# 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 ACCOUNTABLE INSTITUTIONS

DECEMBER, 2022

# TABLE OF CONTENTS

## LIST OF ACRONYMS & ABBREVIATION

| | | |
|---|---|---|
| **AI** | - | Accountable Institution (Bank of Ghana Licensed Institutions) |
| **AML** | - | Anti-Money Laundering |
| **AML/CFT&P** | - | Anti-Money Laundering, Combating the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction |
| **AML/CFT/CPF** | - | Anti-Money Laundering, Combating the Financing of Terrorism and Counter Proliferation Financing |
| **AMLRO** | - | Anti-Money Laundering Reporting Officer |
| **ATM** | - | Automated Teller Machine |
| **AU** | - | African Union |
| **BOG** | - | Bank of Ghana |
| **CDD** | - | Customer Due Diligence |
| **CFT** | - | Combating the Financing of Terrorism |
| **CPF** | - | Counter Proliferation Financing |
| **CTR** | - | Cash Transaction Report |
| **DNFBPs** | - | Designated Non-Financial Businesses and Professions |
| **ECOWAS** | - | Economic Community of West African States |
| **EDD** | - | Enhanced Due Diligence |
| **ERMF** | - | Enterprise Risk Management Framework |
| **FA** | - | Foreign Account |
| **FATF** | - | Financial Action Task Force |
| **FIC** | - | Financial Intelligence Centre |
| **KYC** | - | Know Your Customer |
| **KYE** | - | Know Your Employee |
| **LEAs** | - | Law Enforcement Agencies |
| **MDAs** | - | Ministries, Departments and Agencies |
| **MMDAs** | - | Metropolitan, Municipals and District Assemblies |
| **ML** | - | Money Laundering |
| **ML/TF&PF** | - | Money Laundering, Terrorism Financing and Proliferation Financing |
| **MVTS** | - | Money or Value Transfer Service |
| **NGO** | - | Non-Governmental Organisation |
| **NIA** | - | National Identity Authority |
| **NIC** | - | National Insurance Commission |
| **NPO** | - | Non-Profit Organisation |
| **NRA** | - | National Risk Assessment |
| **OFAC** | - | Office of Foreign Assets Control |
| **PEP** | - | Politically Exposed Person |
| **PF** | - | Proliferation Financing |
| **RO** | - | Religious Organisation |

| | | |
|---|---|---|
| **SAR** | - | Suspicious Activity Report |
| **SDD** | - | Simplified Due Diligence |
| **SEC** | - | Securities and Exchange Commission |
| **STR** | - | Suspicious Transaction Report |
| **TF** | - | Terrorism Financing |
| **UNSCRs** | - | United Nations Security Council Resolutions |
| **VAs** | - | Virtual Assets |
| **VASPs** | - | Virtual Assets Service Providers |

## FOREWORD

The world has experienced phenomenal growth in financial services over the last couple of decades. This globalisation 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, Terrorist Financing and Proliferation Financing (ML/TF&PF) perpetuated by both formal and underground economies.

The emergence of technology and the increasing use of digital channels in Ghana, has made it easier for unlawful activities to thrive. To help combat ML/TF&PF, AIs need to have robust Anti-Money Laundering, Combating the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction (AML/CFT&P) regime.

ML/TF&PF affect whole economies, and consequently impact negatively on the economic, political and social development, posing serious challenges across the globe.

The need for countries to have strong anti-money laundering mechanisms, coupled with the enhancement of transparent financial integrity cannot therefore be over-emphasised. Ghana is determined to maintain a sound financial system and to join global efforts to minimise the scourge of ML/TF&PF.

In pursuit of the above goal and in order to avoid the risk of under-regulation, the Bank of Ghana (BOG) and the Financial Intelligence Centre (FIC) hereby provide this Guideline to assist Bank of Ghana Licensed Institutions design and implement their respective AML/CFT&P compliance regime.

This Guideline is made in pursuance of sections 52 and 61 of the Anti-Money Laundering Act, 2020 (Act 1044) and section 92(2)(a)(vii) of the Banks and Specialized Deposit-Taking Institutions, Act 2016, (Act 930).

GOVERNOR
BANK OF GHANA

CHIEF EXECUTIVE OFFICER
FINANCIAL INTELLIGENCE CENTRE

# INTRODUCTION

The enactment of the now repealed Acts:- Anti-Money Laundering Act, 2008 (Act 749) and Anti-Money Laundering (Amendment) Act, 2014 (Act 874), together with the Anti-Terrorism Act, 2008 (Act 762), Anti-Terrorism (Amendment Act), 2012 (Act 842), Anti-Terrorism (Amendment Act), 2014 (Act 875), Anti-Money Laundering Regulations, 2011 (L.I.1987) and the subsequent passage of the Anti-Money Laundering Act, 2020 (Act 1044) has intensified Ghana's efforts towards the fight against money laundering, terrorism and proliferation financing (ML/TF&PF).

The purpose of Act 1044 will not be realized unless there is an 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 accountable institutions (AIs). It is against this background that the BOG and FIC have developed this Guideline for AIs.

This Guideline has incorporated essential elements of Act 1044, Act 762 as amended and Regulations, relevant Financial Action Task Force (FATF) Recommendations, the sound practices of the Basel Committee on Banking Supervision and other international best practices on Anti-Money Laundering and the Combating of the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction (AML/CFT&P).

To provide a compliance regime and to avoid ambiguity, the provision on KYC procedures are also provided to assist AIs in their implementation of this Guideline.

## OBJECTIVE OF THIS GUIDELINE

This Guideline is being issued pursuant to section 52 of Act 1044 and intended to assist AIs to:

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

## DEFINITIONS

Money Laundering (ML) is defined as the process where criminals attempt to conceal the illegal origin and/or illegitimate ownership of property and assets that are proceeds of their criminal activities. It is, thus, a derivative crime.

Terrorism Financing (TF) is defined here to include both legitimate and illegitimate money characterised by concealment of the origin or intended criminal use of the funds.

Terrorist financing offences shall 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.

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.

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.

Proliferation Financing (PF) is defined by FATF as "the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations."

## SCOPE OF UNLAWFUL ACTIVITIES

AIs 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, 2020 (Act 1044) and Anti-Terrorism Act 2008 (Act 762) as amended and Criminal and Other Offences Act, 1960 (Act 29).

## OVERVIEW OF THIS GUIDELINE

ML/TF&PF are global phenomena and there has been growing recognition in recent times, and indeed well-documented evidence, that both ML/TF&PF pose major threats to international peace and security which could seriously undermine Ghana's development and progress.

Consequently, Ghana has made concerted efforts to check these crimes. AIs, in particular, have come under sustained regulatory pressure to improve their monitoring and surveillance systems with a view to detecting, preventing, and responding effectively to the threat of ML/TF&PF.

This Guideline covers among others the following key areas of AML/CFT&P policy:

i. Anti-Money Laundering Reporting designation and duties;
ii. the need to co-operate with the supervisory authority;
iii. customer due diligence;
iv. monitoring and reporting of suspicious transactions /activities;
v. statutory reporting requirements;
vi. record keeping; and
vii. AML/CFT&P employee training programme.

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

AIs are also reminded that AML/CFT&P policies governing their operations should not only prescribe money laundering and predicate offences but also prescribe sanctions for non-compliance with the relevant AML/CFT&P requirements. It is, therefore, in the best interest of the institutions to entrench a culture of compliance which would be facilitated by this Guideline.

This revised AML/CFT&P Guideline comes into effect from the date of issue. All AIs must conduct a gap analysis of their AML/CFT&P policies against the requirements of this Guideline and submit the updated AML/CFT&P policies and the gap analysis report to Bank of Ghana and the Financial Intelligence Centre.

AIs will be required to conduct their AML/CFT&P audits using this revised AML/CFT&P Guideline.

## SANCTIONS FOR NON-COMPLIANCE

Failure to comply with the provisions contained in this Guideline shall attract appropriate administrative sanctions as prescribed in the BOG/FIC Administrative Penalties Guideline.

This Guideline is structured as follows;

Part A – Obligations and co-operations among competent authorities
Part B – Elements for effective AML/CFT&P Regime
Part C – Further Guidance on KYC/CDD/EDD Procedures
Appendices
References

# PART A - OBLIGATIONS AND CO-OPERATIONS AMONG COMPETENT AUTHORITIES

## 1.0 AML/CFT&P OBLIGATIONS OF BANK OF GHANA

1. In compliance with sections 52(1) and (5) of Act 1044, Bank of Ghana is hereby designated as a supervisory body to ensure supervision and enforcement of compliance by AIs in relation to AML/CFT&P requirements.

2. Bank of Ghana shall carry out the following functions:
   i. adopt a risk-based approach in supervising and monitoring AIs;
   ii. monitor and periodically assess the level of ML/TF&PF risk of the AIs;
   iii. carry out an examination of AIs based on the Bank of Ghana risk-assessment framework.
   iv. request production of, access to, the records, documents, or any other information relevant to the supervision and monitoring of AIs;
   v. develop guidelines, directives or notices to ensure compliance;
   vi. provide feedback on compliance with obligations under the Act 1044 by AIs;
   vii. approve the appointment of the AMLRO of AIs; and
   viii. undertake any other activity necessary for assisting AIs to understand their obligations under Act 1044.

## 1.1 CO-OPERATION AND INFORMATION SHARING WITH COMPETENT AUTHORITIES

1. In accordance with section 52(5)(f) of Act 1044, Bank of Ghana, shall co-operate and share information with any other competent authorities in the performance of functions and the exercise of powers under Act 1044.

2. In this regard, the Bank of Ghana shall;
   i. initiate and act on a request from a foreign counterpart and notify FIC immediately;
   ii. impose administrative penalties for non-compliance with Act 1044;
   iii. issue Guidelines/Notices/Directives to ensure compliance with Act 1044;
   iv. perform any other function as may be required to ensure compliance with Act 1044;
   v. during an examination, require an employee, officer, or agent of AIs to:
      a. answer questions relating to the records and documents of that AIs; and
      b. provide any other information that Bank of Ghana may require for the purpose of the examination.

## 1.2 ACCOUNTABLE INSTITUTION'S CO-OPERATION WITH COMPETENT AUTHORITIES

1. AIs 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.

2. AI's procedures for responding to authorized requests for information on ML/TF&PF shall be such that it can:
   i. immediately search the institution's records to enable it to respond to the request;
   ii. report promptly to the requesting authority the outcome of the search; and
   iii. protect the security and confidentiality of such requests.

3. Notwithstanding, a competent authority shall have access to information in order to perform its functions in combating ML/TF&PF. This shall include the sharing of information between competent authorities, either domestically or internationally, and also the sharing of information between AIs.

# PART B - ELEMENTS FOR EFFECTIVE AML/CFT&P REGIME

## 2.0 AML/CFT&P INSTITUTIONAL POLICY FRAMEWORK

1. All AIs shall develop and implement policies indicating their commitment to comply with AML/CFT&P obligations under Act 1044, this Guideline and other relevant regulations to prevent ML/TF&PF risks.

2. AIs shall formulate and implement internal rules, procedures and other controls that will deter criminals from using their facilities for ML/TF&PF activities and shall ensure compliance with the relevant laws and regulations.

## 2.1 ASSESSING AML/CFT&P RISK MANAGEMENT FRAMEWORK AND APPLYING A RISK–BASED APPROACH

1. The AI's AML/CFT&P risk management framework must be aligned and integrated with their overall Enterprise Risk Management Framework (ERMF). AIs are required to take appropriate steps to identify, assess and understand their ML/TF&PF risks in relation to their customers, countries or geographical areas, products and services, transactions or delivery channels in a form of an AML/CFT&P framework to guide the staff in the organization.

2. In assessing ML/TF&PF risks, AIs are required to have the following:
   i. develop and implement AML/CFT&P risk assessments framework and obtain Board approval before implementation;
   ii. Conduct AML/CFT&P risk assessment and prepare a report for Board approval;
   iii. Consider all the relevant risk factors before determining the level of overall risk, the appropriate level and type of mitigation to be applied;
   iv. Keep the assessment up-to-date through a periodic review within a two-year cycle. However, in the event of a significant occurrence, the AI shall review and update its risk assessment framework;
   v. review AML/CFT&P framework and identify new areas of potential ML/TF&PF risks and shall provide periodic risk assessment report to BOG and FIC;
   vi. design additional procedures and mitigants in their AML/CFT&P operational Guidelines for the newly identified risks;
   vii. submit to the BOG and FIC not later than 15th January of the following year a report containing the new/additional AML/CFT&P specific risks identified with their commensurable mitigants; and
   viii. required to conduct additional risk assessment as and when required by the BOG.

AIs shall be guided by the results of the National Risk Assessment (NRA)Reports in conducting their respective risk assessments.

## 2.2 AML/CFT&P RISK ASSESSMENT FOR NEW PRODUCTS

**2.2.1.1** AIs shall review, identify and record areas of potential ML/TF&PF risks and submit to BOG for approval before new products, practices and technologies are launched.

**2.2.1.2** AIs are therefore required to review their AML/CFT&P risk frameworks from time to time with a view to determining their adequacy and identifying other areas of potential risks when introducing new products, practices and technologies.

Further Guidance on Risk Assessment and Risk Rating is provided in the Appendix D.

## 2.3 AML/CFT&P GOVERNANCE FRAMEWORK

### 2.3.1 CULTURE OF COMPLIANCE

1. AIs shall have a comprehensive AML/CFT&P compliance programme 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 the AI being used to launder the proceeds of crime but also provide protection against unlawful activities as well as reputational and financial risks.

### 2.3.2 ROLE OF THE BOARD OF DIRECTORS (BOARD)

1. The Board has ultimate responsibility for ensuring the effectiveness of the AML/CFT&P compliance programme. In this regard, the Board's oversight in respect of AML/CFT&P shall align with international best practices, including the Bank of Ghana's Corporate Governance Directive. The Board must ensure that there is documented evidence of its oversight function, for example, in minutes of meetings of the Board (or committees of the Board).

2. Key responsibilities of the Board include:
   i. Approving the appointment of the AMLRO;
   ii. Approving AML/CFT&P policy/manual;
   iii. Approving the AML/CFT&P compliance programme, training programme, compliance reports, Internal Risk Assessment Framework;
   iv. Ensuring the establishment of appropriate mechanisms to periodically review key AML/CFT&P policies and procedures to ensure their continued relevance in line with changes in the AI's products and services and to address new and emerging ML/TF&PF risks;

v. Ensuring the establishment of an appropriate AML/CFT&P risk management framework with clearly defined lines of authority and responsibility for AML/CFT&P and effective separation of duties between those implementing the policies and procedures and those enforcing the controls;

vi. Ensuring that the Board receives the requisite training on AML/CFT&P generally as well as on the institution's specific AML/CFT &P risks and controls at least once a year;

vii. Ensuring receipt of regular and comprehensive reports on the AI's AML/CFT&P function from the AMLRO for its information and necessary action including but not limited to:

a. Remedial action plans if any, to address the results of independent audits (either internal or external); regulatory reports received from the Bank of Ghana or other regulators on its assessment of the institution's AML/CFT&P programme;
b. results of compliance testing and self-identified instances of non-compliance with AML/CFT&P requirements;
c. Recent developments in AML/CFT&P laws and regulations and their implications if any, to the AIs;
d. Details of recent significant risk events and potential impact on the AI; and
e. Statistics of statutory report to the FIC, orders from law enforcement agencies, refused or declined business and de-risked relationships.

AIs shall submit copies of the approved AML/CFT&P policy and manual to the BOG within five (5) working days

### 2.3.3 ROLE OF SENIOR MANAGEMENT

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

2. Senior Management must review policies and procedures periodically for consistency with the AI's business model, product and service offerings, and risk appetite. Attention should be paid to **new and developing technologies** and AIs

should identify and assess the ML/TF&PF risks arising from **new products/services and delivery channels; new business practices, new delivery mechanisms and new or developing technologies for new and pre-existing products; and put measures in place to manage and mitigate such risks**. Risk assessments should take place prior to the launch or use of such products/services, channel, business practices and technologies.

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

### 2.3.4 ROLE AND DUTIES OF ANTI – MONEY LAUNDERING REPORTING OFFICER (AMLRO)

1. AIs shall appoint an Anti-Money Laundering Reporting Officer (AMLRO) of a key managerial level (as specified in section 156 of Act 930 and the BOG Corporate Governance Directive) and of minimum Senior Management grade/status or equivalent. This appointment shall be in accordance with section 50(1)(b) of the Anti-Money Laundering Act, 2020 (Act 1044) and Regulation 5(1) of L.I. 1987.

2. The AMLRO shall report to the Board or a Sub-Committee of the Board to ensure operational independence.

3. The AMLRO must have sufficient authority, independence and seniority to be able to effectively carry out his duties in accordance with the Act 1044 and this Guideline. The identity of the AMLRO must be treated with the strictest confidence by the employees of the AI. The AI shall ensure that the AMLRO acquires professional qualification in anti-money laundering and financial crime.

4. The duties of the AMLRO shall include but not limited to the following:

i. Develop written AML/CFT&P policies and procedures that are kept up to date and approved by the Board;
ii. Have oversight of the AML/CFT&P control activity in all relevant business areas for the purposes of establishing a reasonable risk level consistent across the AI;
iii. Keep the AML/CFT&P programme current relative to the institution's identified inherent risks and give consideration to local and international developments in ML/TF&PF;
iv. Receive and vet suspicious (unusual) transaction/activity reports from the staff;
v. Conduct regular risk assessments of the inherent ML/TF&PF risks including timely assessments of new products, services and business acquisition initiatives to identify potential ML/TF&PF risks and develop appropriate control mechanisms;
vi. File suspicious, Electronic Currency, Politically Exposed Persons, Cash Transaction Reports and other relevant regulatory reports with the BOG and FIC (where applicable);
vii. Conduct periodic assessments of AML/CFT&P control mechanisms to ensure their continued relevance and effectiveness in addressing changing ML/TF&PF risks, assess operational changes, including the introduction of new technology and processes to ensure that ML/TF&PF risks are addressed;
viii. Ensure systems, resources, including those required to identify and report suspicious transactions and suspicious attempted transactions, are appropriate in all relevant areas of the institution;
ix. Ensure that ongoing training programmes on ML/TF&PF are current and relevant and are carried out for all employees, senior management and the Board;
x. Ensure that systems and other processes that generate information used in reports to Senior Management and the Board are adequate and appropriate, use reasonably consistent reporting criteria, and generate accurate information;
xi. Report pertinent information to the Board and Senior Management regarding the adequacy of the AML/CFT&P framework or any associated issues; and
xii. Serve both as a liaison officer with the BOG and the FIC and a point-of-contact for all employees on issues relating to ML/TF&PF.

AIs shall ensure that the AMLRO has access to all information that may be of assistance to him/her in consideration of a suspicious or unusual transaction/activity report.

### 2.3.5 INTERNAL CONTROLS, COMPLIANCE AND AUDIT

1. AIs shall establish and maintain internal procedures, policies and controls to prevent ML/TF&PF and to communicate these to their employees. These procedures, policies and controls should cover the CDD, record retention, the detection of unusual and suspicious transactions/activities, the reporting obligation, among other things.

2. The AMLRO and appropriate staff are to have timely access to customer

identification data, CDD information, transaction records and other relevant information.

3. AIs are therefore required to develop programmes against ML/TF&PF 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 programmes to ensure that employees are kept informed of new developments, including:
      a. Information on current ML/TF&PF techniques, methods and trends;
      b. Clear explanation of all aspects of AML/CFT&P laws and obligations; and
      c. Requirements concerning CDD and suspicious transaction/activity reporting.
   iii. Adequately resourced and independent audit function to test compliance with the procedures, policies and controls.

AIs shall put in place a structure that ensures the operational independence of the AMLRO.

### 2.3.6 TESTING FOR THE ADEQUACY OF THE AML/CFT&P COMPLIANCE FUNCTION

1. AIs shall make a policy commitment and subject their AML/CFT&P compliance function to independent-testing.

2. It is important that these reviews are performed by auditors (internal or External) who have had appropriate AML/CFT&P training and experience in respect of ML/TF&PF risk and an appropriate level of knowledge of the regulatory requirements and guidelines. It is required that the auditor shall determine the adequacy, completeness and effectiveness of the AML/CFT&P compliance function.

3. Where an AIs fails to engage the services of an auditor, the BOG shall appoint a competent professional to perform those functions and the costs shall be borne by the AI.

4. The report of the independent testing/review of AML/CFT&P compliance function shall be submitted to the BOG and FIC not later than January 15 of every financial year.

5. Any identified weaknesses or inadequacies should be promptly addressed by the AI and subsequently provide update to BOG and FIC.

## 2.4 CUSTOMER DUE DILIGENCE PROGRAMME

1. AIs must develop and implement risk-based policies and procedures to mitigate the ML/TF&PF risks identified in their business and customer risk assessments. The risk assessment framework should identify which customers or categories of customers present higher risk and therefore require the application of enhanced due diligence (EDD). Similarly, where the AIs determine that a customer or a category of customers presents low risk, simplified due diligence (SDD) should be applied. Where SDD measures are applied on the basis of an assessment of low ML/TF&PF risk, the customer due diligence (CDD) policies and procedures should clearly articulate the rationale and the applicable measures to be undertaken.

2. CDD is the identification and verification of both the customer and beneficiary including but not limited to continuous monitoring of the business relationship with the AIs. AIs are not permitted to operate anonymous accounts or accounts in fictitious names.

### 2.4.1 CONDUCTING CUSTOMER DUE DILIGENCE

1. AIs shall undertake customer due diligence (CDD) per section 30 of Act 1044 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;
   c. Acquisition of prepaid credit cards;
   d. There is a suspicion of ML/TF&PF regardless of any exemptions or any other thresholds referred to in this Guideline;
   e. There are doubts about the veracity or adequacy of previously obtained customer identification data;
   f. The following transactions are however, exempted:
      i. Any transfer flowing from a transaction carried out using a credit or debit card on a terminal other than the terminal of the issuing AI's card so long as the credit or debit card number accompanying such transfers flows from the transactions such as withdrawals from a bank account through an ATM, cash advances from a credit card or payment for goods.
      ii. AI-to-AI transfers and settlements on their own behalf.

### 2.4.2 CUSTOMER DUE DILIGENCE PROCEDURES (IDENTIFICATION AND VERIFICATION)

1. AIs shall identify their customers and verify the customers' identities using the Ghana Card as the sole identifier for all financial transactions. All AIs are required to carry out and complete CDD procedures in this Guideline. However, in reasonable circumstances, AIs can apply the CDD procedures on a risk-based approach.

2. Types of customer information to be obtained and identification data to be used

to verify the information are provided in the Appendix B.

In respect of customers that are legal persons or legal arrangements, AIs 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
iii. where applicable, request and verify any additional license (or statutory certification) from a competent authority or similar evidence of establishment or existence and any other relevant information.

3. AIs 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.

4. AIs 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 AI shall take reasonable steps to obtain sufficient identification data and to verify the identity of that other person as pertains in (a) above.

5. AIs 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), the AI shall apply a risk-based approach to identify and verify the identity of the shareholders of such a public company.

6. AI shall obtain information on the purpose and intended nature of the business relationship of their potential customers.

7. AIs shall conduct ongoing due diligence on the business relationship as stated by the customers above.

8. The ongoing due diligence above includes scrutinizing the transactions undertaken by the customer throughout the course of the AI customer relationship to ensure that the transactions being conducted are consistent with the AI's knowledge of the customer, its business and risk profiles, and the source of funds (where necessary).

9. In compliance with the above, AIs shall develop or acquire automated monitoring tools to monitor all transactions aimed at detecting suspicious transactions by their customers in real time or by close of day.

10. AIs 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.

11. AIs shall screen all customers (existing and new customers) at onboarding and periodically against all domestic and international sanctions lists.

### 2.4.3 TIMING OF VERIFICATION

1. AIs 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.

2. AIs 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; and
   ii. it is essential not to interrupt the normal business conduct of the customer; and the ML/TF&PF risks can be effectively managed.

3. Examples of situations where it may be essential not to interrupt the normal conduct of existing 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; and
   iii. 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.

4. Where a customer is permitted to utilize the business relationship prior to verification, AIs 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.

### 2.4.4 FAILURE TO COMPLETE CDD

1. The AIs which is unable to perform requirements under this Guideline:
   i. shall not open the account, commence business relationship or perform the transaction; and
   ii. shall submit a Suspicious Activity Report (SAR)/Suspicious Transaction Report (STR) to the Financial Intelligence Centre (FIC) within twenty-four hours.

2. The AIs that has already commenced the business relationship as indicated in this Guideline shall terminate the business relationship immediately and submit STR/SAR to the Financial Intelligence Centre (FIC) within twenty-four hours.

### 2.4.5 EXISTING CUSTOMERS

1. AIs shall apply CDD/EDD 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.

2. The appropriate time to conduct CDD/EDD by AIs 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.
   v. in the absence of the above, AIs shall take appropriate steps to update customer records within two (2) years cycle.

3. The AIs shall properly identify the customer in accordance with the criteria above. The customer identification records should be made available to the AMLRO, other appropriate staff and competent authorities as and when is needed.

### 2.4.6 NEW BUSINESS FOR EXISTING CUSTOMERS

1. When an existing customer closes one account and opens another or enters into a new agreement to purchase products or services, the AI shall apply a risk-based approach in the CDD/EDD procedures. This is particularly important:
   a. if there was an existing business relationship with the customer and identification evidence had not previously been obtained;
   b. or if there had been no recent contact or correspondence with the customer within the past twenty-four (24) months; or
   c. when a previously dormant account is re-activated.

2. 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 section 32 of Act 1044.

### 2.4.7 RISK-BASED CDD

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

## 2.5 LOW RISK CUSTOMERS, TRANSACTIONS OR PRODUCTS

1. AIs shall apply reduced or simplified measures where there are low risks. There are low risks in circumstances where the risk of ML/TF&PF is low, where information on the identity of the customer and the beneficial owner of a customer is publicly available or where adequate checks and controls exist elsewhere in other public institutions. In circumstances of low risk, AIs shall apply the simplified or reduced CDD procedures when identifying and verifying the identity of their customers and the beneficial owners.

2. SDD procedures shall not be applied to a customer whenever there is suspicion of ML/TF&PF or specific high-risk scenarios. In such a circumstance, enhanced due diligence is mandatory.

3. Examples of low risk customers include but not limited to:
   a. AIs - provided they are subject to requirements for the AML/CTF&P which are consistent with the provisions of this Guideline;
   b. Public companies (listed on a stock exchange) that are subject to regulatory disclosure requirements;
   c. Life insurance policies where the annual premium and single monthly premium are within the threshold determined by National Insurance Commission (NIC);
   d. Insurance policies for pension schemes if there is no surrender-value clause and the policy cannot be used as collateral;
   e. 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;
   f. Refugees and asylum seekers; and
   g. Any other low risk as may be determined by the National Risk Assessment findings.

## 2.6 HIGH-RISK CATEGORIES OF CUSTOMERS

1. AIs shall perform enhanced due diligence (EDD) for high risk categories of customers, business relationship or transaction. AIs are to adopt EDD procedures on a risk sensitive basis. In adopting the EDD procedures in determining the risk profile, AIs shall have regard to the type of customer, product, transaction, the location of the customer and other relevant factors.

   Examples of high-risk customer categories include but not limited to:

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

## 2.7 SPECIFIC HIGH-RISK CUSTOMERS, ENTITIES, LOCATIONS OR TRANSACTIONS

### 2.7.1 POLITICALLY EXPOSED PERSONS (PEPs)

1. 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 persons who are or have been entrusted with a prominent public function by an international organization.

   Examples of PEPs include but are not limited to;

   i. Heads of State or Government;
   ii. Ministers of State;
   iii. Members of Parliament (both local or foreign);

iv. Politicians (including High ranking political party officials);
v. Ministries, Department and Agencies (MDAs);
vi. Metropolitans, Municipals and District Assemblies (MMDAs) and other public institutions;
vii. High ranking political party officials (National, Regional, District and Constituency Executives etc.);
viii. Legal entity belonging to a PEP;
ix. Senior public officials;
x. Senior Judicial officials;
xi. Senior Security officials appointed by Head of State or Government;
xii. Chief executives and Board Members of state-owned companies/corporations (both local and foreign);
xiii. Family members or close associates of PEPs; and
xiv. Traditional Rulers.

2. AIs are required to have appropriate risk-management systems and procedures to identify when their customer (or the beneficial owner of a customer) is a PEP and to manage any elevated risks. Business relationships with the family and known close associates of a PEP should also be subjected to greater scrutiny. These requirements are intended to be preventive and should not be interpreted as stigmatising all PEPs as being involved in criminal activity.

3. AIs shall, in addition to performing EDD procedures, put in place appropriate risk management systems to determine whether a potential customer or existing customer or the beneficial-owner is a PEP.

4. AIs shall obtain senior management approval before they establish a business relationship with PEP and all other high-risk customers.

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

6. AIs shall take reasonable measures to establish the source of wealth and the sources of funds of customers and beneficial-owners identified as PEPs or high-risk and report all anomalies immediately to the FIC and other relevant authorities.

7. AIs in business relationships with PEPs or high-risk customers are required to conduct enhanced ongoing monitoring of that relationship.

8. AIs shall report to the FIC all transactions conducted by PEPs.

9. In the event of any transaction/activity that is abnormal, AIs are required to flag the account and file an STR/SAR immediately to the FIC.

### 2.7.2 CROSS-BORDER CORRESPONDENT BANKING

1. 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.

2. 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.

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

4. Where a correspondent relationship involves the maintenance of payable through- accounts, the AI shall:
   i. perform EDD on its customers that have direct access to the accounts of the correspondent bank;
   ii. provide relevant EDD information and customers identification upon request to the correspondent bank; and
   iii. be prohibited from entering into or continuing, correspondent banking relationships with shell banks. AIs are required to satisfy themselves that correspondent banks do not permit their accounts to be used by shell banks.

### 2.7.3 SHELL BANKS

1. These are banks which have no physical presence in any country. AIs are prohibited from 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.

### 2.7.4 NEW TECHNOLOGIES AND NON-FACE-TO-FACE TRANSACTIONS

1. The accelerated development and increased functionality of new technologies to provide financial services create challenges for countries and private sector AIs in ensuring that these types of payment products and services are not misused for ML/TF&PF purposes. Virtual currencies and various forms of electronic money, for example, are emerging as potential alternatives to traditional financial services.

2. AIs must assess the ML/TF&PF risks associated with the introduction of:
   i. New financial products and services and/or changes to existing products and services;
   ii. New or developing technologies used to provide products and services.

3. To achieve paragraph 2 above;
   i. AIs shall have policies in place or take such measures as may be needed to prevent the misuse of new technological developments against ML/TF&PF risks.
   ii. AIs 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 shall include specific and effective EDD procedures that apply to non-face-to-face customers.
   iii. The AIs shall satisfy themselves that the third party is a regulated and supervised institution and has measures in place to comply with requirements of EDD and reliance on intermediaries and other third parties on EDD as contained in this Guideline.
   iv. AIs that relies on a third party shall 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 ML/TF&PF or any other unlawful acts. Such AIs shall satisfy itself that copies of identification data and other relevant documentation relating to the EDD requirements will be made available from the third party upon request without delay.

4. The Bank of Ghana will continue to monitor developments on new technologies and provide additional guidance as necessary on emerging best practices to address regulatory issues in respect of ML/TF&PF risks.

### 2.7.5 RELIANCE ON INTERMEDIARIES AND THIRD-PARTY SERVICE PROVIDERS

1. AIs relying on intermediaries or other third parties service providers must ensure enhanced due diligence is performed and there is a binding agreement signed.

2. The following criteria should also be met:

i. Immediately obtain from the intermediary or the third-party service providers the relevant information concerning CDD/EDD procedures;
ii. Take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD/EDD requirements will be made available from the intermediary or the third-party service providers upon request without delay;
iii. Satisfy themselves that the intermediary or the third-party service provider is regulated and supervised in accordance with FATF standards and has measures in place to comply with the CDD/EDD and Record Keeping requirements set out in section 32 of Act 1044 and this Guideline;
iv. When determining in which countries the intermediary or the third-party service provider that meets the conditions are based, the AIs shall have regard to information available on the level of country risk; and make sure that adequate EDD provisions are applied to the intermediary or the third-party service provider in order to get account information for competent authorities.
v. For AIs that rely on an intermediary or a third-party service provider 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:
    a. the group applies CDD/EDD and record-keeping requirements, in line with Act 1044 and FATF Standards against ML/TF&PF.
    b. the implementation of those CDD/EDD and record-keeping requirements and AML/CFT&P programmes is supervised at a group level by a competent authority; and
    c. any higher country risk is adequately mitigated by the group's AML/CFT&P policies.

3. The ultimate responsibility for CDD/EDD measures and verification remains with the AIs when relying on intermediaries and third-party service providers.

### 2.7.6 HIGH RISK COUNTRIES

1. AIs shall give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF recommendations.

2. AIs shall report suspicious transactions that have no apparent economic or visible lawful purpose. The background and purpose of such transactions shall be examined and written findings made available to assist FIC to carry out its duties.

3. AIs 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 customers and enhancement of advisories, including jurisdiction-specific financial advisories to AIs 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. AIs, in considering requests for licensing or approval for the establishment of subsidiaries or branches or representative offices, shall take into account that the country does not have adequate AML/CFT&P systems and as such conduct the appropriate EDD procedures;
iv. Advise customers that transact with natural or legal persons within that country that there is a high risk of ML/TF&PF. The AI shall thus limit business relationships or financial transactions with the identified country or persons in that country.

### 2.7.7 FOREIGN BRANCHES AND SUBSIDIARIES

1. AIs shall ensure that their foreign branches and subsidiaries or parent observe group AML/CFT&P procedures consistent with the provisions of Act 1044 and this Guideline and to apply them to the extent that the local/host country's laws and regulations permit.

2. AIs 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 this Guideline. Where these minimum AML/CFT&P requirements and those of the host country differ, branches and subsidiaries or parent of AIs in the host country are required to apply the higher standard and such must be applied to the extent that the host country's laws, regulations or other measures permit.

3. Financial groups shall implement group-wide programmes against ML/TF&PF which shall be applicable and appropriate to all branches and majority-owned subsidiaries of the financial group. These programmes include:
   i. compliance management arrangements (including the appointment of an AMLRO 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 adequacy of the AML/CFT/CPF programme;
   v. policies and procedures for sharing information required for the purposes of CDD/EDD and ML/TF&PF risk management;
   vi. the provision, at group-level compliance, audit, and/or AML/CFT&CPF functions, of customer, account and transaction information to or from branches and subsidiaries when necessary for AML/CFT&CPF purposes;
   vii. the information referred to under "vi" above shall include the fact that an STR has been submitted on a customer and this shall not amount to a violation of the tipping off rules; and
   viii. adequate safeguards on the confidentiality and use of information exchanged including safeguards to prevent tipping off.

4. Where the foreign branches and majority owned subsidiaries are unable to observe

the appropriate AML/CFT&CPF procedures because they are prohibited by the host country's laws, regulations or other measures, the foreign branches and majority owned subsidiaries shall apply appropriate additional measures to manage the ML/TF&PF risks and the AI shall inform the BOG in writing.

5. AIs are subject to these AML/CFT&P principles and shall therefore apply consistently the CDD/EDD procedures at their group level taking into account the activity of the customer with the various branches and subsidiaries.

### 2.7.8 MONEY OR VALUE TRANSFER SERVICES (MVTS)

1. 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 Act 1044 and this Guideline.

2. 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 in accordance with section 32 of Act 1044.

3. MVTS operators shall assess their agents and correspondent operators AML/CFT&P 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&P responsibilities of each of its agents and correspondent operators.

4. In the case of an MVTS provider that controls both the ordering and the beneficiary side of a wire/electronic transfer, the MVTS provider shall be required to:
   i. take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR/SAR has to be filed; and
   ii. file an STR/SAR in any country affected by the suspicious wire/electronic transfer, and make relevant transaction information available to the FIU/FIC.

### 2.7.9 FOREX BUREAUS

1. Although forex bureaus are subject to BOG regulations, AIs shall conduct EDD procedures in accordance with this Guidelines. Satisfactory evidence of identity must include receipt of a certified copy of the applicant's operating license.

### 2.7.10 WIRE/ELECTRONIC TRANSFERS

#### A. CROSS BORDER WIRE/ELECTRONIC TRANSFERS - ORDERING FINANCIAL INSTITUTIONS

1. AIs shall ensure that all cross-border wire/electronic transfers of USD 1,000 (or its

cedi equivalent) or more are always accompanied by the following:

a. Required originator information:
   i. the name of the originator;
   ii. 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
   iii. the originator's address, or national identity number, or customer identification number, or date and place of birth.
b. Required beneficiary information:
   i. the name of the beneficiary; and
   ii. 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.

2. Where several individual cross-border wire/electronic 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.

3. If countries apply a de minimis (reduced) threshold (USD 1,000 or cedi equivalent) for the requirements, AI shall be required to ensure that all cross-border wire/electronic transfers below any applicable de minimis (reduced) threshold are always accompanied by the following:
   a. Required originator information:
      i. the name of the originator; and
      ii. 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
   b. Required beneficiary information:
      i. the name of the beneficiary; and
      ii. 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

4. The information required above need not be verified for accuracy. However, the financial institution shall be required to verify the information pertaining to its customer where there is a suspicion of ML/TF&PF.

**B. DOMESTIC WIRE/ELECTRONIC TRANSFERS**

1. For domestic wire/electronic transfers, the ordering AI shall be required to ensure that the information accompanying the wire/electronic transfer includes originator information as indicated for cross-border wire/electronic transfers, unless this

information can be made available to the beneficiary AI and appropriate authorities by other means.

2. Where the information accompanying the domestic wire/electronic transfer can be made available to the beneficiary AI and appropriate authorities by other means, the ordering AI need only be required to include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The ordering AI shall be required to make the information available within three business days of receiving the request either from the beneficiary AI or from appropriate competent authorities.
3. LEAs shall be able to compel immediate production of such information.
4. The ordering AI shall be required to maintain all originator and beneficiary information collected, in accordance with Act 1044 and FATF Recommendation 11.
5. The ordering AI shall not be allowed to execute the domestic transfer if it does not comply with the requirements specified above.

## C. INTERMEDIARY ACCOUNTABLE INSTITUTIONS

1. For cross-border wire/electronic transfers, an intermediary financial institution shall be required to ensure that all originator and beneficiary information that accompanies a wire/electronic transfer is retained with it.
2. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire/electronic transfer from remaining with a related domestic wire/electronic transfer, the intermediary financial institution shall be required to keep records in accordance with section 32 of Act 1044, of all the information received from the ordering financial institution or another intermediary financial institution.
3. Intermediary financial institutions shall be required to take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire/electronic transfers that lack required originator information or required beneficiary information.
4. Intermediary financial institutions shall be required to have risk-based policies and procedures for determining:
    a. when to execute, reject, or suspend a wire/electronic transfer lacking required originator or required beneficiary information; and
    b. the appropriate follow-up action.

## D. BENEFICIARY ACCOUNTABLE INSTITUTIONS

1. Beneficiary AIs shall be required to take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire/electronic transfers that lack required originator information or required beneficiary information.

2. For cross-border wire/electronic transfers of a threshold USD 1000 or Cedi equivalent or more, a beneficiary AI shall be required to verify the identity of the beneficiary. If the identity has not been previously verified and maintained, this new information shall be retained in accordance with Act 1044 and FATF standards.
3. Beneficiary AIs shall be required to have risk-based policies and procedures for determining:
    a. when to execute, reject, or suspend a wire/electronic transfer lacking required originator or required beneficiary information; and
    b. the appropriate follow-up action.

### 2.7.11 NON-PROFIT ORGANSISATION (CHARITIES) AND RELIGIOUS GROUPS IN GHANA

1. These organisations differ in size, income, structure, legal status, membership and scope. They engage in raising or disbursing funds for charitable, religious, cultural, educational, social or fraternal purposes or for carrying out other types of "good works". These organisations can range from large regional, national or international charities to community-based self-help groups. They also include research institutes, churches, clubs, and professional associations. They typically depend in whole or in part on charitable donations and voluntary service for support.
2. To assess the risk, an AI shall consider:
    a. The evidence of registration under applicable laws of the home and local operation;
    b. The purpose, ideology or philosophy of the organisation;
    c. The geographic areas served (including headquarters and operational areas);
    d. organizational structure;
    e. The organisation's donor volunteer and member base;
    f. Funding and disbursement criteria (including basic beneficiary information);
    g. Record keeping requirements;
    h. Affiliation with other organisation, Governments or groups;
    i. Identity of all signatories to the account; and
    j. Identity of board members and trustees, where applicable.
3. As part of the CDD/EDD process, AIs shall carry out due diligence against publicly available terrorist lists and monitor on an ongoing basis whether funds are being sent to high-risk countries. A non-profit association should be registered in Ghana and where it is registered as an external entity, then the AI shall as additional due diligence checks contact the appropriate overseas competent authority to confirm its existence. AI shall satisfy themselves as to the legitimacy of the organization by, for example, requesting a copy of the constitution.

### 2.7.12 REGISTERED CHARITIES

1. AIs shall subject Charities to EDD procedures in regards to identification procedures required for onboarding. For emphasis, accounts for charities in Ghana shall be operated by a minimum of two signatories, duly verified and documentation evidence obtained.

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

3. 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) an AI shall send a letter to the official correspondent, informing him of the charity's application before it. The official correspondent shall be requested to respond as a matter of urgency especially where there is a reason to suggest that the application has been made without due authority.

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

5. Applications on behalf of un-registered charities is prohibited.

### 2.7.13 RELIGIOUS ORGANIZATIONS (ROs)

1. 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.

## 2.8 TRANSACTION MONITORING, SUSPICIOUS ACTIVITY AND TRANSACTION REPORTING

### 2.8.1 DEFINITION OF A SUSPICIOUS TRANSACTION/ACTIVITY

For the purpose of this 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 a transaction that is inconsistent with a customer's known legitimate business or personal activities or normal business for that type of account or that the transaction lacks an obvious economic rationale.

### 2.8.2 DEVELOPMENT AND IMPLEMENTATION OF INSTITUTIONAL POLICY

1. AI 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 the Appendix of this Guideline.

2. AMLROs shall supervise the monitoring and reporting of suspicious transactions/activities.

3. AIs shall be alert to the various patterns of conduct that have been known to be suggestive of ML/TF&PF and maintain a check list of such transactions/activities which shall be disseminated to the relevant staff.

4. When any staff of AI detects any "red flag" or suspicious ML/TF&PF activity, the staff is required to promptly report to the AMLRO. Every action taken shall be recorded. The institution and its staff shall maintain confidentiality in respect of such investigation and any suspicious transaction report that may be filed with the FIC. This action is, however, in compliance with the provisions of Act 1044 which criminalizes "tipping off" (i.e. doing or saying anything that might alert or give information to someone else that he/she is under suspicion of ML/TF&PF).

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

6. AIs, their directors and employees (permanent and temporary) are prohibited from disclosing the fact that a report is required to be filed or has been filed with the FIC and any competent authority.

### 2.8.3 COMPLEX, UNUSUAL OR LARGE TRANSACTIONS

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

2. AIs are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing. They are required to report such findings to the FIC within twenty-four (24) hours upon confirmation of suspicion.

## 2.9 TRANSACTION REPORTING

### 2.9.1 CASH TRANSACTION REPORT (CTR)

1. AIs shall report to the FIC through a prescribed medium all cash transactions within Ghana in any currency and with a threshold of GHS50,000.00 for banks and GHS20,000.00 for specialized deposit-taking institutions (or its foreign currency equivalent) or amounts as may be determined by the FIC.

### 2.9.2 ELECTRONIC CURRENCY TRANSACTION REPORT (ECTR)

1. AIs shall institute policies and procedures to ensure funds transfer into or out of Ghana satisfy AML/CFT&P Regulations. Where AIs through electronic means and in accordance with the Foreign Exchange Act 2007 (Act 723) and Regulations made under that Act:
   a. transfers currency outside the country, or
   b. Receives currency from outside the country

2. On behalf of a customer which exceeds the amount prescribed by the Bank of Ghana, the AI shall within twenty-four (24) hours after the transfer or receipt of the currency, report the particulars of the transfer or receipt to the FIC through a prescribed medium all Electronic Transactions with a threshold of $1,000.00 or its Cedi equivalent for both individuals and business entities or amounts as may be determined by the FIC.

## 2.10 TRANSACTION MONITORING SYSTEMS

1. AIs must have appropriate processes in place that allow for the identification of unusual transactions, patterns and activities that are not consistent with the customer's risk profile.

2. AIs shall implement processes to analyse transactions, patterns and activities to determine if they are suspicious and meet the reporting threshold.

3. Transaction monitoring processes or systems may vary in scope or sophistication (automated and complex systems which integrates the customer data information with core banking application) depending on the size, volumes and complexity of the business operations. Regardless, the key element of any system is having up-to-date customer information to facilitate the identification of unusual activity.

4. Monitoring can be either:
   i. In real time, in that transactions and/or activities can be reviewed as they take place or are about to take place; or
   ii. After the event through an independent review of the transactions and/or activities that a customer has undertaken.

5. AIs shall also have systems and procedures to deal with customers who have not had contact for some time, such as dormant accounts or relationships, to be able to identify future reactivation and unauthorized use.

6. In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer, product risk and delivery channels. Monitoring processes and systems shall enable trend analysis of transaction activities including monitoring of transactions with parties in high risk countries or jurisdictions, to identify unusual or suspicious business relationships and transactions. The monitoring system shall enable AMLRO to monitor and report to Board and senior management on significant customer relationships

and activities on an individual or consolidated basis across the financial group and identify activities that are inconsistent with the AI's knowledge of the customer, their business and risk profile.

7. The parameters and thresholds used to generate alerts of unusual transactions/activities shall be customized to be commensurate with AI's ML/TF&PF risk profile and the complexity and extent of its business activities. Standard parameters provided by the vendor may be used but the AI must be able to validate and demonstrate to the Bank of Ghana that these are appropriate for the institution's risk position. The monitoring system shall be tested at most on a yearly basis to ensure that the parameters are performing as expected and remain relevant. Modifications may be required as a result of such testing. Findings, analysis and the proposed modifications shall be documented indicating:
   i. The rationale for reviewing the parameters and thresholds;
   ii. Details of testing; any assumptions made and the analysis of outcomes; and
   iii. The changes made to the parameters and thresholds.

8. AIs shall refer to the guidance on conducting ML/TF&PF risk assessment of customers in the Appendix of this Guideline for the implementation of a robust transaction monitoring system.

## 2.11 IDENTIFICATION OF DESIGNATED ENTITIES AND PERSONS & FREEZING OF FUNDS

1. AIs must be able to identify and to comply with reporting and freezing instructions issued by the FIC regarding individuals and entities designated by the United Nations Security Council, OFAC, EU, His Royal Majesty or a competent authority as terrorist entities.

2. Notices issued by the FIC in this regard and the consolidated list shall be duly communicated to AIs.

3. In accordance with section 63 of Act 1044, AIs shall have specific obligations to immediately report to the FIC where any of the following apply:
   i. A person or entity named on the UN or third party lists has funds in the AI;
   ii. The AI has reasonable grounds to believe that the designated person or entity has funds in Ghana; and
   iii. If the designated person or entity attempts to enter into a transaction or continue a business relationship, a suspicious transaction/activity report must be submitted immediately to the FIC.

4. The AI shall not enter into or continue such transaction with the designated person or entity. Funds already deposited with or held by the AI must remain frozen subject to the laws of Ghana.

5. It shall be noted that third party lists as set out in section 63 of Act 1044 and Act 762 as amended include an obligation to immediately freeze the funds of the listed entity.

6. In such cases, where the AI identifies funds of a listed person in Ghana, the AI should treat such funds as frozen pursuant to the Act 1044 and Act 762 as amended.

7. Terrorist screening is not a risk-based due diligence measure and must be carried out regardless of the customer's risk profile. AIs shall have processes in place to screen customer details and payment instructions against the designated lists of persons and entities and to ensure that the lists being screened against are up to date.

8. Screening measures shall consider:
   i. Continuous risk-based screening of customer records;
   ii. Immediate screening of one-off, occasional transactions before the transaction is completed;
   iii. Procedures to screen applicable payment messages; and
   iv. Procedures to screen payment details on wire/electronic transfers and remittances to reasonably ensure that originator, intermediary and beneficiary details are included on the transfers.

9. AI's policies and procedures shall address:
   i. The information sources used by the AIs for screening (including commercial databases used to identify designated individuals and entities);
   ii. The roles and responsibilities of the AI's employees and officers involved in the screening, reviewing and dismissing of alerts, maintaining and updating of the various screening databases and escalating potential matches;
   iii. The frequency of review of such policies, procedures and controls;
   iv. The frequency of periodic screening;
   v. How potential matches from screening are to be resolved by the AI's employees and officers, including the process for determining that an apparent match is a positive hit and for dismissing a potential match as a false match; and
   vi. The steps to be taken by the AMLRO for escalating potential or positive matches to senior management and reporting suspicious or positive matches to the FIC.

### 2.11.1 TRADE/ECONOMIC SANCTIONS

1. Economic and trade sanctions are imposed against countries, governments, entities and persons with a view to bringing about changes in policies and behavior. Governments typically impose economic sanctions to give effect to decisions made by international organizations such as the United Nations or individual or groups of countries such as the United States, United Kingdom (His Royal Majesty), Canada or the European Union, AU, ECOWAS.

2. These may take the form of:
   i. Prohibitions against providing financial services;
   ii. Travel bans;
   iii. Embargoes on arms and military products; and
   iv. Prohibitions or control of trade involving certain markets, services and goods.

3. AIs shall be aware of such sanctions and consider whether these affect their operations and any implications to the AI's policies and procedures particularly with respect to international transfers and its correspondent relationships. In addition to screening payment instructions to identify designated terrorists, AIs shall screen or filter payment instructions prior to their execution in order to prevent making funds available in breach of sanctions, embargoes or other measures.

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

## 2.12 KNOW YOUR EMPLOYEE

1. In addition to knowing the customer, AIs shall have robust procedures in place for knowing its employees. In this regard, every AIs shall have a recruitment policy to attract and retain employees with the highest levels of integrity and competence. The ability to implement an effective AML/CFT&P programme depends in part on the quality and integrity of employees.

2. Consequently, AIs shall undertake due diligence on prospective employees and throughout the course of employment.

   At a minimum, the AIs shall:

   i. Verify the applicant's identity and personal information including employment history and background and also consider credit history checks on a risk-based approach;
   ii. Develop a risk-based approach to determine when pre-employment background screening is considered appropriate or when the level of screening should be increased, based upon the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which shall include verification of references, experience, education and professional qualifications;
   iii. Maintain an ongoing approach to screening for specific positions, as circumstances change, or for a comprehensive review of employees over a period of time. Internal policies and procedures shall be in place (e.g. codes for conduct, ethics, conflicts of interest) for assessing employees;
   iv. Have a policy that addresses appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or employee provided.

   Verification shall generally include the following:

   i. Reference checks
   ii. Checking the authenticity of academic qualifications
   iii. Verifying Employment History
   iv. Police background checks

v. Integrity checks against BoG Engaged and Disengaged Database

3. AIs shall document and keep evidence of the above processes.

4. AIs shall in addition maintain records of the names, addresses, position, titles and other official information pertaining to employees appointed or recruited in accordance with section 32 of Act 1044.

5. AIs, to the extent permitted, shall ensure the laws of the relevant country and similar recruitment policies are followed by its branches, subsidiaries and associate companies abroad, especially in those countries which are not sufficiently compliant with FATF standards.

6. In addition to a robust recruitment policy, AIs shall implement ongoing monitoring of employees to ensure that they continue to meet the institution's standards of integrity and competence.

7. AIs shall establish and maintain procedures to ensure high standards of integrity among employees, including the meeting of statutory "fit and proper" criteria of the officers of the AI. Integrity standards shall be documented and accessible to all employees. These internal procedures may include standards for:
   i. acceptance of gifts from customers;
   ii. social liaisons with customers;
   iii. disclosure of information about customers who may be engaged in criminal activity;
   iv. confidentiality;
   v. detection of any unusual growth in employees' wealth; and
   vi. deterring employees from engaging in illegal activities that can be detected by reference to his investment records.

8. The standards shall include a code of ethics for the conduct of all employees and procedures shall allow for regular reviews of employees' performance and their compliance with established rules and standards. It shall also provide for disciplinary action in the event of breaches of these rules.

### 2.12.1 MONITORING OF EMPLOYEE CONDUCT

1. AIs shall monitor employees' accounts for potential signs of ML/TF&P and also pay particular attention to employees whose lifestyles cannot be supported by their salary or known financial circumstances. Supervisors and managers shall be encouraged to know the employees in their department and investigate any substantial changes in their lifestyles which do not match their financial position. Internal procedures shall provide for special investigation of employees who are associated with unexplained shortages of funds.

2. AIs shall also subject employees' accounts, including accounts of key management personnel, to the same AML/CFT&P procedures as applicable to other customers' accounts. This is required to be performed under the supervision of the AMLRO.

The AMLRO's account is to be reviewed by the Internal Auditor or any other Senior Officer designated by the Management of the AI. Compliance reports including findings on the AMLRO's account shall be submitted to the BOG and FIC on or before **15th July (half-year) and on or before 15th January (End of Year) of the following year**.

3. The AML/CFT&P performance review of staff shall be part of employees' annual performance appraisal.

### 2.12.2 EMPLOYEE-EDUCATION AND TRAINING PROGRAMME

**Institutional Policy**

1. AIs shall design comprehensive employee education and training programmes 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&P tasks. Indeed, the establishment of such an employee training programme is not only considered as best practice but also a statutory requirement.

2. The timing, coverage and content of the employee training programme shall be tailored to meet the perceived needs of the AIs. A comprehensive training programme is however required to encompass staff/areas such as reporting officers; new staff (as part of the orientation programme 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.

3. AIs are required to submit their annual AML/CFT&P employee training programme for the ensuing year to the BOG and FIC not later than **December 31 every financial year**.

4. The employee training programme is required to be developed under the guidance of the AMLRO in collaboration with the Senior Management.

5. At a minimum, an AI shall;
   i. Develop an appropriately tailored training and awareness programme consistent with the AI's size, resources and type of operation to enable relevant employees to be aware of the risks associated with ML/TF&PF. The training should also ensure employees understand how the institution might be used for ML/TF&PF; enable them to recognize and handle potential ML/TF&PF transactions; and to be aware of new techniques and trends in money laundering and terrorist financing;
   ii. Document, as part of their AML/CFT&P policy/manual, their approach to training, including the frequency, delivery channels and content;
   iii. Ensure that all employees are aware of the identity and responsibilities of the AMLRO to whom they shall report unusual or suspicious transactions;
   iv. Establish and maintain a regular schedule of new and refresher programmes, appropriate to their risk profile, for the different types of training required for:

a. new employees;
b. operations employees;
c. agents;
d. supervisors/line managers;
e. Board and Senior Management; and
f. audit and compliance employees.

v. Obtain an acknowledgement from each employee on the training received;
vi. Assess the effectiveness of training; and
vii. Provide all relevant employees with reference manuals/materials that outline their responsibilities and the institution's policies. These shall complement rather than replace formal training programmes.

6. The employee training programme shall include but not limited to the following:
   i. AML regulations and offences;
   ii. The nature of ML/TF&PF;
   iii. Money laundering 'red flags' and suspicious transactions, including trade-based money laundering typologies;
   iv. AML/CFT&P reporting requirements;
   v. Customer due diligence;
   vi. Risk-based approach to AML/CFT&P regime;
   vii. Record keeping and retention policy; and
   viii. Any other relevant AML/CFT&P topic

7. AIs are also required to maintain records of employee training which at a minimum shall include:
   i. Details of the content of the training programmes provided;
   ii. The names of employees who have received the training;
   iii. The date on which the training was delivered;
   iv. The results of any testing carried out to measure employees understanding of the anti-money laundering requirements; and
   v. An on-going training plan.

8. AIs shall submit half yearly report on their level of compliance to the BOG and FIC by **July 15 of the year under review and January 15 of the following year**.

9. AIs shall fully participate in all AML/CFT&P interactive programmes organized by BOG and/or FIC and failure to attend shall attract administrative sanctions.

### 2.12.3 WHISTLEBLOWING

1. AIs shall develop policies on whistleblowing. These policies shall at a minimum:
   a. direct their employees in writing and ensure that they always co-operate fully with the Regulators and law enforcement agencies;

b. make provisions for directors, officials and employees to report any violations of the institution's AML/CFT&P compliance programme to the AMLRO;
c. In cases where the violations involve the AMLRO, employees are required to report such to a designated higher authority such as the Internal Auditor; and
d. inform their employees in writing to make such reports confidential and that they will be protected from victimization for making them.

## 2.13 RECORD KEEPING

AIs shall keep books and records with respect to customers and transactions as set out in section 32 of Act 1044

### 2.13.1 MAINTENANCE OF RECORDS ON TRANSACTIONS

1. AIs are required to maintain all necessary records of transactions, both domestic and international, in accordance with section 32 of Act 1044.
2. AIs shall maintain these records in a manner that upon request by the BOG, FIC or any other competent authority can be made readily available.
3. The above requirements apply regardless of whether the account or business relationship is ongoing or has been terminated.
4. Examples of the necessary components of transaction-records include customer's and beneficiary's names, addresses (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the currency and amount involved, the type and identification number of any account involved in the transaction.
5. AIs shall maintain records of the identification data, account files and business correspondence in accordance with section 32 of Act 1044.
6. AIs shall ensure that all customer-transaction records and information are made available on a timely basis.

# PART C - KNOW YOUR CUSTOMER (KYC) / CUSTOMER DUE DILIGENCE (CDD) PROCEDURES

AIs shall not establish a business relationship until all relevant parties to the relationship have been identified, verified and the nature of the business they intend to conduct ascertained. Once an on-going business relationship is established, any inconsistent activity can then be examined to determine whether or not there is an element of ML/TF&PF suspicion.

## 3.1 WHAT IS IDENTITY

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

## 3.2 DUTY TO OBTAIN IDENTIFICATION EVIDENCE

1. The first requirement of knowing your customer for ML/TF&PF purposes is for the AI to be satisfied that a prospective customer is who he/she is or claims to be.
2. AIs shall not carry out or agree to carry out financial business or provide advice to a customer or potential customer unless they are certain of the identity of that customer. 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 AI has the obligation to identify and verify the identity of both the customer and the agent/trustee unless the customer is itself an AI.
3. AIs have the duty to obtain identification evidence in respect of their customers and all other relevant parties to the relationship from the outset.

## 3.3 ESTABLISHMENT OF IDENTITY

1. 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 verification, validating and updating identity, and the extent of obtaining additional KYC/CDD information shall be the sole prerogative of the National Identification Authority (NIA) for individuals' resident/working in Ghana and the Registrar General's Department for legal persons (entities).

2. The general principles for establishing the identity of both legal and natural persons and the procedures of obtaining satisfactory identification evidence at minimum is set out below:

    a. AIs shall obtain sufficient information on the:
        i. nature of the business that their customer intends to undertake, including the expected or predictable pattern of transactions;
        ii. purpose and reason for opening the account or establishing the relationship;
        iii. nature of the activity that is to be undertaken;
        iv. expected origin of the funds to be used during the relationship; and
        v. details of occupation/employment/business activities and sources of wealth or funds (income).

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

## 3.4 VERIFICATION OF IDENTITY

1. Identity shall be verified whenever a business relationship
    a. is to be established;
    b. involves account opening; or
    c. during a one-off transaction(s); or
    d. when series of linked transactions take place.

2. "Transaction" in this Guideline is defined to include giving of advice. The "advice" here does not apply when information is provided about the availability of products or services nor when a first interview/discussion prior to establishing a relationship takes place.

3. AIs shall verify the identity of customers for all transactions.
4. Once identification procedures have been satisfactorily completed and the business relationship established, AIs shall maintain and keep record up to date.

## 3.5 CUSTOMERS TO BE VERIFIED

1. AIs shall verify the identity of customers (natural/legal) to ascertain that the customer is the very person he/she claims to be.

2. AIs shall verify the identity of the person acting on behalf of another and obtain and verify identities of the other persons involved.

3. AIs shall take appropriate steps to identify directors and all signatories to an account.

4. AIs shall verify all parties in joint accounts.

5. For high risk business undertaken for private companies (i.e. those not listed on the stock exchange) sufficient evidence of identity and EDD procedures shall be conducted in respect of:
   i. the principal underlying beneficial owner(s); and
   ii. persons with controlling interest in the company.

6. AIs shall be alert to circumstances that might indicate any significant changes in the nature of the business or its ownership (controlling interest) and make enquiries accordingly and to observe the additional provisions for High Risk Categories of Customers as provided in this Guideline.

7. Trusts – AIs 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.

8. When one AI acquires the business and accounts of another AI, it shall identify all the acquired customers. It is also mandatory to carry out due diligence procedures to confirm that the acquired institution had conformed with the requirements in this Guideline prior to the acquisition.

## 3.6 TIMING OF IDENTIFICATION

1. 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. 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 regards to the risk appetite of the AI.

2. To this end, the AI shall:
   i. obtain identification evidence within ninety (90) days after it has contact with a customer with a view to agreeing with the customer to carry out an initial transaction; or reaching an understanding (whether binding or not) with the customer that it may carry out future transactions;
   ii. where the customer does not supply the required information as stipulated above, the AI shall immediately discontinue any activity it is conducting for the customer; and bring to end any understanding reached with the customer; and
   iii. where the AI suspects any unusual or ML/TF&PF risks, the AI shall file an STR/SAR to FIC

3. AI shall 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.

4. The failure or refusal by an applicant to provide satisfactory identification evidence within a reasonable time-frame (90 days) may lead to a suspicion that the depositor or investor is engaged in ML/TF&PF. The AI shall therefore make an STR/SAR to the FIC based on the information in its possession.

5. AIs shall have in place written and consistent policies of closing an account or reversing a transaction where satisfactory evidence of identity cannot be obtained.

6. AIs shall respond promptly to inquiries made by competent authorities.

## 3.7 CERTIFICATION OF IDENTIFICATION DOCUMENTS

1. In order to guard against the dangers of identity fraud and ML/TF&PF risks, AIs shall take adequate steps to verify the authenticity of the documents with the issuing or identification authority.

## 3.8 RISK-BASED APPROACH TO CUSTOMER IDENTIFICATION AND VERIFICATION

1. AIs shall take a risk-based approach to the KYC/CDD requirements for all customers. Furthermore, AIs shall decide on the number of times to verify the customer's records during the relationship, the identification evidence required and when additional checks are necessary. These decisions shall equally be recorded.

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

## 3.9 RISK BASED CUSTOMER DUE DILIGENCE

### 3.9.1 LOW RISK/SIMPLIFIED DUE DILIGENCE

1. With a risk-based approach, where the identified ML/TF&PF risks are low, AIs shall apply SDD. SDD shall be commensurate with the identified low risk factors (e.g. the simplified measures may relate only to customer acceptance measures or to aspects of ongoing monitoring). It shall be noted that SDD never means a complete exemption or absence of CDD measures but rather, AIs may adjust the frequency and intensity of measures to satisfy the minimum CDD standards. AIs

are reminded that simplified measures are not acceptable whenever there is suspicion of ML/TF&PF risks or where specific high risk is determined.

2. With respect to beneficial ownership in a financial inclusion context, the beneficial owner will in most instances be the customer himself or a closely related family member. Where there is a suspicion of ML/TF&PF, that the account owner is being used as a 'straw man' and is not the beneficial owner, enhanced due diligence measures shall be applied and an internal suspicious report must be filed with the AMLRO and a subsequent report to FIC.

3. This Guideline identifies the specific instances when SDD measures may be applied including where low risks have been identified through a national risk assessment or through an adequate assessment of ML/TF&PF risk by the AI.

4. In addition, AIs shall, based on their risk assessments, apply SDD to specifically defined low risk customers or products and services. Such instances may include but are not limited to:

    i. Customers whose sole source of funds is a salary credit to an account or with a regular source of income from a known source which supports the activity being undertaken;
    ii. Pensioners, social benefit recipients or customers whose income originates from their spouses'/partners' employment; and
    iii. Customers represented by those whose appointment is subject to legal instruments;

5. For customers who do not have photo identification or have limited identification documentation such as tourists or those who are socially or economically vulnerable such as the disabled, elderly, minors or students, a 'tiered' SDD approach allows financial access with limited functionality. For example, AI shall offer banking accounts with low transaction/payment/balance limits with reduced documentation requirements. Access to additional services such as higher transaction limits or account balances or access to diversified delivery channels shall only be allowed if and when the customer can satisfy additional identification requirements. Where this applies AIs shall have monitoring systems to ensure that transaction and balance limits are observed. The AIs shall ensure that the customer shall provide the valid identification (Ghana Card) within ninety (90) days.

6. Where there is suspicion of ML/TF&PF risk, the AIs shall not apply SDD measures.

#### 3.9.1.1 EXAMPLES OF SDD MEASURES

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

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

AIs shall verify the customer's or beneficial owner's identity after the establishment of the business relationship where financial products or services provided have limited functionality or restricted services to certain types of customers for financial inclusion purposes. For example, limits shall be imposed on the number or total value of transactions per week/month; the product or service shall only be offered to nationals or only domestic transactions shall be allowed.

Similarly, general insurance products such as car insurance present low ML/TF&PF risk so verification of identity may be postponed until there is a claim or until the customer requests additional insurance products. In such instances, AIs must ensure that:

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

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

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

c. *Adjust the frequency of SDD updates and reviews of the business relationship*

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

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

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

### 3.9.1.2 FINANCIAL INCLUSION

1. AIs shall have financial inclusion policies for the socially and financially disadvantaged citizens in Ghana.

2. 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 shall 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 AIs shall make allowance for such persons by way of providing appropriate advice to staff on how the identities of such group of persons can be confirmed and what checks shall be made under these exceptional circumstances.

3. Where an AI has reasonable grounds to conclude that an individual customer is not able to produce the detailed evidence of his/her identity and cannot reasonably be expected to do so, the AI shall do the following:
   i. accept as identification evidence a letter or statement from a person in a position of responsibility who knows the customer and can confirm that the customer is who he/she says he/she is, including confirmation of his/her permanent address;
   ii. accept and verify the ID of the guarantor;
   iii. offer basic low risk account services;
   iv. have a 90-day deferral waiver for the customer to obtain the Ghana Card;
   v. where the customer does not supply the required information as stipulated above, the AI shall immediately discontinue any activity it is conducting for the customer; and
   vi. where the AI suspects any unusual or ML/TF&PF risks, the AI shall file an STR to FIC.

### 3.9.2 ENHANCED DUE DILIGENCE (HIGH RISK)

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

2. The AI's policy framework shall therefore include a description of the type of customers that are likely to pose higher than average risk and the EDD procedures to be applied in such instances. The commencement of a business relationship with a high-risk customer shall be approved by senior management. Senior management shall receive sufficient information to make an informed decision on the level of ML/TF&PF risk the institution would be exposed to if it enters into or continues that business relationship and how well equipped it is to manage that risk effectively.

3. AIs shall also ensure that monitoring systems are appropriately tailored and provide timely and comprehensive reports to facilitate effective monitoring of such relationships and periodic reporting on such relationships to Board and senior management.

4. Act 1044 and this Guideline identify specific instances that AIs must always treat as high risk and to which EDD must be applied. EDD shall be applied in the following circumstances:
    i. Business transactions with persons and AIs in or from other countries which do not or insufficiently comply with the FATF Standards;
    ii. Complex, unusual or large transactions, whether completed or not, to all unusual patterns of transaction and to insignificant but periodic transactions which have no apparent economic or visible lawful purpose;
    iii. Where ML/TF&PF risks are high;
    iv. When establishing correspondent banking relationships;
    v. Where high risks have been identified with a PEP customer; and
    vi. Non-face to face business relationships or transactions

5. AIs shall exercise due caution if entering into business relationships or otherwise doing business with persons from high risk jurisdictions named in Public Statements issued by international organisations such as OFAC, EU, His Royal Majesty (UK), UNSCRs, FATF, AU and ECOWAS.

**3.9.2.1 EXAMPLES OF EDD MEASURES**

1. When a new customer falls within high risk category, or an AI launches a high risk product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the following shall apply:
    i. Increase the quantity/quality of information obtained for EDD purposes (e.g. request additional information as to the customer's residential status, employment, salary details and other sources of income) and requesting additional documentary evidence or utilizing publicly available sources (e.g. scrutiny of negative media news, internet searches, use of social media).
    ii. Understand the customer's ownership and control structure to ensure that the risk associated with the relationship is well-known. This may include obtaining and assessing information regarding the customer's reputation including any negative media allegations against the customer.
    iii. Understand the intended nature of the business relationship and the reasons for intended or performed transactions. This may include obtaining information on the number, size and frequency of transactions that are likely to be conducted. It may be appropriate to request a customer's, business plans, cash flow projections, copies of contracts with vendors etc. The AI shall understand why the customer is requesting a certain service or product particularly when it is unclear why the customer is seeking to establish business relationships in another jurisdiction from where he is domiciled. The account shall be regularly monitored to establish a full

view of the nature of activity and whether it fits with the initial risk profile of the customer.

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

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

vi. Review current financial statements; and

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

2. The availability and use of other financial information held is important for reducing the additional costs of collecting customer due diligence information and can help increase AI's understanding of the risk associated with the business relationship. Where appropriate and practical and where there are no data protection restrictions, AIs shall take reasonable steps to ensure that where customer due diligence information is available in one part of the business, there are information sharing mechanisms to link it to information held in another.

**3.9.2.2 ENHANCED MONITORING**

1. The following are examples of measures AI shall employ to monitor high-risk customers:
   i. Conducting more frequent reviews of the business relationship and establishing more stringent thresholds for updating EDD information;
   ii. Setting specific business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
   iii. Requiring senior management approval at the transaction level for products and services that are new for the customer;
   iv. Reviewing transactions more frequently against red flag indicators relevant to the relationship. This may include establishing the purpose and destination of funds and obtaining more information on the beneficiary before conducting the transaction;
   v. Flagging unusual activities and escalating concerns and transactions for senior management's attention.

### 3.9.3 PROVISION OF SAFE CUSTODY AND SAFE DEPOSIT BOXES

1. AIs shall take precautions in relation to requests to hold boxes, parcels and sealed envelopes in a safe custody. Where such facilities are made available to non-account holders, the EDD procedures set out in this Guideline shall apply.

### 3.9.4 VIRTUAL ASSETS (VAS) AND VIRTUAL ASSETS SERVICE PROVIDERS (VASPS)

1. FATF defines Virtual Asset (VA) as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations

2. Virtual Asset Service Provider (VASP) means any natural or legal person who is not covered elsewhere under the Recommendation and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
    i. Exchange between virtual assets and fiat currencies;
    ii. Exchange between one or more forms of virtual assets;
    iii. Transfer of virtual assets;
    iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
    v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

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

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

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

6. AIs shall identify and assess the ML/TF&PF risks emerging from virtual assets activities and the activities or operations of VASPs.
7. AIs shall take appropriate measures to manage and mitigate such risks.

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

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

10. AIs shall report SAR/STR on identified VASP activities to the FIC within 24 hours.

**NB: Please note VASPs are not currently licensed by Bank of Ghana**

## APPENDIX A - DEFINITION OF TERMS

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

| Terms | Definition |
|---|---|
| ***Accountable Institution*** | All Bank of Ghana licensed institutions |
| ***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 obtained and verified. |
| ***Batch transfer*** | A batch transfer is a transfer comprising a number of individual wire/electronic transfers that are being sent to the same Bank of Ghana licensed 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 AI*** | All Bank of Ghana licensed institutions which receives the wire/electronic transfer or domestic transfer from the ordering AI or financial institution directly or through an intermediary and make funds available to the beneficiary (customer). |
| ***Beneficiary*** | Beneficiary includes those natural or legal person(s), or groups of natural persons who enjoys the benefits or rights of an account, receive charitable, humanitarian or other types of assistance through the products or services of AI. |
| ***Business Relationship*** | Business relationship is any arrangement between the AI and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a frequent or one-off basis and where the monetary value of dealings in the course of the arrangement is known or not known. These include but not limited to: from the date of opening account, when the customer deposit or withdraws money or the customer becomes indebted to the AI. |
| ***Business Entity*** | Business entity includes:<br>(a) a firm,<br>(b) an individual licensed to carry out a business,<br>(c) a limited liability company, or<br>(d) a partnership,<br>(e) company limited by guarantee, and<br>(f) public listed companies |

| | |
|---|---|
| ***Cross-border transfer*** | Cross-border transfer means any wire/electronic transfer where the originator and beneficiary institutions are located in different jurisdictions.<br>This term also refers to any chain of wire/electronic transfers that has at least one cross-border element. |
| ***Designated categories of offences*** | Designated categories of offences mean:<br>• participation in an organised criminal group and racketeering;<br>• terrorism, including terrorist financing, proliferation financing;<br>• trafficking in human beings and migrant smuggling;<br>• sexual exploitation, including sexual exploitation of children;<br>• illicit trafficking in narcotic drugs and psychotropic substances;<br>• illicit arms trafficking;<br>• illicit trafficking in stolen and other goods;<br>• corruption and bribery;<br>• fraud;<br>• counterfeiting currency;<br>• counterfeiting and piracy of products;<br>• environmental crime;<br>• murder, grievous bodily injury;<br>• kidnapping, illegal restraint and hostage- taking;<br>• robbery or theft;<br>• smuggling;<br>• tax evasion<br>• extortion;<br>• forgery;<br>• piracy; and<br>• insider trading and market manipulation;<br>• any other similar offence or related prohibited activity punishable with imprisonment of not less than twelve (12) months;<br>• any activities that occurred in another country which constitute an offence in that country and which would have constituted an unlawful activity had it occurred in Ghana; and<br>• a contravention of a law in relation to a serious offence which occurs in the country or elsewhere. |

| | |
|---|---|
| **Designated non-financial businesses and professions** | Designated non-financial businesses and professions means:<br>• Casinos (which also includes internet casinos).<br>• Real estate agents.<br>• Dealers in precious metals.<br>• Dealers in precious stones.<br>• Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to "internal" professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat ML/TF&PF.<br>• Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under the FATF Recommendations, and which as a business, provide any of the following services to third parties:<br>i. acting as a formation agent of legal persons;<br>ii. 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;<br>iii. providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;<br>iv. acting as (or arranging for another person to act as) a trustee of an express trust;<br>v. acting as (or arranging for another person to act as) a nominee shareholder for another person. |
| ***Domestic transfer*** | Domestic transfer means any wire/electronic transfer where the originator and beneficiary institutions are both located in Ghana. This term therefore refers to any chain of wire/electronic transfers that takes place entirely within Ghana's borders, even though the system used to effect the wire/electronic transfer may be located in another jurisdiction. |
| ***The FATF Recommendations*** | The Financial Action Task Force Recommendations refers to the internationally endorsed global standards against ML/TF&PF |
| ***Financial institutions*** | Financial institutions (under correspondent banking) means any entity outside Ghana who conducts a correspondent banking relationship either as an ordering or intermediary for or on behalf of a customer. |
| ***Funds Transfer*** | The terms funds transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) by electronic means with a view to making an amount of money available to a beneficiary person. The originator and the beneficiary may be the same person. |

| | |
|---|---|
| *High Net Worth* | High Net Worth means individuals who have been classified by the AIs as High Net Worth person per the internal policies and procedures. |
| ***Legal arrangement(s)*** | Legal arrangement means a trust or partnership or other entity created between parties which lacks separate legal personalities. |
| ***Legal person(s)*** | Legal persons refer to a separate legal entity (body corporate, foundations, partnerships, or associations, or any similar bodies) that can establish a permanent customer relationship with AI 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 to perform the wire/electronic 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. |
| ***Physical presence*** | means the physical location of the AI and its' management in a country. |
| ***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 this Guideline refer 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. |
| ***Simplified Due Diligence*** | Simplified due diligence is the lowest level of due diligence that can be completed on a customer. Simplified due diligence is applied when a risk assessment has shown low risk of ML/TF&PF. |
| ***Source of Funds*** | Source of funds is the origin of funds used for transactions or activities that occur within the business relationship or occasional transaction. In establishing the source of funds, one must understand not only where the funds are coming from but the activities that were involved in generating those funds. |
| ***Source of Wealth*** | Source of wealth describes the economic, business and or commercial activities that generated or significantly contributed to the customers' overall net worth/entire body of wealth. Examples of source of wealth includes salaries, inheritances, investments, business ownership, property or gifts. |
| ***Terrorist*** | It refers to any natural person who:<br>i. commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully;<br>ii. participates as an accomplice in terrorist acts;<br>iii. organizes or directs others to commit terrorist acts; or<br>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:<br><br>An act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997); and 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 (TF) 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.<br><br>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. |
| ***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:<br>• commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully;<br>• participates as an accomplice in terrorist acts;<br>• organizes or directs others to commit terrorist acts; or<br>• 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 |
| ***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.<br>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 transaction or an activity. |
| ***Wire/Electronic transfer*** | The term wire/electronic transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) by electronic means with a view to making an amount of money available to a beneficiary person. The originator and the beneficiary may be the same person. |

## APPENDIX B - INFORMATION TO ESTABLISH IDENTITY

| **MINIMUM REQUIREMENTS FOR VERIFICATION AND KYC/CDD FOR NEW AND EXISTING CUSTOMERS** | | |
|---|---|---|
| Customer Type | Customer Sub-type | Identification / Verification Requirements |
| Individuals | Ghanaian Citizen | Ghana Card KYC Data Set<br><br>Additional minimum requirements<br><br>Proof of Residential Address<br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document issued by an authorized government agency or institution. |
| | Ghanaians Living Abroad | Ghana Card KYC Data Set<br><br>Additional minimum requirements<br><br>Proof of Residential address (foreign)<br>i. Utility Bill, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document issued by an authorized government agency or institution.<br><br><u>Supplementary requirement</u><br>Proof of Residential Address (local)<br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document |
| | Foreigners with Permanent Residence in Ghana | Non- Citizen Card KYC Data Set<br><br>Additional minimum requirements<br><br>Proof of Residential Address (local)<br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document.<br><br>Proof of Residential address (foreign)<br>i. Utility Bill, or |

| | | |
|---|---|---|
| | | ii. Tenancy Agreement, or<br>iii. Any other relevant document **issued by an authorized government agency or institution.** |
| | Students (18+) | Ghana Card KYC Data Set<br><br>Additional minimum requirement<br>i. Introductory letter (school / parent / Guardian)<br>ii. Student ID Card<br><br>Proof of Residence<br>i. GPS Address<br>ii. Tenancy / Hostel Agreement<br>iii. Any other relevant document issued by an authorized government agency or institution. |
| | Minors | Ghana Card KYC Data Set of Parent/Guardian<br><br>Additional Requirements (Minor's Details)<br>Full Name<br>Date of Birth<br>Birth Certificate<br><br>Parent / Guardian<br>Proof of Address Residential<br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document issued by an authorized government agency or institution. |
| | Refugees and Asylum Seekers | Non- Citizen Card KYC Data Set<br><br>Additional minimum requirement;<br><br>References / letter from Ministry of Interior or an appropriate government / international agency<br><br>Proof Residential Address (local)<br>i. GPS Address, or |

| | | |
|---|---|---|
| | | ii. Tenancy Agreement, or<br>iii. Any other relevant document issued by an authorized government agency or institution.<br><br>Details of last Residential address or country of origin (foreign) |
| | Foreign Diplomats | Diplomatic Card / Diplomatic Passport<br><br>Additional minimum requirement Reference/Letter from<br>i. Ministry of Foreign Affairs and Regional Integration and or<br>ii. Embassy / Consulate Office<br><br>Proof of Residential Address (local)<br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document issued by an authorized government agency or institution.<br><br>Proof of Residential address (foreign)<br>i. Utility Bill, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document issued by an authorized government agency or institution. |
| | Dependents of Foreign Diplomats | Diplomatic Card / Diplomatic Passport of the Diplomat<br><br>Additional Requirements (Dependents Details):<br>i. Full Name<br>ii. Date of Birth<br>iii. Passport Details<br><br>Proof of Address Residential (local) of the Diplomat<br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document issued by an authorized |

| | | |
|---|---|---|
| | | government agency or institution.<br><br>Proof of Residential address (foreign) of applicant<br>i. Utility Bill, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document issued by an authorized government agency or institution**.** |

| **Customer Type** | **Customer Sub-type** | **Identification/Verification Requirement** |
|---|---|---|
| **Sole Proprietorship / UBO** | Sole Proprietorship / UBO | *Ghana Card KYC Data Set*<br><br>*Additional Minimum Requirement*<br>i. Full name of Business<br>ii. Full Registered Business Address<br>iii. Registration Number<br>iv. Country of Registration<br>v. Date of Business Registration<br>vi. Nature of Business<br><br>Proof of Residential/Business Address<br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document issued by an authorized government agency or institution. |

| **Client Type** | **Client Sub-type** | **Identification/Verification Requirement** |
|---|---|---|
| **Legal Entities** | Ghanaian Owned Companies and their Directors / Shareholders / Ultimate Beneficiary Owner (UBO) | Ghana Card KYC Data Set for each Director/Shareholder/Ultimate Beneficiary Owner<br><br>Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner<br>i. Certificate of Incorporation<br>ii. Certificate to Commence |

| | | |
|---|---|---|
| | | Business<br><br>Proof of Residential Address for each Director/Shareholder/UBO<br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document issued by an authorized government agency or institution |
| | Foreign Owned Companies and their Foreign Directors and Shareholders/UBO | Non- Citizen Card KYC Data Set<br><br>Additional minimum requirement for each Director / Shareholder / Ultimate Beneficiary Owner<br>i. Certificate of Incorporation<br>ii. Certificate to Commence Business<br>iii. GIPC certification<br>iv. Relevant Industry license<br><br>Proof of Corporate/Residential Address (local) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner<br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document.<br><br>Proof of Residential address (foreign) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner<br>i. Utility Bill, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document |

| **Client Type** | **Client Sub-type** | **Identification/Verification Requirement** |
|---|---|---|
| **Public Registered Companies (Directors / Shareholders / UBO)** | Local Directors / Shareholders with Controlling interest | Ghana Card KYC Data Set for each Director/Shareholder/Ultimate Beneficiary Owner |

| | | |
|---|---|---|
| | | Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner<br>i. Certificate of Incorporation<br>ii. Certificate to Commence Business<br><br>Proof of Residential Address for each Director/Shareholder/UBO<br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document |
| | Foreign Directors/Shareholders with Controlling interest | Non- Citizen Card KYC Data Set<br><br>Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner<br><br>i. Certificate of Incorporation<br>ii. Certificate to Commence Business<br><br>Proof of Corporate/Residential Address (local) for each Foreign Director / Shareholders / Ultimate Beneficiary Owner<br><br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document.<br><br>Proof of Residential address (foreign) for each Foreign Director / Shareholder / Ultimate Beneficiary Owner<br><br>i. Utility Bill, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document |
| | Local UBO | Ghana Card KYC Data Set for each Director/Shareholder/Ultimate Beneficiary Owner<br><br>Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner<br>i. Certificate of Incorporation |

| | | |
|---|---|---|
| | | ii. Certificate to Commence Business<br><br>Proof of Residential Address for each Director/Shareholder/UBO<br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document |
| | Foreign UBO | Non- Citizen Card KYC Data Set<br><br>Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner<br><br>i. Certificate of Incorporation<br>ii. Certificate to Commence Business<br><br>Proof of Corporate/Residential Address (local) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner<br><br>i. GPS Address, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document.<br><br>Proof of Residential address (foreign) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner<br><br>i. Utility Bill, or<br>ii. Tenancy Agreement, or<br>iii. Any other relevant document |

| **Client Type** | **Client Sub-type** | **Identification/Verification Requirement** |
|---|---|---|
| **Government** | State Owned Enterprises (SOEs) | Minimum Requirements<br><br>i. Ghana Card KYC Data Set for all Directors and Account |
| | Ministries, Departments and Agencies | |

| | | |
|---|---|---|
| | Regulatory Bodies /Agencies | Signatories |
| | Public Institutions (E.g. Universities, Hospitals) | ii. Board Resolution<br>iii. Details of Address of Government |
| | Foreign Government – Embassies/Consulate | Minimum Requirements |
| | Foreign Government – Development Organisation | i. Diplomatic Card/Passport of account signatories |
| | International Development Organisations – (E.g. UN, WHO, Africa Development Bank etc.) | ii. Reference/Introductory Letter<br>iii. Details of Address |

| **Customer Type** | **Customer Sub-type** | **Identification/Verification Requirement** |
|---|---|---|
| **Financial Institutions** | Regulated Institutions of;<br>Bank of Ghana<br>Securities and Exchange Commission<br>National Insurance Commission<br>National Pension Regulatory Authority<br>Credit Unions Association<br>And any other regulated financial institution | Minimum Requirements<br>i. Board Resolution<br>ii. Certificate of Incorporation<br>iii. Certificate of Commencement<br>iv. Copy of license from a Regulatory Authority<br>v. Ghana Card/ Non- Citizen Card KYC Data Set for Directors/ Account Signatories<br>vi. Details of Business Address |

| **Customer Type** | **Customer Sub-type** | **Identification/Verification Requirement** |
|---|---|---|
| **Non-Profit Organisations (NPOs) / Clubs and Societies** | Non-Profit Organisations (NGOs) | i. Minimum Requirements<br>ii. Board Resolution<br>iii. Certificate of Incorporation<br>iv. Certificate of Commencement<br>v. Copy of license from a Regulatory Authority<br>vi. Ghana Card/ Non- Citizen Card KYC Data Set for Directors/ Account Signatories<br>vii. Details of Business Address |
| | Religious Organisations / Bodies | |
| | Charities /Foundations | |

| | | |
|---|---|---|
| | | viii. Nature of Business |
| | Clubs | Minimum Requirements<br>i. Board Resolution<br>ii. Constitution<br>iii. Ghana Card KYC Data Set for Account Signatories<br>iv. Details of Business Address<br>v. Nature of Business |
| | Societies/ Associations | |

| **Customer Type** | **Customer Sub-type** | **Identification/Verification Requirement** |
|---|---|---|
| **Trust** | Trust | Minimum requirement<br>i. Certified copy of Trust Deed and supplemental Trustee, or Equivalent constitutive document detailing purpose and structure of the Trust.<br>ii. Details of settlors, trustee and beneficiaries and authorised signatories in the Trust.<br>iii. Where signatories are not identified in the Trust Deed, a certified copy of the authorised signatories list shall be provided.<br>iv. Ghana Card KYC Data Set for;<br>a. Settlors (Donor / Grantors)<br>b. Trustees<br>c. Beneficiaries<br>d. Authorised Signatories |

## APPENDIX C – SUPERVISORY GUIDANCE NOTE ON THE USE OF THE GHANA CARD

For the complete guidance note on the use of the Ghana Card, please refer to supervisory guidance note on the use of the Ghana Card for accountable institution issued by the Bank of Ghana in June 2022 and available on the Bank of Ghana Website.

## APPENDIX D - FURTHER GUIDANCE ON RISK ASSESSMENT AND BUSINESS/CUSTOMER RISK RATING

This Risk Assessment/Customer Risking Rating is designed to assist AIs in conducting an ML/TF&PF risk assessment. A risk assessment is the first step an AI shall take in developing an AML/CFT&P programme. It involves identifying and assessing the risks the business reasonably expects to face from ML/TF&PF. Once a risk assessment is completed, the AI can then put in place a programme that minimises or mitigates these risks. This sets out the minimum requirements in preparing a risk assessment that best suits the AI.

### SOURCES OF INFORMATION FOR THE RISK ASSESSMENT

When conducting or updating risk assessments, the AI shall consider information obtained from relevant internal and external sources, such as:

i. The AI's heads of business lines and relationship managers;
ii. Internal/external audit and regulatory findings;
iii. Sectoral emerging risks and typologies;
iv. Corruption indices and country risk reports;
v. Guidance issued by regulators;
vi. Threat reports and typologies issued by the FIC and law enforcement agencies;
vii. National Risk Assessment Reports;
viii. Independent and public assessment of a country's or jurisdiction's overall AML/CFT&P regime such as Mutual Evaluation report and IMF Financial Sector Assessment Programme Reports.
ix. Public sources of adverse news or relevant public criticism of a country or jurisdiction, including FATF, GIABA and public statements.

### ML/TF&PF RISK ASSESSMENTS

There is no single prescribed or universally accepted methodology for conducting an AML/CFT&P risk assessment. A risk assessment shall consist of three but related steps:

i. identification of ML/TF&PF risk, and
ii. assessment of the ML/TF&PF risk and
iii. the exposure of the AI to ML/TF&PF.

The steps taken to identify and assess ML/TF&PF risk must be proportionate to the nature, size and complexity of the AI. AIs that do not offer complex products or services and have limited or no international exposure may not need an overly sophisticated risk assessment. However, where products and services offered by the AI are more varied and where there are multiple subsidiaries and different business units catering to a more diverse customer base through multiple delivery channels, the AI shall conduct a more comprehensive risk assessment and identify and assess the ML/TF&PF risks on a group-wide level across all its business units, product lines and delivery channels.

In conducting the risk assessment to identify those areas of its business that may be susceptible to ML/TF&PF risk, the AI shall consider the following risk factors where applicable:

i. In relation to customers:
    - Target customer markets and segments;
    - Profile and number of customers identified as higher risk;
    - Complexity, volume and size of its customers' transfers, considering the usual activity and the risk profile of its customers (e.g. whether the ownership structure is highly complex; whether the customer is a PEP; whether the customer's employment income supports account activity).

ii. In relation to the countries or jurisdictions the AI is exposed to, either through its cross border and international operations or through the activities of its customers, including correspondent relationships, the AI shall consider the countries or jurisdictions:
    - The AML/CFT laws, regulations and standards of the country or jurisdiction and quality and effectiveness of implementation of the AML/CFT regime;
    - Contextual factors such as political stability, maturity and sophistication of the regulatory and supervisory regime, level of corruption, financial inclusion etc.

iii. In relation to the products, services, transfers and delivery channels of the AI shall consider:
    - Nature, scale, diversity and complexity of the financial institution's business activities including its geographical diversity;
    - Nature of products and services offered by the financial institution;

- Delivery channels, including the extent to which there is direct interaction between the financial institutions and the customer or the extent to which reliance is placed on technology, intermediaries, third parties, correspondents or non-face to face access;
- the degree to which the operations are outsourced to other entities in the Group or third parties; and
- The development of new products and new business practices, including new delivery mechanisms and partners; or the use of new or developing technologies for both new and pre-existing products.

**RISK ASSESSMENT TEMPLATE**

This template is not intended as a substitute for the requirement for an AI to determine the most appropriate way to categorize and weigh ML/TF&PF risks. AIs are expected to perform their own due diligence in determining the most appropriate methodology for conducting the assessment.

**IDENTIFICATION OF SPECIFIC RISK CATEGORIES**

The first step of the risk assessment process is to identify at a minimum customers, countries or geographic areas, products, services, transactions and delivery channels unique to the AI. Although attempts to launder money, finance terrorism, proliferation financing or conduct other illegal activities through an AI 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 an AI interacts with the customer (face- to-face contact versus electronic banking) should also be considered. These factors risks will vary from AI to another.

**PRODUCT, SERVICE, TRANSACTION OR DELIVERY CHANNEL RISK FACTORS**

Certain products and services offered by AIs may pose a higher risk of ML/TF&PF depending on the nature of the specific product or service offered. Some products and services

may facilitate a higher degree of anonymity or involve the handling of high volumes of currency or currency equivalents. Examples of these products and services are listed below;

1. Private/Prestige banking,
2. Non-face-to-face business relationships or transactions,
3. Payment(s) received from unknown or un-associated third parties

**CUSTOMER RISK FACTORS**

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

1. The business relationship is conducted in an unusual circumstance (e.g. significant unexplained geographic distance between the AI and the customer).
2. Non-resident customers.
3. Legal persons or arrangements that are personal asset-holding vehicles.
4. Business that are cash-intensive.
5. The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

**GEOGRAPHICAL RISK FACTORS (LOCAL)**

It is essential for AI's AML/CFT&P compliance programs that they identify geographic locations that may pose a higher risk. AIs shall 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.

**GEOGRAPHIC RISK FACTORS (INTERNATIONAL) GENERALLY**

1. Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT&P systems.
2. Countries subject to sanctions, embargos or similar measures issued by for example UNSCRs, OFAC, EU.
3. Countries identified by credible sources as having significant levels of corruption or other criminal activity.

4. 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.

AI's in its risk assessment framework shall identify the risks various delivery channels pose. AIs shall understand and evaluate the specific risks associated with their delivery channels.

Delivery channels, includes the extent to which there is direct interaction between the AIs and the customer or the extent to which reliance is placed on technology, intermediaries, third parties, correspondents or non-face-to-face.

Examples include:

1. Branch Banking
2. Mobile/ Phone Banking
3. ATM/POS channel of banking
4. Tele-Banking
5. Self- Service banking
6. Internet / Online/ E- banking

**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&P risk. When assessing the ML/TF&PF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, an AI shall take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures.

Examples of such variables include:

1. The purpose of an account or relationship.
2. The source and level of assets (funds) to be deposited by a customer or the size of transactions undertaken.
3. The regularity or duration of the business relationship.

4. Location and delivery channel of the transaction

**DEVELOPING THE BANK'S AML/CFT COMPLIANCE PROGRAMME BASED ON ITS RISK ASSESSMENT**

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

Audit shall review the AI's risk assessment for adequacy and completeness. Additionally, management shall 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 high-risk AML/CFT&P profile, management shall provide a more robust AML/CFT&P compliance programme that specifically monitors and controls the high risks that management and the board have accepted.

**CONSOLIDATED AML/CFT&P COMPLIANCE RISK ASSESSMENT**

AI that implement a consolidated or partially consolidated AML/CFT&P compliance programme should assess risk both individually within business lines and across all activities and legal entities. Aggregating AML/CFT&P 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&P risk exposures, the bank should continually reassess its AML/CFT&P risks, review its risk rating of customers and communicate with business units, functions, and legal entities. The identification of an AML/CFT&P risk or deficiency in one area of business may indicate concerns elsewhere in the

organization, which management shall identify and control.

**PERIODIC RISK ASSESSMENT AND RATING**

An effective AML/CFT&P compliance programme controls risks associated with the AI's 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 AI's risk profile, as necessary (e.g., when new products and services are introduced, existing products and services change, high-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 AIs to periodically reassess their AML/CFT&P risks at least every 12 to 18 months.

## APPENDIX E - MONEY LAUNDERING, TERRORISTFINANCING AND PROLIFERATION FINANCING "RED FLAGS"

### INTRODUCTION

Monitoring and reporting of suspicious transactions is key to AML/CFT&P effectiveness and compliance. AIs 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 ML/TF&PF are numerous, it is possible to identify certain basic features which tend to give reasonable cause for suspicion of ML/TF&PF. This appendix, which lists various transactions and activities that indicate potential ML/TF&PF, is not exhaustive. It does reflect the ways in which ML/TF&PF have been known to operate.

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

### SUSPICIOUS TRANSACTIONS "RED FLAGS"

i. **Potential Transactions Perceived or Identified as Suspicious**

a. Transactions involving high-risk countries/jurisdictions vulnerable to ML/TF&PF, subject to this being confirmed.
b. Transactions involving shell banks/companies.
c. Transactions with correspondents that have been identified as high-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 AIs 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 AIs**

The following transactions may indicate possible ML/TF&PF, 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 AI 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 who 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 AI or different AIs 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 AI 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 AIs.

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 customer accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other customer 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 AI 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 F - STATUTORY RETURNS

| TYPE OF REPORT | RECEPIENT BODY | CHANNEL | FREQUENCY |
|---|---|---|---|
| **Compliance Report**<br>This shall include but not limited to the following keys areas<br>1. **Staff AML/CFT&P Trainings**<br>2. **Additional AML/CFT&P Risk Assessment**<br>3. **Additional Procedures and Mitigants**<br>4. **New Technologies'/Products, Non-face-to-face Transactions**<br>5. **Reliance on Intermediaries or Third-Party Service Providers**<br>6. **Update appointment / re-designation / dismissal / resignation / retirement**<br>7. **Monitoring of Employee Conduct**<br>8. **Fraud activities**<br>9. **Review of Risk Assessment Conducted**<br>10. **Review of AML/CFT&P policy/framework**<br>11. **Record Keeping Procedures**<br>12. **Update on AML/CFT&P Software/Application**<br>13. **Statistics of STRs, CTRs and ECTRs** submitted to the FIC during the review period | BOG & FIC | Hardcopy or E-mail (info.aml@bog.gov.gh / info@fic.gov.gh) | **HALF YEARLY** (not later than the 15th day of the month after the half year); and<br>**END OF YEAR** (not later than the 15th day of the month after the end of year) |

| | | | |
|---|---|---|---|
| 14. **Other relevant compliance activities** | | | |
| **Employee Education & Training Programme** | BOG & FIC | Hardcopy or E-mail (info.aml@bog.gov.gh / info@fic.gov.gh) | **YEARLY** (not later than 31st December of every financial year) |
| **Independent Audit Report on the AML/CFT&P function**<br><br>The report may include but not limited to the following areas:<br><br>1. Review of AML/CFT&P programme for the year<br>2. Board/staff training<br>3. Review of AML/CFT&P policy & Risk Assessment Framework<br>4. Filing of CTRs/STRs/ECTRs<br>5. Transaction Monitoring<br>6. KYC/CDD/EDD on customers<br>7. Review of AMLROs account<br>8. Due diligence on new staff<br>9. Any other AML/CFT&P related activity | BOG & FIC | Hardcopy or E-mail (info.aml@bog.gov.gh / info@fic.gov.gh) | **YEARLY** (not later than 15th day of January) |
| **Annual AML/CFT&P Self Risk Assessment Questionnaire** | BOG | ORASS / Email (info.aml@bog.gov.gh) | **YEARLY** (not later than 15th day of January) |
| **Quarterly Returns (Data Capture)** | BOG | ORASS / Email (info.aml@bog.gov.gh) | **QUARTERLY** (not later than the 15th day of the month after the end of the quarter) |
| **Updated PEP List** | BOG | Email (info.aml@bog.gov.gh) | **QUARTERLY** (not later than the 15th day of the month after the end of the quarter) |
| **Fraud and Defalcation Report** | BOG | ORASS / Email (info.aml@bog.gov.gh) | **As and When** |
| **Disengaged Staff Return** | BOG | ORASS / Email (info.aml@bog.gov.gh) | **As and When** |

| | | | |
|---|---|---|---|
| **Engaged Staff (BoG opinions)** | BOG | Hardcopy / Email (info.aml@bog.gov.gh) | **As and When** |

## REFERENCES


1. Anti-Money Laundering Act, 2020 (Act 1044)
2. Anti-Terrorism Act, 2008 (Act 762) as amended
3. Anti- Money Laundering Regulations, 2011 (L.I. 1987)
4. Anti-Terrorism Regulations, 2012 (L.I. 2181)
5. Banks and Specialised Deposit Taking Institutions Act, 2016 (Act 930)
6. Foreign Exchange Act, 2007 (Act 723) and Regulations
7. Notices and Guidelines issued by Bank of Ghana for the regulation of Foreign Exchange Bureaux
8. Criminal and Other Offences Act, 1960 (Act 29) as amended
9. Payment Systems and Services Act, 2019 (Act 987)
10. Bank of Ghana Guideline for Inward Remittance Services by Payment Service Providers, February 2021
11. Bank of Ghana Corporate Governance Directive for Banks, Savings and Loans Companies, Finance Houses and Financial Holding Companies, 2018
12. Bank of Ghana Corporate Governance Directive for Rural and Community Banks, 2021
13. Central Bank of Trinidad and Tobago Anti-Money Laundering Guideline, 2018
14. Financial Action Task Force (FATF) Recommendations