated Lending

For syndicated lending arrangements, the verification of identity and any additional KYC requirements rest with the lead-manager or agent required to supply the normal confirmation letters.

(o) Correspondent Relationship

Transactions conducted through correspondent relationships need to be managed, taking a risk-based approach. “Know Your Correspondent” procedures shall be established to ascertain whether or not the correspondent bank or the counterparty is itself regulated for money laundering prevention. If regulated, the correspondent shall verify the identity of its customers in accordance with FATF standards.

Where this is not the case, additional due diligence will be required to ascertain and assess the correspondent's internal policy on money laundering prevention and know your customer procedures.

(p) The volume and nature of transactions flowing through correspondent accounts with financial institutions from high risk jurisdictions or those with inadequacies or material deficiencies should be monitored against expected levels and destinations and any material variances should be checked.

(q) Financial institutions shall maintain records of having ensured that sufficient diligence has been undertaken by the remitting bank on the underlying client and the origin of the funds in respect of the funds passed through their accounts.

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

(s) Staff dealing with correspondent banking accounts are required to be trained to recognize higher risk circumstances and be prepared to challenge the correspondents over irregular activity (whether isolated transactions or trends) and to submit a suspicious transaction report (STR) to the FIC.

(t) Financial institutions shall terminate their accounts with correspondent banks that fail to provide satisfactory answers to reasonable questions including confirming the identity of customers involved in unusual or suspicious circumstances.

2.45 ACQUISITION OF ONE FINANCIAL INSTITUTION/BUSINESS BY ANOTHER

(a) When one financial institution acquires the business and accounts of another financial institution, it is not necessary for the identity of all the existing customers to be re-identified, provided that all the underlying customers' records are acquired with the business. It is, however, important to carry out due diligence enquiries to confirm that the acquired institution had conformed with the requirements in the Guideline.

(b) Verification of identity should be undertaken as soon as it is practicable for all the transferred customers who were not verified by the transferor in line with the requirements for existing customers that open new accounts, where:

i. the Anti-Money Laundering procedures previously undertaken have not been in accordance with the requirements of the Guideline;

ii. the procedures cannot be checked; or

iii. where the customer-records are not available to the acquiring financial institution.

2.46 RECEIVING FINANCIAL INSTITUTIONS AND AGENTS

(a) Vulnerability of Receiving Bankers and Agents to Money Laundering Receiving financial institutions 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 unlawful activity. New issues that trade at a discount will, therefore, still prove acceptable to the money launderer. Proceeds from unlawful activity 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 should be identified?

Receiving financial institutions shall obtain satisfactory identification evidence of new applicants, including such applicants in a rights issue.

If funds to be invested are provided 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.

2.47 APPLICATIONS RECEIVED THROUGH BROKERS

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

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

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

(b) The terms and conditions of the issue should state that any requirements to obtain identification evidence are the responsibility of the broker lodging the application and not the receiving financial institution.

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

2.48 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.

2.49 MULTIPLE FAMILY APPLICATIONS

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

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

ii. a joint account holder; or

iii. an application in the name of a child where the 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.

(b) However, identification evidence of the signatory of the financial instrument will be required for any multiple family applications 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 Anti-Money Laundering legislation, regulation and guidelines.

(c) Where an application is supported by a financial institution's branch cheque or bankers draft, the applicant should state the name and account number from which the funds were drawn:

i. on the face of the cheque; or

ii. on the back of the cheque together with a branch stamp; or

iii. providing other supporting documents.

2.50 LINKED TRANSACTIONS

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

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

(c) Applications that are believed to be linked 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 submitted to the FIC accordingly. Copies of the supporting cheques, application forms and any repayment-cheque must be retained to provide an audit trail until the receiving financial institution is informed by FIC or the investigating officer that the records are of no further interest.

2.51 DOMICILIARY ACCOUNT (DA)

Where a customer wishes to open a DA or make a wholesale deposit by means of cash or inter-bank transfer, the financial institution shall obtain identification evidence in accordance with the requirements for private individuals, companies or professional intermediaries operating on behalf of third parties as appropriate.

It should satisfy itself that the transferring institution is regulated for money laundering prevention in its country of origin.

2.52 PROVISION OF SAFE CUSTODY AND SAFE DEPOSIT BOXES

Precautions should be taken in relation to requests to hold boxes, parcels and sealed envelopes in a safe custody. Where such facilities are made available to non-accountholders, the identification procedures set out in the Guideline shall be followed, depending on the type of individual involved.

2.53 EXEMPTION FROM IDENTIFICATION PROCEDURES

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

(a) Ghanaian Financial Institutions

Identification evidence is not required where the applicant for business is a Ghanaian financial institution or person covered and regulated by the requirements of the Guideline.

(b) 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 customers who do not have an account or other established relationship with the financial institution (i.e. walk in customers) 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 financial institution's business, identification evidence must be observed.

(c) Re-investment of Income

The proceeds of a one-off transaction due can be paid to a customer or be further re-invested where records of his identification requirements were obtained and kept.

In the absence of this his/her identification requirements must be obtained before the proceeds are paid to him or be re-invested on his behalf in accordance with the relevant provision of the Guideline.

2.54 FINANCIAL INCLUSION

Financial inclusion for the socially and financially disadvantaged applicant's resident in Ghana.

(a) Access to basic banking facilities and other financial services is a necessary requirement for most adults. It is important therefore that the socially and financially disadvantaged should not be precluded from opening accounts or obtaining other financial services merely because they do not possess evidence to identify themselves. In circumstances where they cannot reasonably do so, the internal procedures of the financial institutions must make allowance for such persons by way of providing appropriate advice to staff on how the identities of such group of persons can be confirmed and what checks should be made under these exceptional circumstances.

(b) Where a financial institution has reasonable grounds to conclude that an individual client is not able to produce the detailed evidence of his identity and cannot reasonably be expected to do so, the institution may accept as identification evidence a letter or statement from a person in a position of responsibility who knows the client and can confirm that the client is who he/she says he/she is, including confirmation of his permanent address. The ID of the guarantor must be obtained and verified.

(c) When a financial institution has decided to treat a client as "financially excluded", it shall record and maintain the reasons for doing so along with the account opening documents. This is to guard against financial exclusion and to minimize the use of exception procedures.

(d) The financial institution shall satisfy itself that such customer is the person he/she claims to be.

(e) Financial institutions shall put in place additional monitoring of accounts opened under the financial inclusion exception procedures to ensure that such accounts are not misused.

2.55 SANCTIONS FOR NON-COMPLIANCE WITH KYC

Failure to comply with the provisions contained in this Guideline will attract appropriate sanctions in accordance with existing laws.

The extent to which the contravention departs from the required standard. In line with this BOG shall make distinction between a breach, deficiency and recommendation.

- Breaches of the AML/CFT acts – The reporting entity has failed to meet the requirements of the AML/CFT acts. The BOG considers the breach to be a material issue and / or a systemic issue that requires immediate steps to be taken to achieve on-going compliance. This will attract immediate penalties or sanctions from BOG.
- Deficiency - The reporting entity has failed to meet the standard requirements of the AML/CFT acts. BOG considers supervisory action is required to achieve ongoing compliance within a specified time line stated by BOG. Failure to comply within the specified time frame shall attract administrative penalties.
- Recommendations – BOG considers it best practice for reporting entity to consider and implement the appropriate changes in line with BOG recommendations. These recommendations do not constitute regulatory action.

APPENDIX A

INFORMATION TO ESTABLISH IDENTITY

A. Natural Persons

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

i. legal name and any other names used by the prospective client;

ii. location including important landmarks close to the prospective client's residence;

iii. telephone number, fax number and mailing address;

iv. date and place of birth;

v. nationality;

vi. hometown;

vii. occupation, position held and employer's name;

viii. identity document;

ix. nature of business;

x. type of account and nature of the banking relationship; and

xi. signature.

The financial institution should verify this information by at least one of the following methods:

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

- Confirming the permanent address (e.g. utility bill, tax assessment, bank statement, a letter from a public authority);
- Contacting the customer by telephone, by letter or by 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 should warrant further investigation);
- Confirming the validity of the official documentation provided through certification by an authorized person (e.g. embassy official, notary public) and
- any other means of verification the bank deems appropriate

Financial institutions should apply the same standard of identification and verification in respect of non-face-to-face customers.

Risk Profiling

Based on the information provided, financial institutions should assess the risk profile of their customers taking into consideration the following:

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

A financial institution's customer acceptance policy should not be so restrictive as to deny the general public access to banking services.

B. Institutions

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

i. Business Entities

(a) Identification and Verification

For business entities the following information should be obtained:

- Name of institution;
- Principal place of institution's business operations;
- Mailing address of institution;
- Contact telephone, fax numbers and website address;
- Some form of official identification number, if available (e.g. tax identification number);
- The original or certified true copy of the certificate of incorporation and
- Regulations;
- The resolution of the Board of Directors to open an account and identification of
- those who have authority to operate the account;
- Nature and purpose of business and its legitimacy.
- The financial institution should verify this information by at least one of the
- following methods:
- For established corporate entities - reviewing a copy of the latest annual report
- (audited, if available);
- Conducting an enquiry by a business information service, or an under taking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
- 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;
- Utilizing an independent information verification process, such as accessing public and private databases;

- Obtaining prior bank references;
- Visiting the corporate entity; and
- Contacting the corporate entity by telephone, mail or e-mail.

The financial institution should also take reasonable steps to verify the identity and reputation of any agent that opens an account on behalf of a corporate customer, if that agent is not an officer of the corporate customer.

(b) Ownership and Control

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

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

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

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

Where a company is listed on a recognized stock exchange or is a subsidiary of such a company then the company itself may be considered to be the principal to be identified. However, consideration should 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 should also be considered to be principals and identified accordingly.

ii. Other Types of Institution

The following information should 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 and any other institution as specified under the Act 749as amended and L.I.1987:

- Name of account;
- Mailing address;
- Contact telephone, fax number, website and email address;
- 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 register of charities.

The financial institution should verify this information by at least one of the following:

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

(a) Retirement Benefit Programme

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

(b) Mutual/Friendly, Cooperative and Provident Societies

Where these entities are an applicant for an account, the principals to be identified should be considered to be those persons exercising control or significant influence

over the organization's assets. This often includes board members, executives and account signatories.

(c) Charities, Clubs and Associations

In the case of accounts to be opened for charities, clubs and societies, the financial institution should take reasonable steps to identify and verify at least two signatories along with the institution itself. The principals who should be identified should 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 should be obtained that the persons involved are true representatives of the institution. Independent confirmation should also be obtained of the purpose of the institution.

(d) Trusts and Foundations

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

(e) Professional Intermediaries

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

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

Where the funds are co-mingled, the financial institution should look through to the beneficiary-owners.

However, there may be circumstances that the financial institution 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 financial institution).

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 financial institution, the following should be considered as principals and the financial institution should take steps to identify them:

- The fund itself;
- Its directors or any controlling board, where it is a company;
- Its trustee, where it is a unit trust;
- Its managing (general) partner, where it is a limited partnership;
- Account signatories;
- Any other person who has control over the relationship such as fund administrator or manager.

Where other investment vehicles are involved, the same steps should be taken as in above (where it is appropriate to do so). In addition, all reasonable steps should be taken to verify the identity of the beneficial owners of the funds and of those who have control over the funds.

Intermediaries should be treated as individual customers of the financial institution and the standing of the intermediary should be separately verified by obtaining the appropriate information itemized above.

APPENDIX B

DEFINITION OF TERMS

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

Terms	Definition
Applicant for Business	The person or company seeking to establish a 'business relationship' or an occasional customer undertaking a 'one-off 'transaction whose identity must be verified.
Batch transfer	A batch transfer is a transfer comprising a number of individual wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.
Beneficial owner	Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
Beneficiary	Beneficiary includes those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of Non-Profit Organizations (NPO). They comprise all trusts (other than charitable or statutory permitted non-charitable trusts) that must have beneficiaries, who may include the settlor, and a maximum time, known as the perpetuity period, normally of 100 years.
Business	Business relationship is any arrangement between the financial institution and the

Relationship	applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a 'frequent, habitual or regular' basis and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset.
Business Entity	Business entity includes (a) a firm, (b) an individual licensed to carry out a business, (c) a limited liability company, or (d) a partnership,
Cross-border transfer	Cross-border transfer means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element.
Designated categories of offences	• Designated categories of offences means: • participation in an organised criminal group and racketeering; • terrorism, including terrorist financing; • trafficking in human beings and migrant smuggling;

	• sexual exploitation, including sexual exploitation of children; • illicit trafficking in narcotic drugs and psychotropic substances; • illicit arms trafficking; • illicit trafficking in stolen and other goods; • corruption and bribery; • fraud; • counterfeiting currency; • counterfeiting and piracy of products; • environmental crime; • murder, grievous bodily injury; • kidnapping, illegal restraint and hostage-taking; • robbery or theft; • smuggling; • tax evasion • extortion; • forgery; • piracy; and • insider trading and market manipulation.
Designated nonfinancial businesses and professions	• Designated non-financial businesses and professions means: • Casinos (which also includes internet casinos).

- Real estate agents.
- Dealers in precious metals.
- Dealers in precious stones.
- Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to “internal” professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
- Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:
- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as)a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative

	address for a company, a partnership or any other legal person or arrangement; • acting as (or arranging for another person to act as) a trustee of an express trust; • acting as (or arranging for another person to act as) a nominee shareholder for another person.
Domestic transfer	Domestic 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 declaration	False declaration refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
False disclosure	False disclosure refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required

The FATF Recommendations	The FATF Recommendations refers to the Forty Recommendations and the Nine Special Recommendations on Terrorist Financing.
Financial institutions	Financial institutions means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public. 2. Lending. 3. Financial leasing. 4. The transfer of money or value. 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveler's cheques, money orders and bankers' drafts, electronic money). 6. Financial guarantees and commitments. 7. Trading in: 8. money market instruments (cheques, bills, CDs, derivatives etc.); 9. foreign exchange; 10. exchange, interest rate and index instruments; 11. transferable securities; 12. commodity futures trading. 13. Participation in securities issues and the provision of financial services related to such

	issues. 14. Individual and collective portfolio management. 15. Safekeeping and administration of cash or liquid securities on behalf of other persons. 16. Otherwise investing, administering or managing funds or money on behalf of other persons. 17. Underwriting and placement of life insurance and other investment related insurance. 18. Forex Bureaus. The list is not exhaustive but subject to the definition contained in the Banks & SDI Act 2016, Act 930.
Funds Transfer	The terms funds transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.
Legal arrangements	Legal arrangement refers to express trusts or other similar legal arrangements.
Legal persons	Legal persons refer to bodies corporate, foundations, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.

Non-profit Organizations/ Non-governmental Organizations	The term non-profit organization/non-governmental organizations refers to a legal entity or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of good works.
Originator	The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.
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	Payable through account refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.
Proceeds	Proceeds refer to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	Property means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal

	documents or instruments evidencing title to, or interest in such assets.
Risk	All references to risk in the Guideline refers to the risk of money laundering and/or terrorist financing.
Settlor	Settlors are persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trust's assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets
Shell bank	Shell 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.
Physical presence	means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.
Terrorist	It refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist

	acts; (iii) organizes 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	A terrorist act includes but are not limited to: 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 forthe 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 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 organization to do or to abstain from doing any act.
Terrorist financing	Terrorist financing (FT) includes the financing of terrorist acts, and of terrorists and terrorist organizations.
Terrorist financing offence	A terrorist financing (FT) offence refers not only to the primary offence or offences, but also to ancillary offences.
Terrorist organization	Refers to any group of terrorists that: • commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; • participates as an accomplice in terrorist acts; • organizes or directs others to commit terrorist acts; or • contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of

	furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Those who finance Terrorism	Those who finance terrorism refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts.
Trustee	Trustees, include paid professionals or companies or unpaid persons who hold the assets in a trust fund separate from their own assets. They invest and dispose of them in accordance with the settlor‘s trust deed, taking account of any letter of wishes. There may also be a protector who may have power to veto the trustees‘ proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.
Unique identifier	A unique identifier refers to any unique combination of letters, numbers or symbols that

	refer to a specific originator.
Wire transfer	The term wire transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.

APPENDIX C

MONEY LAUNDERING AND TERRORISTFINANCING "RED FLAGS"

1. INTRODUCTION

Monitoring and reporting of suspicious transactions is key to AML/CFT effectiveness and compliance. Financial institutions are, therefore, required to put in place effective and efficient transaction monitoring programmes to facilitate the process. Although the types of transactions which could be used for money laundering are numerous, it is possible to identify certain basic features which tend to give reasonable cause for suspicion of money laundering.

This appendix, which lists various transactions and activities that indicate potential money laundering, is not exhaustive. It does reflect the ways in which money launderers have been known to operate.

Transactions or activities highlighted in this list are not necessarily indicative of actual money laundering if they are consistent with a customer's legitimate business. Identification of any of the types of transactions listed here should put financial institutions on enquiry and provoke further investigation to determine their true legal status.

2. SUSPICIOUS TRANSACTIONS "RED FLAGS"

(i) Potential Transactions Perceived or Identified as Suspicious

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

(b) Transactions involving shell banks/companies.

(c) Transactions with correspondents that have been identified as higher risk.

(d) Large transaction activity involving monetary instruments such as traveler's cheques, bank drafts, money order, particularly those that are serially numbered.

(e) 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.

(ii) Money Laundering Using Cash Transactions

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

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

(c) Frequent exchange of cash into other currencies.

(d) Customers who deposit cash through many deposits slips such that the amount of each deposit is relatively small, the overall total is quite significant.

(e) Customers whose deposits contain forged currency notes or instruments.

(f) Customers who regularly deposit cash to cover applications for bank drafts.

(g) Customers making large and frequent cash deposits but with cheques always drawn in favour of persons not usually associated with their type of business.

(h) Customers who request to exchange large quantities of low denomination banknotes for those of higher denominations.

(i) Branches of banks that tend to have far more cash transactions than usual, even after allowing for seasonal factors.

(j) Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

(iii) Money Laundering Using Financial Institutions

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

(a) Minimal, vague or fictitious information on the transaction provided by a customer that the financial institution is not in a position to verify.

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

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

(d) Customers maintaining multiple accounts at a financial institution or different financial institutions for no apparent legitimate reason or business rationale. The accounts may be in the same names or have different signatories.

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

(f) Accounts with large volumes of activity but low balances or frequently overdrawn positions.

(g) Customers making large deposits and maintaining large balances with no apparent rationale.

(h) Customers who make numerous deposits into accounts and soon thereafter request for electronic transfers or cash movement from those accounts to other accounts, perhaps in other countries, leaving only small balances. Typically, these transactions are not consistent with the customers' legitimate business needs.

(i) Sudden and unexpected increase in account activity or balance arising from deposit of cash and non-cash items. Typically, such an account is opened with a small amount which subsequently increases rapidly and significantly.

(j) Accounts that are used as temporary repositories for funds that are subsequently transferred outside the bank to foreign accounts. Such accounts often have low activity.

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

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

(m) Retail businesses which deposit many cheques into their accounts but with little or no withdrawals to meet daily business needs.

(n) Frequent deposits of large amounts of currency, wrapped in currency straps that have been stamped by other banks.

(o) Substantial cash deposits by professional customers into client, trust or escrow accounts.

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

(q) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

(r) Greater use of safe deposit facilities by individuals, particularly the use of sealed packets which are deposited and soon withdrawn.

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

(t) Large number of individuals making payments into the same account without an adequate explanation.

(u) High velocity of funds that reflects the large volume of money flowing through an account.

(v) An account of a license forex bureau that receives unusual deposits from third parties.

(w) An account operated in the name of an off-shore company with structured movement of funds.

(iv) Trade-Based Money Laundering

a. Over and under-invoicing of goods and services.

b. Multiple invoicing of goods and services.

c. Falsely described goods and services and “phantom” shipments whereby the exporter does not ship any goods at all after payments had been made, particularly under confirmed letters of credit.

d. Transfer pricing.

e. Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.

f. Items shipped are inconsistent with the nature of the customer’s normal business and the transaction lacks an obvious economic rationale.

g. Customer requests payment of proceeds to an unrelated third party.

h. Significantly amended Letters of Credit (L/C) without reasonable justification or changes to the beneficiary or location of payment.

(v) Lending Activity

a. Customers who repay delinquent loans unexpectedly.

b. A customer who is reluctant or refuses to state the purpose of a loan or the source of repayment or provides a questionable purpose and/or source of repayment.

c. Loans secured by pledged assets held by third parties unrelated to the borrower.

d. Loans secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties. Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.

e. Loans lack a legitimate business purpose, provide the bank with significant fees for assuming minimal risk, or tend to obscure the movement of funds (e.g. loans made to a borrower and immediately sold to an entity-related to the borrower).

(vi) Terrorist Financing "Red flags"

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

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

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

d. Large number of incoming or outgoing funds transfers takes place through a business account, and there appears to be no logical business or other economic

purpose for the transfers, particularly when this activity involves designated high-risk locations.

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

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

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

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

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

(vii) Other Unusual or Suspicious Activities

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

b. Employee fails to comply with approved operating guidelines, particularly in private banking.

c. Employee is reluctant to take a vacation.

d. Safe deposit boxes or safe custody accounts opened by individuals who do not reside or work in the institution’s service area despite the availability of such services at an institution closer to them.

e. Customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high value assets awaiting conversion to currency, for placement in the banking system.

f. Customer uses a personal account for business purposes.

g. Official Embassy business is conducted through personal accounts.

h. Embassy accounts are funded through substantial currency transactions.

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

APPENDIX D

Further Guidance on Accountable Institutions' Risk Assessment and Business/Customer Risk Rating

AML/CFT Risk Assessment and Rating — Overview

This document explains the concept of AIs' assessment and management of their ML/TF risks, including assignment of risk rating scores of business/customer ML/TF risks into the categories of "low risk", "medium risk", "medium-high risk" and "high risk". The notes relating to risk assessment, customer risk factors, geographic or country risk factors, product, service and delivery channel risk factors and risk variables are primarily sourced from the FATF Recommendation 1 on Risk Assessment and Recommendation 10 on Customer Due Diligence and the accompanying Interpretative Notes.

The same risk management principles that the AI uses in traditional operational areas should be applied to assessing and managing AML/CFT risk. A well-developed risk assessment and rating will assist in identifying the AI's AML/CFT risk profile and properly rating its business/customer ML/TF risk. Understanding the risk profile enables the AI to apply appropriate risk management processes to the

AML/CFT compliance program to mitigate risk. This risk assessment process enables management to better identify and mitigate gaps in the bank's controls.

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

Identification of Specific Risk Categories

The first step of the risk assessment process is to identify the customers, countries or geographic areas; and products, services, transactions or delivery channels unique to the AI. Although attempts to launder money, finance terrorism, or conduct other illegal activities through anAI can emanate from many different sources, certain customers, countries or geographic areas; and products, services, transactions or delivery channels may be more vulnerable or have been historically abused by money launderers and criminals. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered when the AI prepares its risk assessment. The differences in the way a AI interacts with the customer (face-to-face contact versus electronic banking) also should be considered. Because of these factors, risks will vary from one bank to another.

Product, service, transaction or delivery channel risk factors:

Certain products and services offered by banks may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Some of these products and services are listed below, but the list is not all inclusive:

Private banking.

Anonymous transactions (which may include cash).

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

Payment received from unknown or un-associated third parties

Customer risk factors

FATF has set out the categories of PEPs, correspondent banking and wire transfers as categories which are considered as high-risk or which require specific due diligence measures. In addition, banks should consider the following customer risk factors:

The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).

Non-resident customers.

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

Companies that have nominee shareholders or shares in bearer form.

Business that are cash-intensive.

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

Country or geographic risk factors:

It is essential for AI's AML/CFT compliance programs that they identify geographic locations that may pose a higher risk. AIs should understand and evaluate the specific risks associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not necessarily determine a customer's or transaction's risk level, either positively or negatively.

International higher-risk geographic locations generally include:

Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.

Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.

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

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

Analysis of Specific Risk Categories and Risk Variables

The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess AML/CFT risk. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, anAI should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures.

Examples of such variables include:

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

Developing the Bank's AML/CFT Compliance Program Based Upon Its Risk Assessment

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

Audit should review the AI's risk assessment for reasonableness. Additionally, management should consider the staffing resources and the level of training necessary to promote adherence with these policies, procedures, and processes. For those AIs that assume a higher-risk AML/CFT profile, management should provide a more robust AML/CFT compliance program that specifically monitors and controls the higher risks that management and the board have accepted.

Consolidated AML/CFT Compliance Risk Assessment

AIs that implement a consolidated or partially consolidated AML/CFT compliance program should assess risk both individually within business lines and across all activities and legal entities. Aggregating AML/CFT risks on a consolidated basis for larger or more complex organizations may enable an organization to better identify risks and risk exposures within and across specific lines of business or product categories. Consolidated information also assists senior management and the board of directors in understanding and appropriately mitigating risks across the organization.

To avoid having an outdated understanding of the AML/CFT risk exposures, the bank should continually reassess its AML/CFT risks, review its risk rating of customers and communicate with business units, functions, and legal entities. The identification of a AML/CFT risk or deficiency in one area of business may indicate concerns elsewhere in the organization, which management should identify and control.

Updating of AIs Risk Assessment and Rating

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

APPENDIX E

Guidance on Enhanced Due Diligence (EDD)

This guideline assists AIS to conduct enhanced customer due diligence (EDD) on customers under the Anti-Money Laundering and Countering Financing of Terrorism acts, Act 749 as amended and Act 762 as amended respectively.

EDD is required when you consider, based on your AML/CFT risk assessment (risk assessment), that the level of risk involved is high.

EDD requires the collection and verification of the same identity information that is required for standard customer due diligence. However, when undertaking EDD, you may need to use increased or more sophisticated measures to do this. EDD also requires the collection and verification of information relating to the source of wealth (SoW) or source of funds (SoF) of your customer.

Your AML/CFT programme (programme) must outline how your business will determine when EDD is required for a customer and when other types of customer due diligence are permitted.

A risk-based approach allows you some flexibility in the steps you take when conducting EDD. Your risk assessment and programme will determine the amount of time and effort you spend on EDD.

Customer due diligence (CDD) is a cornerstone of your AML/CFT programme. CDD is the process through which you develop an understanding of your customers and the ML/TF risks they pose to your business.

In some higher ML/TF risk circumstances an increased level of CDD is required. This is known as enhanced CDD or “EDD”. As part of standard CDD you must obtain sufficient information to determine whether you require EDD on your customer.

EDD is required for certain types of customers and some transactions or activities. This includes situations where you consider (based on your risk assessment) that the level of risk involved is such that EDD should apply.

For instance, EDD helps you:

- Determine whether complex beneficial ownership structures are legitimate and intended to facilitate business or if they are deliberately complicated to hinder investigation and conceal the identity of the beneficial owners.
- Determine whether a customer's source of wealth or funds are legitimately derived, or intended for legitimate use, or whether there are reasonable grounds to suspect it may be the proceeds of crime.
- Distinguish between a customer that has a higher risk profile but is not involved in ML/TF, as opposed to a customer whose transactions or activities may be linked to ML/TF.

Customers that **must** have EDD are:

- A trust or another vehicle for holding personal assets
- A non-resident customer from a country that has insufficient AML/CFT systems or measures in place
- A company with nominee shareholders or shares in bearer form,
- A **politically exposed person (PEP)**
- Customers seeking to conduct a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose
- Any other customer that you assess (based on your risk assessment and standard CDD) to be of high ML/TF risk,
- Customers seeking to use new and developing technologies or products that might favour anonymity.

EDD and Source of Wealth (SoW) and Source of Funds (SoF)

In many cases, SoW or SoF information and documents required for EDD will be readily available and quickly provided by your customer. In other cases, you may need to inquire further into complex ownership or control structures, or you may need to examine the origins of your customer's wealth in detail.

Establishing your customer’s SoW or SoF is a core requirement of EDD. You must collect information relating to the SoW or SoF of your customer and you must, according to the level of risk involved, take reasonable steps to verify that information.

What is the difference between SoW and SoF?

Your customer's SoW is the origin of their entire body of assets. This information gives an indication of the amount of wealth your customer would be expected to have and a picture of how they acquired it.

Your customer's SoF is more narrowly focused. It is the origin of the funds used for the transactions or activities that occur within the business relationship with you. This also applies for an occasional transaction or activity.

In circumstances where you are establishing or updating your customer's risk profile you may need to collect and verify information regarding their SoW. However, when EDD is triggered by circumstances involving transactions or activities, you may need to focus more specifically on the SoF.

It is important to remember that your customer's SoW and SoF do not exist in isolation of each other. In a situation where an individual transaction is disproportionately large compared to your knowledge of a customer's wealth, this should trigger a more detailed examination of that transaction or activity. It is for you to determine when to examine your customer's SoW, when to examine their SoF, or when to examine both.
ld set out how you will do this.

EDD and Politically Exposed Persons

A PEP is a person who has held a prominent. The term PEP includes their relatives and close associates, which are sometimes called RCAs. It also includes people who have beneficial ownership of legal entities or arrangements existing to benefit PEPs.

You must as soon as practicable after establishing a business relationship (or occasional activity or transactions) take reasonable steps to determine if your customer, or their beneficial owner, is a PEP.

The AI must ensure that adequate and effective procedures, policies and controls are in place to identify customers that are PEPs. This will depend on the size, nature and complexity of your business and the likelihood of having a PEP as a customer.

You must conduct EDD on a customer who is a PEP.[50] In addition, your senior management (if applicable) must approve continuing the business relationship with a PEP You must obtain and take reasonable steps to verify the PEP's SoW or SoF.

According to the level of risk involved, it may be appropriate, as part of your EDD, to use internet/media searches and publicly available reports to check if your customer is a PEP. With larger or more complex businesses you may want to consider using the services of a third-party provider and commercially available databases to screen for PEPs.

For ongoing CDD and account monitoring of a higher risk PEP, you may need to undertake ongoing media monitoring or increase transaction monitoring activity. You may wish to conduct more frequent EDD reviews and submit quicker, more thorough STRs.

Key EDD questions to consider are:

- Is the PEP's transaction/activity in line with expectations?
- Is the PEP's identity data, address, employment, SoW or SoF and relatives and close associates status up to date?
- Are there any unexplained changes to the PEP's details?
- If the PEP's net worth has grown substantially in a short amount of time, do you have a clear explanation for the sudden growth?
- Have you sought clarification from the PEP where necessary and updated their details?