

**BANK OF GHANA
AND
FINANCIAL INTELLIGENCE
CENTRE**

**ANTI-MONEY LAUNDERING /
COMBATING THE FINANCING OF
TERRORISM / COMBATING
PROLIFERATION FINANCING OF
WEAPONS OF MASS DESTRUCTION
(AML/CFT/CPF) GUIDELINE
FOR ACCOUNTABLE INSTITUTIONS**

SEPTEMBER, 2025

FOREWORD

The world has experienced phenomenal growth in financial services interconnectedness over the last few decades. This globalisation has led to increased cross-border activities, which is enhancing global financial intermediation. Unfortunately, this development has heightened transnational organised crimes, including Money Laundering, Terrorist Financing and Proliferation Financing (ML/TF/PF), perpetuated by both formal and underground actors.


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, Accountable Institutions (AIs) need to have robust Anti-Money Laundering, Combating the Financing of Terrorism and Combating Proliferation Financing of Weapons of Mass Destruction (AML/CFT/CPF) frameworks.

ML/TF/PF affects economies, and consequently impacts negatively on the economic, political and social developments, posing serious challenges across the globe.

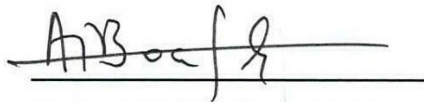
The need for countries to have strong anti-money laundering mechanisms, coupled with the enhancement of transparent financial integrity, cannot therefore be overemphasised. Ghana is determined to maintain a sound financial system and to join global efforts to prevent the scourge of ML/TF/PF.

In pursuit of the above goal and 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 in designing and implementing their respective AML/CFT/CPF compliance frameworks.

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

EFFECTIVE DATE

This revised AML/CFT/CPF Guideline comes into effect from the date of issue and replaces the BOG/FIC AML/CFT/CPF Guideline, 2022.

PUBLIC

RESPONSIBILITIES OF ACCOUNTABLE INSTITUTIONS(AIs)

1. All AIs must conduct gap analysis of their AML/CFT/CPF policies and Risk Assessment Framework to align with the requirements of this Guideline and submit the following to Bank of Ghana and the Financial Intelligence Centre
2. AIs will be required to conduct their AML/CFT/CPF audits using this revised Guideline.
3. For a robust AML/CFT/CPF function, the following officers of an AI shall be responsible for the effective implementation of this Guideline and other AML/CFT/CPF legislations.
 - i. Anti-Money Laundering Reporting Officer (AMLRO)
 - ii. Board and Management
 - iii. Internal Audit
 - iv. Heads of Business Units
 - v. Human Resource Team
 - vi. Customer Services Officers

PUBLIC

TABLE OF CONTENTS

FOREWORD.....	Error! Bookmark not defined.
EFFECTIVE DATE.....	iii
LIST OF ACRONYMS & ABBREVIATIONS	ix
INTRODUCTION.....	xi
OBJECTIVE OF THIS GUIDELINE.....	xii
DEFINITIONS	xiii
SCOPE OF UNLAWFUL ACTIVITIES.....	xiv
OVERVIEW OF THIS GUIDELINE	xv
PART A - OBLIGATIONS AND CO-OPERATIONS AMONG COMPETENT AUTHORITIES ...	1
1.0 AML/CFT/CPF OBLIGATIONS OF BANK OF GHANA	1
1.1 CO-OPERATION AND INFORMATION SHARING WITH COMPETENT AUTHORITIES	1
1.2 ACCOUNTABLE INSTITUTIONS CO-OPERATION WITH COMPETENT AUTHORITIES	2
PART B - SCOPE OF AML/CFT/CPF REGIME	3
2.0 AML/CFT/CPF INSTITUTIONAL POLICY FRAMEWORK.....	3
2.1 ASSESSING AML/CFT/CPF RISKS AND APPLYING RISK-BASED APPROACH.....	3
2.2 AML/CFT/CPF RISK ASSESSMENT FOR NEW PRODUCTS AND NEW TECHNOLOGIES.....	4
2.3 AML/CFT/CPF GOVERNANCE FRAMEWORK.....	4
2.3.1 CULTURE OF COMPLIANCE.....	4
2.3.2 ROLE OF THE BOARD OF DIRECTORS (BOARD)	4
2.3.3 ROLE OF SENIOR MANAGEMENT	5
2.3.4 ROLE AND DUTIES OF ANTI-MONEY LAUNDERING REPORTING OFFICER	

(AMLRO)	6
2.3.5 INTERNAL CONTROLS, COMPLIANCE AND AUDIT	7
2.3.6 TESTING FOR THE ADEQUACY OF THE AML/CFT COMPLIANCE PROGRAMME	8
2.4 CUSTOMER DUE DILIGENCE PROGRAMME.....	8
2.4.1 CONDUCTING CUSTOMER DUE DILIGENCE	8
2.4.2 CUSTOMER DUE DILIGENCE PROCEDURES (IDENTIFICATION AND VERIFICATION)	9
2.4.3 TIMING OF VERIFICATION	11
2.4.4 EXISTING CUSTOMERS.....	11
2.4.5 NEW BUSINESS FOR EXISTING CUSTOMERS	12
2.4.6 FAILURE TO COMPLETE CDD	12
2.5 CATEGORIES OF CUSTOMERS, TRANSACTIONS OR PRODUCTS	12
2.5.1 LOW RISK CUSTOMERS, TRANSACTIONS OR PRODUCTS	12
2.5.2 HIGH-RISK CUSTOMERS, TRANSACTIONS OR PRODUCTS	13
2.6 SPECIFIC HIGH-RISK CUSTOMERS, PRODUCTS, ENTITIES, LOCATIONS OR TRANSACTIONS.....	13
2.6.1 POLITICALLY EXPOSED PERSONS (PEPs)	13
2.6.2 CROSS-BORDER CORRESPONDENT BANKING.....	15
2.6.3 NEW TECHNOLOGIES AND NON-FACE-TO-FACE TRANSACTIONS.....	15
2.6.4 VIRTUAL ASSETS (VAs) AND VIRTUAL ASSETS SERVICE PROVIDERS (VASPs) .	17
2.6.5 RELIANCE ON INTERMEDIARIES AND THIRD-PARTY SERVICE PROVIDERS FOR CDD PROCEDURES.....	18
2.6.6 HIGH-RISK COUNTRIES.....	20
2.6.7 FOREIGN BRANCHES AND SUBSIDIARIES.....	20
2.6.8 MONEY OR VALUE TRANSFER SERVICES (MVTs).....	21
2.6.9 FOREIGN EXCHANGE BUREAUX.....	23
2.6.10 WIRE/ELECTRONIC TRANSFERS AND PAYMENT TRANSACTIONS	23
2.6.11 PROVISION OF SAFE CUSTODY AND SAFE DEPOSIT BOXES.....	27

2.6.12 SHELL BANKS AND SHELL COMPANIES	27
2.7 REQUIREMENTS FOR NON-PROFIT ORGANISATIONS (NPOs)	27
2.7.1 NON-PROFIT ORGANISATION (NPO)	28
2.7.2 REGISTERED CHARITIES	28
2.7.3 RELIGIOUS ORGANIZATIONS (ROs)	28
2.8 SUSPICIOUS ACTIVITY / TRANSACTION REPORTING (SAR/STR), TIPPING OFF AND CONFIDENTIALITY AND TRANSACTION MONITORING	29
2.8.1 DEVELOPMENT AND IMPLEMENTATION OF INSTITUTIONAL POLICY ON SARs/STRs	29
2.8.2 COMPLEX, UNUSUAL OR LARGE TRANSACTIONS	29
2.8.3 SUSPICIOUS TRANSACTION REPORTING	30
2.8.4 TIPPING OFF AND CONFIDENTIALITY	30
2.8.5 TRANSACTION REPORTING	31
2.8.6 TRANSACTION MONITORING	31
2.8.6.1 TRANSACTION MONITORING SYSTEMS	32
2.9 IDENTIFICATION OF DESIGNATED ENTITIES AND PERSONS & FREEZING AND UNFREEZING OF FUNDS	33
2.10 TRADE/ECONOMIC SANCTIONS	34
2.11 KNOW YOUR EMPLOYEE	35
2.11.1 MONITORING OF EMPLOYEE CONDUCT	36
2.12 EMPLOYEE-EDUCATION AND TRAINING PROGRAMME	37
2.13 WHISTLEBLOWER POLICY	38
2.14 FRAUD MANAGEMENT	38
2.15 RECORD KEEPING	40
2.16 STATISTICS	40
PART C - KNOW YOUR CUSTOMER (KYC) / CUSTOMER DUE DILIGENCE (CDD) / ENHANCED DUE DILIGENCE (EDD) PROCEDURES	41
3.0 ESTABLISHMENT OF BUSINESS RELATIONSHIP	41
3.1 WHAT IS IDENTITY	41

3.2	DUTY TO OBTAIN IDENTIFICATION EVIDENCE	41
3.3	ESTABLISHMENT OF IDENTITY.....	41
3.4	VERIFICATION OF IDENTITY	42
3.5	CUSTOMERS TO BE VERIFIED	42
3.6	TIMING OF IDENTIFICATION	43
3.7	RISK-BASED APPROACH TO CUSTOMER IDENTIFICATION AND VERIFICATION 44	
3.8	RISK-BASED CUSTOMER DUE DILIGENCE	44
3.8.1	LOW RISK/SIMPLIFIED DUE DILIGENCE (SDD)	44
3.8.1.1	MINIMUM SDD MEASURES	45
3.8.1.2	FINANCIAL INCLUSION	46
3.8.2	ENHANCED DUE DILIGENCE (HIGH-RISK).....	47
3.8.2.1	MINIMUM EDD MEASURES.....	48
3.8.2.2	ENHANCED MONITORING	49
3.8.3	MINORS / STUDENTS	49
3.9	VIRTUAL ASSETS (VAS) AND VIRTUAL ASSETS SERVICE PROVIDERS (VASPS) 50	
	REGULATORY REPORTING OBLIGATIONS	52
	SANCTIONS FOR NON-COMPLIANCE	52
	APPENDIX A - DEFINITION OF TERMS	53
	APPENDIX B - INFORMATION TO ESTABLISH IDENTITY	61
	APPENDIX C – SUPERVISORY GUIDANCE NOTE ON THE USE OF THE GHANA CARD ...	71
	APPENDIX D - FURTHER GUIDANCE ON RISK ASSESSMENT AND BUSINESS/CUSTOMER RISK RATING	72
	APPENDIX E - MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING “RED FLAGS”	79
	APPENDIX F - STATUTORY RETURNS	86

LIST OF ACRONYMS & ABBREVIATIONS

AI	-	Accountable Institution (Bank of Ghana Licensed Institutions)
AML	-	Anti-Money Laundering
AML/CFT/CPF	-	Anti-Money Laundering, Combating the Financing of Terrorism and Combating Proliferation Financing of Weapons of Mass Destruction
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	-	Combating Proliferation Financing of Weapons of Mass Destruction
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 Organisations
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
WMD	-	Weapons of Mass Destructions

PUBLIC

INTRODUCTION

Following the outcome of the second-round mutual evaluation, which was geared toward assessing the effectiveness of available mechanisms and frameworks, Ghana was placed on an enhanced follow-up process due to identified strategic deficiencies in its AML/CFT/CPF regime. Among these gaps were inconsistencies in the Anti-Money Laundering Act, 2008 (Act 749) as amended and lack of effective, dissuasive and proportionate sanctions for money laundering offences. Subsequently, to improve the legal framework as identified during the 2nd Mutual Evaluation, Act 749 and its amendments were repealed for a comprehensive Anti-Money Laundering Act, 2020 (Act 1044). Ghana has in place other existing laws in the fight against ML/TF/PF, which includes the Anti-Terrorism Act, 2008 (Act 762), Anti-Terrorism (Amendment Act), 2012 (Act 842), the Anti-Terrorism (Amendment Act), 2014 (Act 875), Anti-Money Laundering Regulations, 2011 (L.I. 1987).

Accordingly, this Guideline is issued in line with AML/CFT/CPF Acts and Regulations to ensure that AIs put in place effective AML/CFT/CPF regime, which also conforms with Financial Action Task Force (FATF) standards, Basel Principles and other best international practices on AML/CFT/CPF.

To ensure an effective compliance regime, a provision on Know Your Customer/Customer Due Diligence/Enhanced Due Diligence (KYC/CDD/EDD) procedures have been provided in this Guideline to assist AIs.

OBJECTIVE OF THIS GUIDELINE

This Guideline is being issued pursuant to sections 52 and 61 of Act 1044 and section 92(2)(a)(vii) of the Banks and Specialised Deposit-Taking Institutions Act, 2016 (Act 930) and is intended to assist AIs to:

1. Understand and apply practicable steps to comply with AML/CFT/CPF laws and regulatory requirements;
2. Develop and implement an effective risk-based approach to identify, assess and understand their ML/TF/PF risks.
3. Understand the expectations of the Bank of Ghana with respect to the minimum standards for AML/CFT/CPF regime and to build a culture of compliance;
4. Provide adequate guidance in conducting KYC/CDD/EDD measures; and
5. Understand the implications of non-compliance of AML/CFT/CPF requirements.

DEFINITIONS

Money Laundering (ML) is defined as the process where a person attempts to convert/conceal/disguise/transfer the illegal origin and/or illegitimate ownership of property and assets that are proceeds of criminal activities. (Refer to section 1 (2) of Act 1044). It is, thus, a derivative crime.

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

Terrorist financing offences occurs where a 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 organisation or by an individual terrorist.

Proliferation Financing (PF) is defined by Financial Action Task Force (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.” Natural /Legal Persons involved in these acts are identified and listed for targeted financial sanctions by the United Nations Security Council Resolutions (UNSCRs), third parties or on the domestic lists of affected countries.

SCOPE OF UNLAWFUL ACTIVITIES

The following are unlawful activities.

- i. Participation in an organised 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. Cybercrime
- xxiii. 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

This Guideline covers, among others, the following key areas of the AML/CFT/CPF regime:

- i. Anti-Money Laundering Reporting Officer designation and duties;
- ii. co-operation with supervisory and competent authorities;
- iii. customer due diligence;
- iv. monitoring and reporting of suspicious transactions /activities;
- v. record keeping; and
- vi. 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/CPF policies governing their operations should not only prescribe money laundering and predicate offences but also prescribe sanctions for non-compliance with the relevant AML/CFT/CPF requirements. It is, therefore, in the best interest of the institutions to entrench a culture of compliance which would be facilitated by this Guideline.

This Guideline is structured as follows;

Part A – Obligations and co-operations among competent authorities

Part B – Scope of AML/CFT/CPF Regime

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

Appendices

References

PUBLIC

PART A - OBLIGATIONS AND CO-OPERATIONS AMONG COMPETENT AUTHORITIES

1.0 AML/CFT/CPF 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/CPF 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 both domestically and internationally 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 INSTITUTIONS CO-OPERATION WITH COMPETENT AUTHORITIES

1. AIs shall comply with all requests made pursuant to the law, regulations, guidelines and other enforceable means and provide information to the BOG, FIC and other relevant competent authorities. Failure to comply with such requests shall attract sanctions.
2. AIs' procedures for responding to authorised 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 - SCOPE OF AML/CFT/CPF REGIME

2.0 AML/CFT/CPF INSTITUTIONAL POLICY FRAMEWORK

1. All AIs shall develop and implement policies indicating their commitment to comply with AML/CFT/CPF 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/CPF RISKS AND APPLYING RISK-BASED APPROACH

1. The AI's AML/CFT/CPF risk assessment 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.
2. In assessing ML/TF/PF risks, AIs are required to undertake the following:
 - i. develop ML/TF/PF risk assessment policies, controls and procedures.
 - ii. consider all the relevant risk factors before determining the level of overall risk, the specific risk level and type of mitigation to be applied.
 - iii. document all risk assessments undertaken.
 - iv. obtain Board/Senior Management approval prior to implementation.
 - v. keep the assessment up-to-date through a periodic review within a two-year cycle. However, in the event of a significant occurrence and or results from the NRA, the AI shall review and update its risk assessment policies, controls and procedures.
 - vi. monitor the implementation of the ML/TF/PF risk assessment policies, controls and procedures to identify new risk areas.
 - vii. update ML/TF/PF risk assessment policies, controls and procedures with identified new areas of potential ML/TF/PF risks.
 - viii. provide the updated ML/TF/PF risk assessment policies, controls and procedures to Board/Senior Management, BOG and FIC.
 - ix. design additional controls and procedures in their AML/CFT/CPF operational

- Guidelines for the newly identified risks and
 - x. conduct additional risk assessment as and when required by the BOG and FIC.
3. AIs shall be guided by the results of the National Risk Assessment (NRA) Reports in conducting their respective risk assessments.

2.2 AML/CFT/CPF RISK ASSESSMENT FOR NEW PRODUCTS AND NEW TECHNOLOGIES

1. AIs shall review, identify and record areas of potential ML/TF/PF risks and submit to BOG for approval before new products and new technologies are launched.
2. AIs shall review their AML/CFT/CPF risk assessment frameworks periodically to determine their adequacy and identify other areas of potential risks associated with the new products and new technologies.
3. AIs shall adopt further Guidance on Risk Assessment and Risk Rating as provided in Appendix D.

2.3 AML/CFT/CPF GOVERNANCE FRAMEWORK

2.3.1 CULTURE OF COMPLIANCE

1. AIs shall have a comprehensive AML/CFT/CPF 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 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/CPF compliance programme. In this regard, the Board's oversight in respect of AML/CFT/CPF 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 and ensuring the independence of the AMLRO.
 - ii. Approving AML/CFT/CPF policy/manual.

- iii. Approving the AML/CFT/CPF compliance programme, training programme, compliance reports, and AML/CFT/CPF Risk Assessment Framework and Report.
 - iv. Ensuring the establishment of appropriate mechanisms to review key AML/CFT/CPF policies and procedures quarterly.
 - v. Approving new business relationships, products and services and its associated specific ML/TF risk.
 - vi. Ensuring the establishment of an AML/CFT/CPF risk management framework with clearly defined lines of authority and responsibility for AML/CFT/CPF and effective separation of duties between those implementing the policies and procedures and those enforcing the controls.
 - vii. Ensuring that the Board receives the requisite training on AML/CFT/CPF generally, as well as on the institution's specific AML/CFT &P risks and controls at least once a year.
 - viii. Ensuring that the AMLRO receives training on an ongoing basis to effectively perform his duties.
 - ix. Ensuring that the AMLRO is resourced adequately in terms of personnel, IT systems and budget to implement, administer and monitor the AML/CFT/CPF programme effectively.
 - x. Ensuring receipt of at minimum four (4) compliance reports in a year on the AI's AML/CFT/CPF function from the AMLRO for its information and necessary action including but not limited to:
 - a. Remedial action plans if any, to address the results of independent audits (either internal or external); regulatory reports received from the Bank of Ghana or other regulators on its assessment of the institution's AML/CFT/CPF programme;
 - b. results of compliance testing and self-identified instances of non-compliance with AML/CFT/CPF requirements;
 - c. Recent developments in AML/CFT/CPF laws and regulations and their implications if any, to the 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.
3. AIs shall submit copies of the approved AML/CFT/CPF policy and manual to the BOG within five (5) working days.

2.3.3 ROLE OF SENIOR MANAGEMENT

1. Senior Management shall be responsible and ensure adherence to established AML/CFT/CPF policies and procedures. Among other things, Senior Management shall 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/CPF laws, regulations and guidelines; and
 - iii. Are implemented effectively across business areas or throughout the financial group as applicable. contains succession planning for the AMLRO function.
2. Senior Management must review policies and procedures periodically for consistency with the AI's AML/CFT/CPF Programme. Attention shall be paid to identification, assessing and understanding of ML/TF/PF risks associated with new products/services and delivery channels; new business practices and new or developing technologies for new and existing products; and put measures in place to manage and mitigate such risks. Risk assessments shall 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/CPF programme are addressed in a timely manner;
 - ii. 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/CPF responsibilities.

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 and of minimum Senior Management grade/status in accordance with section 50(1)(b) of the Anti-Money Laundering Act, 2020 (Act 1044), Regulation 5(1) of L.I. 1987, section 156 of Act 930 and the BOG Corporate Governance Directive.
2. The AMLRO shall be a member of the highest Management Decision-Making Body of the AI.
3. The AMLRO shall report to the Board or a Sub-Committee of the Board to ensure operational independence.
4. The AMLRO must have sufficient authority, independence and seniority to be able to effectively carry out 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 a professional qualification in anti-money laundering and financial crime.
5. The duties of the AMLRO shall include, but not limited to the following:

- i. Develop written AML/CFT/CPF policies and procedures that are kept up to date and approved by the Board;
 - ii. Have oversight of the AML/CFT/CPF compliance programme in line with the institution's identified risk and other emerging risks;
 - iii. Receive and vet suspicious (unusual) transaction/activity reports from the employees;
 - iv. Conduct regular risk assessments of the inherent ML/TF/PF risks including assessments of new products, services, new technologies, processes and business initiatives to identify potential ML/TF/PF risks and develop appropriate control mechanisms;
 - v. File suspicious, Electronic Currency, Politically Exposed Persons, Cash Transaction Reports and other relevant regulatory reports with the BOG and FIC (where applicable);
 - vi. Ensure systems, resources, including fraud control management are in place to detect and report suspicious transactions and attempted transactions,
 - vii. 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;
 - viii. Submit at minimum four (4) reports to the Board and Senior Management regarding the adequacy of the AML/CFT/CPF framework or any associated issues; and
 - ix. 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.
6. AIs shall ensure that the AMLRO has access to all information that may be relevant to him/her in consideration of a suspicious or unusual transaction/activity report which includes timely access to customer identification data, CDD information, transaction records and other relevant information.
 7. The AMLRO in collaboration with audit and operational team shall be responsible for fraud management within the AI.
 8. AIs shall put in place a structure that ensures the operational independence of the AMLRO.

2.3.5 INTERNAL CONTROLS, COMPLIANCE AND AUDIT

1. AIs are required to implement programmes against ML/TF/PF which have regard to the ML/TF/PF risks and the size of the business which include the following internal policies, procedures and controls:
 - a. Compliance management arrangements (including the appointment of AMLRO at management level)
 - b. Screening procedures to ensure high standards when hiring employees
 - c. KYC/CDD/EDD procedures
 - d. Ongoing employee training programme
 - e. Independent audit function to test the system
 - f. Monitoring of transactions for the detection and reporting of unusual and suspicious transactions

- g. Record-keeping
2. AIs shall communicate these internal policies, procedures and controls to their employees.

2.3.6 TESTING FOR THE ADEQUACY OF THE AML/CFT COMPLIANCE PROGRAMME

1. AIs shall make a policy commitment and subject their AML/CFT/CPF compliance programme to independent testing.
2. It is important that these reviews are performed by auditors (internal or External) who have had appropriate AML/CFT/CPF training and experience in respect of ML/TF/PF risk and an appropriate level of knowledge of the regulatory requirements and guidelines. It is required that the auditor shall determine the adequacy, completeness and effectiveness of the AML/CFT/CPF compliance programme.
3. Where an AI 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/CPF compliance programme shall be submitted to the BOG and FIC not later than January 15 of every financial year.
5. The AI shall promptly address any identified weaknesses or inadequacies and provide an update to BOG and FIC.

2.4 CUSTOMER DUE DILIGENCE PROGRAMME

1. AIs shall 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 shall identify which customers or categories of customers present higher risk and require the application of enhanced due diligence (EDD).
2. Where the AIs determine that a customer or a category of customers presents low risk, a simplified due diligence (SDD) measure shall, at a minimum, be applied as stated in this Guideline.
3. Where SDD measures are applied on the basis of an assessment of low ML/TF/PF risk, the AML/CFT/CPF policies and procedures shall clearly articulate the rationale and the applicable measures to be undertaken.

2.4.1 CONDUCTING CUSTOMER DUE DILIGENCE

1. AIs shall undertake customer due diligence (CDD) in accordance with 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;
2. AIs are exempted from performing CDD for the following transactions
 - i. Any transfer flowing from a transaction carried out using an issuer's credit or debit card on the issuing AI's terminal/channel such as ATM or point of sale (POS) or channels for payment of goods.
 - ii. AI-to-AI transfers and settlements.
 3. CDD is the identification and verification of both the customer and beneficiary, including but not limited to continuous monitoring of the business relationship by the AIs.
 4. AIs are not permitted to operate anonymous accounts or accounts in fictitious names.

2.4.2 CUSTOMER DUE DILIGENCE PROCEDURES (IDENTIFICATION AND VERIFICATION)

CDD procedures outlined below apply to customers at onboarding and existing customers.

1. AIs shall identify and verify customers' identities using the Ghana Card during onboarding.
2. AIs shall verify customers using the Ghana Card for financial transactions on a risk-based approach.
3. AIs in conducting CDD procedures in relation to the Ghana Card shall undertake the following
 - i. Identify and biometrically verify all third-party transactions
 - ii. Implement multifactor authentication and liveness check for all transactions on mobile banking application during onboarding.
4. AIs shall refer to Appendix B for KYC/CDD/EDD requirements during onboarding and ongoing due diligence.
5. AIs shall obtain information on the purpose and intended nature of the business relationship of their potential customers.
6. AIs shall conduct ongoing due diligence on the business relationship with existing

customers in line with the risk associated with the customer, i.e. high-risk, yearly etc.

7. Where the ongoing due diligence includes scrutinizing the transactions undertaken by the customer, AIs shall ensure that the transactions being conducted are consistent with the AI's knowledge of the business, risk profile, and the source of funds of the customer.
8. AIs shall screen customers at onboarding and against all domestic, international sanctions lists and internal list developed by the AI.
9. For existing customers, AIs shall screen existing customers based on transaction patterns and the receipt of new international sanctions list from the relevant authorities (United Nations Security Council Resolutions (UNSCR), Office of Foreign Assets Control (OFAC), European Union (EU), His Majesty's Treasury, African Union (AU), Economic Community of West African States (ECOWAS).
10. AIs shall ensure that documents, data or information collected under the KYC/CDD/EDD process are kept up-to-date.
11. 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 competent authority responsible for the registration and licensing of legal persons and legal arrangements.
 - 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.
12. AIs shall identify a beneficial owner(s) (BOs) and take measures to verify the identity of the BOs using relevant information or data obtained from a reliable source to satisfy that the AI knows who the B/O(s) is/are (BOs with 5% or more controlling interest).
13. 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 which include obtaining sufficient identification data (the name, address, contact, purpose of transaction, and signature) and verifying the identity of the third party (acting on behalf of the other person).
14. AIs shall take measures in respect of customers that are legal persons or legal arrangements to:
 - i. understand the ownership and control structure; and
 - ii. determine the natural persons who exercise ultimate ownership and/or control of such a customer.
15. 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 recognised stock exchange), the AI shall apply a risk-based approach to identify and verify the identity of the shareholders of such a public company.

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.
2. Where a customer is permitted to utilize the business relationship prior to verification in order not to interrupt the business or transaction, AIs are required to adopt risk-based procedures to effectively mitigate ML/TF/PF risks and document the rationale for such an activity.
3. AIs shall follow procedures that include measures such as limits on the number, types and amount of transactions that can be performed.
4. AIs shall undertake the activity of paragraph 2 above only on one occasion.

2.4.4 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 shall include, when:
 - i. a transaction of significant value takes place,
 - ii. a receipt or transfers of a negligible yet consistently frequent amount on the customer's account
 - iii. customer documentation change substantially,
 - iv. there is a material change in the way that the account is operated,
 - v. the institution becomes aware that it lacks sufficient information about an existing customer.
 - vi. customer is onboarded onto a high-risk product/service of the AI.
3. In the absence of the above, AIs shall take appropriate steps to update customer records within a one-year (1-year) cycle for high-risk customers, three-year (3-year) for medium-risk customers and at least five-year (5-year) for low-risk customers.
4. An AI shall properly identify the customer in accordance with the criteria above. The customer identification records shall be made available to the AMLRO and competent authorities as and when needed.

2.4.5 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 reactivated.
2. In the circumstances above, details of the previous account(s) and any identification evidence previously obtained or any introduction records shall be updated and linked to the new account records and retained for the prescribed period in accordance with section 32 of Act 1044.

2.4.6 FAILURE TO COMPLETE CDD

1. An AI that is unable to perform the CDD requirements under this Guideline:
 - i. shall not open the account, commence business 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.

2.5 CATEGORIES OF CUSTOMERS, TRANSACTIONS OR PRODUCTS

2.5.1 LOW RISK CUSTOMERS, TRANSACTIONS OR PRODUCTS

1. AIs shall apply reduced or simplified measures where there are low risks. Examples of low-risk customers include but not limited to:
 - a. Public companies (listed on a stock exchange) that are subject to regulatory disclosure requirements;
 - b. Life insurance policies where the annual premium and single monthly premium are within the threshold determined by the National Insurance Commission (NIC);
 - c. Insurance policies for pension schemes if there is no surrender-value clause and the policy cannot be used as collateral;
 - d. 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;
 - e. Any other low-risk as may be determined by the National Risk Assessment findings.
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.

2.5.2 HIGH-RISK CUSTOMERS, TRANSACTIONS OR PRODUCTS

1. AIs shall perform enhanced due diligence (EDD) for high-risk categories of customers, business relationships or transactions. 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.
2. 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) and their associates;
 - vi. High Net Worth individuals;
 - vii. Religious Groups and Leaders;
 - viii. Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs)
 - ix. Chief Executives and Board Members of privately-owned companies/corporations of High-Risk industries/sectors as defined by the NRA, emerging trends/AI's policy.
 - x. Cross-border banking and business relationships;
 - xi. Natural or legal persons who do business in precious metals/minerals, petroleum
 - xii. Designated Non-Financial Businesses and Professions;
 - xiii. Beneficial-owners of pooled-accounts held and managed by either a law firm or lawyer.
 - xiv. Any customer deemed high-risk by the AI; and
 - xv. other high-risk categories as may be determined by the NRA findings.
3. AIs shall take into consideration emerging trends and patterns in implementing CDD/EDD procedures relating to the products/services and other business relationship stated in the NRA.

2.6 SPECIFIC HIGH-RISK CUSTOMERS, PRODUCTS, ENTITIES, LOCATIONS OR TRANSACTIONS

2.6.1 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, Departments and Agencies (MDAs) and signatories;
 - vi. Metropolitans, Municipals and District Assemblies (MMDAs) and other public institutions and signatories;
 - 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 (domestic and foreign). and to manage any elevated risks. Business relationships with the family and known close associates of a PEP (domestic and foreign) shall also be subjected to greater scrutiny. These requirements are intended to be preventive and shall 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 BO is a PEP (domestic and foreign).
 4. AIs shall obtain senior management approval before they establish a business relationship with a PEP (domestic and foreign) 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 BO is subsequently found to be or becomes a PEP (domestic and foreign) or high-risk, the AI shall obtain senior management approval in order to continue the business relationship.
 6. AIs shall take measures to establish the source of wealth and the sources of funds of customers and BOs identified as PEPs (domestic and foreign) or high-risk which include obtaining information and the use of source of wealth form and report all anomalies immediately to the FIC and other relevant authorities.
 7. AIs in business relationships with PEPs (domestic and foreign) 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 (domestic and foreign).
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.

2.6.2 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, among others 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 an ML/TF/PF investigation or a regulatory action;
 - ii. Assess the correspondent institution's AML/CFT/CPF controls and ascertain that the latter are in compliance with FATF standards;
 - iii. Assess the correspondent institutions in relation to the Wolfsberg Questionnaire;
 - iv. Obtain approval from senior management before establishing correspondent relationships; and
 - v. Document and keep records of the EDD procedures undertaken.
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; and
 - ii. provide relevant EDD information and customers identification upon request to the correspondent bank.

2.6.3 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 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 are emerging as potential alternatives to traditional financial services.

2. AIs shall assess and document the specific 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. AI shall assess and identify emerging trends and patterns associated with new technologies, products and services and document same.
4. 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 product/services, business relationships or transactions. These policies and procedures shall be applied automatically when establishing customer relationships and conducting ongoing due diligence.
 - iii. AIs that rely on third-party service providers in deploying such new technologies, products or services shall satisfy themselves that the third-party is a regulated and supervised institution and has measures in place to comply with the requirements of KYC/CDD/EDD and reliance on intermediaries and other third parties as contained in this Guideline.
 - iv. AIs that rely on such third-party shall have measures in place to obtain the necessary information concerning proceeds which has been laundered, or which constitute proceeds of unlawful activities or means used to or intended for use in the commission of ML/TF/PF or any other unlawful acts to report to the FIC or other Competent Authorities.
 - v. AIs shall satisfy itself that copies of identification data and other relevant documentation relating to the KYC/CDD/EDD requirements will be made available from the third party upon request without delay.
 - vi. AIs shall verify customers during onboarding and ongoing transactions by adopting biometric, liveness checks and multifactor authentication tools, where applicable.
5. AIs in developing new technologies/products/services that would onboard customers through a non-face-to-face channel shall ensure the platform;
 - i. collects and keeps records of all identification documents and KYC/CDD/EDD requirements
 - ii. biometrically verify the customer using liveness check against the Ghana Card.
 - iii. identifies the customer uniquely during the course of business.
 - iv. aligns with the requirements in the Supervisory Guidance Note and this Guideline.
6. 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.

2.6.4 VIRTUAL ASSETS (VAs) AND VIRTUAL ASSETS SERVICE PROVIDERS (VASPs)

1. VASPs shall undertake EDD measures when
 - a. Establishing business relations; and
 - b. Carrying out transactions above the applicable designated threshold (USD/EUR 1000).
2. VASPs shall require, obtain and hold the accurate originator and beneficiary information on the virtual assets transfer.
3. The minimum required information;
 - a. Required originator information:
 - i. the name of the originator; and
 - ii. the originator account address, 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
 - iii. the Ghana Card number or the national identification document for foreign nationals, date and place of birth
 - b. Required beneficiary information:
 - i. the name of the beneficiary; and
 - ii. the beneficiary account address, 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
 - iii. the Ghana Card number or the national identification document for foreign nationals, date and place of birth
4. VASPs shall obtain and transmit the above information to the beneficiary VASPs or AI (if any) immediately and securely and make it available on request to the appropriate authorities.
5. Where several VA transfers from a single originator are bundled (mixed) in a block for transmission to beneficiaries, the block should be accompanied by the required and accurate originator information and full beneficiary information that is fully traceable.
6. VASP shall require and obtain the originator and the beneficiary account address, 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.
7. Whereas the cross-border wire/electronic transfers and payment transactions is below the threshold (USD 1,000 or cedi equivalent), VASP shall require, obtain and hold 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
- 8. VASP shall take measures to obtain and verify the missing originator and beneficiary information.
- 9. In cases where the missing originator and beneficiary information cannot be obtained, the VASP shall not execute the trade, transfer, conversions (fiat to crypto and crypto to fiat) and file a suspicious transaction to the FIC within twenty-four (24) hours.
- 10. In processing wire/electronic transfers, VASPs 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 successor resolutions.
- 11. In processing wire/electronic transfer, VA transfers and/or payment transactions, VASPs shall take freezing action and comply with prohibitions from conducting transactions with VA wallet, digital currency addresses, persons or entities listed on the OFAC Specially Designated Nationals (SDN) list and file a report to the FIC within twenty-four (24) hours.

2.6.5 RELIANCE ON INTERMEDIARIES AND THIRD-PARTY SERVICE PROVIDERS FOR CDD PROCEDURES

- 1. AIs are permitted to rely on third-party service providers to perform elements of KYC/CDD/EDD measures, such as identification of customers, identification of Beneficial Owner and nature of business. The ultimate responsibility for KYC/CDD/EDD measures shall remain with the AI relying on the third party.
- 2. AI shall undertake the following in relation to the third-party service provider;
 - i. ensure the third-party complies with elements of KYC/CDD/EDD measures set out in this guideline and the Ghana Card requirements.
 - ii. take steps to satisfy itself that copies of identification data and other relevant documentation relating to KYC/CDD/EDD requirements would be made available from the third-party upon request without delay.
 - iii. satisfy itself that the third party is regulated and supervised, and monitored
 - iv. has measures in place for compliance with record-keeping requirements as set out in this guideline and section 32 of Act 1044.

- v. Whereas the third-party service provider is outside Ghana, the AI shall ensure that it is regulated and supervised or monitored in a jurisdiction that complies with FATF standards and assess the level of risk within the jurisdiction
3. AIs shall undertake the following prior to establishing a business relationship with third-party service providers
 - i. conduct due diligence on the third party, which covers any adverse information about the company and directors/BOs etc.
 - ii. assess the risks associated with the third-party relationship and the solution/tool/software
 - iii. ensure board approval to engage the third-party service provider.
 - iv. ensure that there is a signed binding agreement
 - v. Ensure the third-party solution can undertake the following CDD measures:
 - (a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
 - (b) Identifying the beneficial owner and taking measures to verify the identity of the beneficial owner, such that the AI is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this shall include AIs' understanding of the ownership and control structure.
 - (c) Storing and keeping records.
 - vi. seek Bank of Ghana approval.
 - vii. conduct ongoing monitoring and assessment of the solution/tools/software to ensure it meets the KYC/CDD/EDD requirement as prescribed by the AML/CFT/CPF law, regulation and Guideline.
 4. AIs that rely on a third-party service provider that is part of the financial group, shall comply with the above requirements.
 5. AIs that rely on a third party that is part of the same financial group, shall ensure that
 - (a) the group applies CDD, record-keeping requirements, as well as measures in relation to PEPs as stated in Act 1044 and this Guidelines. Additionally, AIs must ensure that the financial groups has implemented group-wide programmes against ML/TF/PF which have regard to the ML/TF/PF risks and the size of the business and are applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group.
 - (b) the implementation of those CDD and record-keeping requirements and AML/CFT/CPF 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/CPF policies.
 6. The ultimate responsibility for customer identification and verification remains with the AIs when relying on intermediaries and third-party service providers.

7. AIs in addition to all above, shall adhere to the BOG third-party outsourcing directive.

2.6.6 HIGH-RISK COUNTRIES

1. AIs shall be required to apply enhanced due diligence, appropriate to the risks, to business relationships, transactions with natural and legal persons (including financial institutions) from countries as published by FATF.
2. AIs shall apply countermeasures proportionate to the risk:
 - a. When called upon to do so by the regulator/FIC
 - b. Independently of any call by the regulator/FIC
3. AIs shall report suspicious transactions that have no apparent economic or visible lawful purpose by customers from high-risk countries to the FIC.
4. 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 beneficial owners before business relationships are established from that jurisdiction;
 - ii. Enhanced monitoring on all financial transactions from such high-risk countries.
 - 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/CPF 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 and shall thus limit business relationships or financial transactions with the identified country or persons in that country.

2.6.7 FOREIGN BRANCHES AND SUBSIDIARIES

AIs that has established offices, branches or subsidiaries outside Ghana shall take note of the following:

1. AIs shall ensure that their foreign branches and subsidiaries observe group AML/CFT/CPF procedures consistent with the provisions of Act 1044 and FATF standards 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/CPF requirements and those of the host country differ, branches and subsidiaries or the 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. AIs shall be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT/CPF measures consistent with the home jurisdiction's requirements. This is to avoid regulatory gaps where the minimum AML/CFT/CPF requirement of the host jurisdiction is less strict than that of the home jurisdiction, to the extent that host jurisdiction laws and regulations permit. If the host jurisdiction does not permit the proper implementation of AML/CFT/CPF measures consistent with the home jurisdiction requirement, financial groups shall be required to apply appropriate additional measures to manage ML/TF/PF risks and inform their home supervisors.
4. These measures may include:
 - i. Policies and procedures for sharing information required for the purposes of CDD/EDD and ML/TF/PF risk management.
 - ii. the provisions, at group level compliance, audit and/or AML/CFT/CPF function, of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT/CPF purposes. This should include information and analysis of transactions or activities which appear unusual. Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management.
 - iii. adequate safeguards on the confidentiality and use of information, including safeguards to prevent tipping off.
5. AIs shall inform the BOG in writing when their foreign branches or subsidiaries are unable to observe the appropriate AML/CFT/CPF procedures because of a conflict with laws, regulations or other measures between the parent country (Ghana) and the host country (foreign).
6. AIs are subject to these AML/CFT/CPF principles and shall therefore apply consistently the KYC/CDD/EDD procedures at their group level taking into account the activity of the customer with the various branches and subsidiaries.

2.6.8 MONEY OR VALUE TRANSFER SERVICES (MVTs)

1. AIs shall undertake the following when establishing business relationship with an MVTs:
 - i. Ensure that it is licensed and supervised in a jurisdiction that complies with FATF standards and has been in operation for at least three (3) years
 - ii. Obtain and verify the license of the MVTs
 - iii. Conduct due diligence on the MVTs to include among other things; screening of the Directors/ BO/Shareholders, Adverse Media findings
 - iv. Ensure the MVTs has a robust AML/CFT/CPF program in place
 - v. Ensure the MVTs has procedures in place to file STRs
 - vi. Seek Board and BOG Approval
2. AIs shall ensure that MVTs comply with all the relevant requirements of Recommendation 16 of FATF standards as stated in Part 2.6.10 of this Guideline.
3. AI shall ensure that the MVTs obtains and maintains sufficient information on the

originator and beneficiary side of the wire/electronic transfer, and in accordance with section 32 of Act 1044.

- a. Required originator information:
 - i. the name of the originator;
 - ii. the originator unique transaction reference number, which permits traceability of the transaction;
 - iii. the originator's address, national identity number and/or customer identification number, or date and place of birth; and
 - iv. Purpose of transaction
 - b. Required beneficiary information:
 - i. the name of the beneficiary;
 - ii. the beneficiary account number or wallet where such transaction is terminated or, in the absence of an account/wallet, a unique transaction reference number which permits traceability of the transaction; and
 - iii. The beneficiary address, Ghana Card Number and/or customer identification number, or date and place of birth
4. AIs shall be required to undertake monitoring of transactions either by close of day or real-time, to identify cross-border wire/electronic transfers and payment transactions that lack required originator information or required beneficiary information.
 5. AIs shall take measures to obtain and verify the missing originator and beneficiary information.
 6. Where the AI is unable to obtain the required originator and/or beneficiary information associated with the wire/electronic transfers, the AI shall not execute the transfer and file a suspicious transaction to the FIC within twenty-four (24) hours.
 7. AIs shall conduct ongoing due diligence and monitoring of the MVTs regarding its operations, Directors/BOs and business to detect any adverse findings and review the decision to continue the business relationship.
 8. 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, obtain and maintain records of all the information from both the ordering and beneficiary sides
 - ii. file an STR/SAR in the country affected by the suspicious wire/electronic transfer, and make relevant transaction information available to the FIU/FIC.
 9. In processing wire/electronic transfers, MVTs shall take freezing action and comply with prohibitions from conducting transactions with designated person 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 resolution.

10. AIs shall ensure that the MVTs comply with the provisions of Act 1044 and this Guideline.

11. AIs acting as a settlement bank in an MVTs business arrangement shall ensure to undertake the following due diligence

- a. Obtain and verify the regulatory approval of the payment service provider (PSP) to process payment for an MVTs
- b. Monitor transactions to report any unusual and suspicious transactions to the FIC within 24 hours.
- c. Obtain and satisfy itself that the PSP has undertaken due diligence on the MVTs which includes requirements specified in paragraph 2.6.8 (1).

2.6.9 FOREIGN EXCHANGE BUREAUX

1. Foreign Exchange Bureaux are licensed and subject to BOG regulations. AIs shall obtain and verify the operating license of the Foreign Exchange Bureaux and conduct due diligence before establishing any business relationship.

2.6.10 WIRE/ELECTRONIC TRANSFERS AND PAYMENT TRANSACTIONS

2.6.10.1 CROSS-BORDER WIRE/ELECTRONIC TRANSFERS AND PAYMENT TRANSACTIONS

1. AIs shall require, obtain and hold the following information accompanying all cross-border wire/electronic transfers and payment transactions of USD 1,000 (or its cedi equivalent) or more
 - 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;
 - iii. the originator's address, and contact information (telephone number and/or email) or national identity number and/or customer identification number, or date and place of birth; and
 - iv. Purpose of transaction
 - b. Required beneficiary information:
 - i. the name of the beneficiary;
 - ii. the beneficiary account number where the transaction terminates, in an account or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and
 - iii. the beneficiary address, Ghana Card Number or national identification document for foreign nationals and/or customer identification number, or date and place of birth

2. Where several individual cross-border wire/electronic transfers and payment transactions from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and the financial institution shall be required to include the originator's account number or unique transaction reference number.
3. Whereas the cross-border wire/electronic transfers and payment transactions is below the minimum threshold (USD 1,000 or cedi equivalent), AI shall require, obtain and hold 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. whereas the cross-border wire/electronic transfers and payment transactions is below the minimum threshold (USD 1,000 or cedi equivalent), AI shall require, obtain and hold the information stated above. However, the AI shall verify the information when there is a suspicion of ML/TF/PF.
5. AI shall take measures to obtain and verify the missing originator and beneficiary information.
6. In cases where the required information in point 1 cannot be obtained, the AI shall not execute the transfer and file a suspicious transaction to the FIC within twenty-four (24) hours.
7. In processing wire/electronic transfers AIs shall take freezing action and comply with prohibitions from conducting transaction 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 successor resolutions.

2.6.10.2 DOMESTIC WIRE/ELECTRONIC TRANSFERS AND PAYMENT TRANSACTIONS

1. AI shall be required to have policies and procedures for determining:
 - i. when to execute, reject, or suspend a wire/electronic transfer and payment transactions lacking required originator or required beneficiary information; and
 - ii. the appropriate follow-up action.

2. For domestic wire/electronic transfers and payment transactions, the ordering AI shall be required to ensure that the information accompanying the wire/electronic transfer and payment transactions includes originator and beneficiary information as indicated above
3. AI shall take measures to obtain and verify the missing originator and beneficiary information.
4. Whereas in cases the information cannot be obtained, the AI shall not execute the transfer and file a suspicious transaction to the FIC within twenty-four (24) hours.
5. In cases of investigation, the ordering AI shall make available the information accompanying the domestic wire/electronic transfer and payment transactions shall be made available to the beneficiary AI and/or appropriate authorities.
6. The ordering AI needs only to make available the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to either the originator or the beneficiary. The ordering AI shall be required to make the information available by the close of the day of receiving the request from the beneficiary AI and/or from appropriate competent authorities.
7. In cases of investigation by LEAs, Ordering and/or beneficiary AI shall make available production of information relevant to the case.
8. The ordering and beneficiary AI shall be required to maintain records of originator and beneficiary information collected, in accordance with Act 1044 and FATF Recommendation 11.
9. The ordering AI shall not be allowed to execute the domestic wire/electronic transfers and payment transactions if it does not comply with the requirements specified above. (cross-border/wire/electronic transfers originator and beneficiary information)
10. In processing wire/electronic transfers AIs shall take freezing action and comply with prohibitions from conducting transaction 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 successor resolutions

2.6.10.3 INTERMEDIARY ACCOUNTABLE INSTITUTIONS

1. Intermediary AI shall be required to have policies and procedures for determining:
 - a. when to execute, reject, or suspend a wire/electronic transfer and payment transactions lacking required originator or required beneficiary information; and
 - b. the appropriate follow-up action.

2. For cross-border wire/electronic transfers and payment transactions, an intermediary AI shall be required to ensure that all originator and beneficiary information that accompanies a wire/electronic transfer and payment transactions is retained with it.
3. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border or domestic wire/electronic transfer and payment transactions, the AI shall take steps to identify the missing information and keep records of all information obtained in accordance with section 32 of Act 1044.
4. Whereas in cases where the information cannot be obtained, Intermediary AI shall refuse the transfer and file a suspicious transaction to the FIC within twenty-four (24) hours.
5. Intermediary AI shall be required to monitor and identify transactions which are consistent with straight-through processing, to identify cross-border wire/electronic transfers and payment transactions that lack required originator information or required beneficiary information.
6. In the case of point 4 above, the Intermediary AI shall suspend the transaction and require the originating institution to provide the missing required originator and/or beneficiary information.
7. Whereas in cases the information cannot be obtained, Intermediary AI shall reverse the transaction.

2.6.10.4 BENEFICIARY ACCOUNTABLE INSTITUTIONS

1. Beneficiary AIs shall be required to undertake monitoring of transactions either by close of day or real-time, to identify cross-border wire/electronic transfers and payment transactions that lack required originator information or required beneficiary information.
2. Beneficiary AIs shall take measures to obtain and verify the missing originator and beneficiary information.
3. Whereas in cases the information cannot be obtained, the Beneficiary AI shall not execute the transfer and file a suspicious transaction to the FIC within twenty-four (24) hours.
4. For cross-border wire/electronic transfers and payment transactions 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.
5. 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 and payment transactions lacking required originator or required beneficiary information; and
- b. the appropriate follow-up action.

2.6.11 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 safe custody. Where such facilities are made available to non-account holders, the EDD procedures set out in this Guideline shall apply.

2.6.12 SHELL BANKS AND SHELL COMPANIES

1. AIs are prohibited from establishing business relationships with shell banks and shell companies.

2.7 REQUIREMENTS FOR NON-PROFIT ORGANISATIONS (NPOs)

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. organisational 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. AIs shall carry out due diligence on these organisations against publicly available terrorist lists and monitor on an ongoing basis the movement of funds.

2.7.1 NON-PROFIT ORGANISATION (NPO)

1. A non-profit organisation shall be registered in Ghana or as a foreign NPO.
2. AI shall contact the appropriate overseas competent authority to confirm the existence of the foreign NPO.
3. AI in conducting due diligence shall obtain and maintain a copy of the registration document of the NPO.
4. AI shall monitor transactions to ensure that the purpose of transactions aligns with the business of the NPO.

2.7.2 REGISTERED CHARITIES

AIs shall subject charities to EDD procedures to include;

1. 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. Obtain and confirm the name and address of the charity concerned.
3. Verification of all signatories.
4. AIs shall not undertake business relationship with unregistered/unincorporated charities.

2.7.3 RELIGIOUS ORGANIZATIONS (ROs)

1. A religious organization is expected by law to be registered by the competent authority responsible for the registration and licensing of legal persons and legal arrangements and will therefore have a registered number.
2. AIs shall verify the identity of an RO by reference to the competent authority responsible for the registration and licensing of legal persons and legal arrangements.
3. AIs shall identify and verify at least two signatories and require the mandate of at least two to sign.

2.8 SUSPICIOUS ACTIVITY / TRANSACTION REPORTING (SAR/STR), TIPPING OFF AND CONFIDENTIALITY AND TRANSACTION MONITORING

2.8.1 DEVELOPMENT AND IMPLEMENTATION OF INSTITUTIONAL POLICY ON SARs/STRs

1. AIs shall have a written policy framework to monitor, detect and report suspicious activity/transactions. A list of ML/TF/PF “Red Flags” is provided in the Appendix of this Guideline as guide at minimum.
2. AMLROs shall supervise the monitoring and reporting of suspicious transactions/activities and document same.
3. AIs shall be alert to the various patterns of customer transactions and behaviour known to be suggestive of ML/TF/PF and maintain a checklist of such transactions/activities, which shall be disseminated to the relevant employees for guidance.
4. When an employee of AI detects any “red flag” or suspicious ML/TF/PF activity/transaction, the employee is required to promptly report to the AMLRO. Every action taken shall be documented.
5. The AI and its employees shall maintain confidentiality in respect of such investigation and any suspicious transaction report that may be filed with the FIC and put safeguards against tipping off.
6. AIs that suspect or has reason to suspect that funds or the proceeds of unlawful activities are related to ML/TF/PF, 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.
7. 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.
8. Noncompliance with the above shall be sanctionable.

2.8.2 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 that fall 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.
3. AIs are required to report such findings to the FIC within twenty-four (24) hours after the knowledge or the grounds of reasonable suspicion.

2.8.3 SUSPICIOUS TRANSACTION REPORTING

1. AIs shall report promptly its suspicions to the FIC if it suspect or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to ML/TF/PF.
2. AIs shall report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction.

2.8.4 TIPPING OFF AND CONFIDENTIALITY

1. Tipping off occurs when an AI, the directors, officers or its employees discloses to another party (customer or third party) that:
 - a. an STR or SAR has been filed, or
 - b. an investigation is underway or about to begin, and
 - c. that disclosure is likely to prejudice the investigation.
2. Examples of Tipping Off:
 - a. Telling a customer that their transactions are being investigated.
 - b. Informing a third party about the filing of an SAR/STR.
 - c. Changing account handling procedures in a way that alerts the customer.
3. An AI, the directors, officers and employees are:
 - (a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIC or information to other Competent Authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.
 - (b) prohibited by law from disclosing (“tipping-off”) the fact that a suspicious transaction report (STR) or related information is being filed with the FIC.
4. AIs in formulating policies on tipping off and confidentiality shall ensure that sharing of information within foreign branches and subsidiaries is not inhibited.
5. To note that any incident of tipping off is sanctionable under Act 1044.

2.8.5 TRANSACTION REPORTING

2.8.5.1 CASH TRANSACTION REPORT (CTR)

1. AIs shall submit daily reports 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 in consultation with the BOG periodically.

2.8.5.2 ELECTRONIC CURRENCY TRANSACTION REPORT (ECTR)

1. AIs shall institute policies and procedures to ensure funds transfer into or out of Ghana satisfy AML/CFT/CPF Regulations.
2. When an AI 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 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
3. AIs shall submit 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 in consultation with the BOG periodically.

2.8.6 TRANSACTION MONITORING

1. Transaction monitoring refers to an ongoing process of reviewing financial transactions to detect suspicious or unusual patterns or activities that may indicate money laundering, terrorist financing, or other financial crimes.
2. AIs shall tailor their monitoring systems based on the risk level of customers, products, services, and geographical locations; i.e. high-risk relationships require enhanced monitoring.
3. AIs shall monitor transactions as part of ongoing due diligence to ensure that transactions are consistent with the AI's knowledge of the customer, their business, and risk profile. This includes monitoring large, complex, or unusual transactions without an apparent economic or lawful purpose.
4. AIs shall document reviews and due diligence that are conducted on transactions triggered (alerts) by the monitoring system.

5. Where a suspicious transaction/activity is detected, AIs shall file an STR or SAR with the FIC.

2.8.6.1 TRANSACTION MONITORING SYSTEMS

1. AIs shall have appropriate processes in place that allow for the detection of unusual transactions, patterns and activities that are not consistent with the customer's risk profile.
2. AIs in the adoption of these transaction monitoring processes shall utilise new technologies that are in scope or sophistication (automated and complex systems which integrate the customer data information with the core banking application), depending on the size, volumes and complexity of the business operations.
3. Monitoring shall 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.
4. AIs shall develop in-house or acquire off-the-shelf automated monitoring tool to monitor all transactions, products/services, and delivery channels aimed at detecting suspicious and unusual transactions in real time or by close of day.
5. The monitoring system at minimum shall have the following features:
 - i. Ability to integrate into the core banking software.
 - ii. Covers all delivery channels, products and services that are outside the AIs core banking system.
 - iii. The rules/scenarios/parameters should be consistent with the frequency, volume and size of transactions of customers, in the context of the risk profile, product risk, geographic and delivery channels.
 - iv. Embedded with sanction screening tools
 - v. Agile to accommodate updates, such as system updates, update of monitoring rules and any others.
6. Where the AI engages a third party in the deployment of the transaction monitoring system, the following shall be undertaken.
 - i. Adhere to the BOG third-party outsourcing directive.
 - ii. Ensure the system satisfies the minimum features as stated in paragraph 4
7. AIs shall also have systems and procedures to update customer information to ensure that the transaction monitoring system can detect unusual activity, such as dormant accounts or relationships.

8. AIs shall conduct an audit on the transaction monitoring system on a yearly basis to ensure that the system is performing as expected and remains relevant in line with its business operations and ML/TF/PF typologies.
9. AIs shall develop and implement procedures to analyse transactions, patterns and activities (alerts) from the transaction monitoring system to determine if they are suspicious or not.

2.9 IDENTIFICATION OF DESIGNATED ENTITIES AND PERSONS & FREEZING AND UNFREEZING OF FUNDS

1. AIs must be able to identify and to comply with reporting, freezing and unfreezing instructions issued by the FIC or any other Competent Authority regarding individuals and entities designated as terrorist entities by the United Nations Security Council Resolutions (UNSCR), Office of Foreign Assets Control (OFAC), European Union (EU), His Majesty's Treasury, African Union (AU), Economic Community of West African States (ECOWAS), third-party lists or a competent authority.
2. 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 by the entities in paragraph 1 above 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.
3. The AI shall not enter into or continue such a 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.
4. 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 person or entity.
5. In such cases, where the AI identifies funds of a listed person or entity in Ghana, the AI shall treat such funds as frozen pursuant to Act 1044 and Act 762 as amended.
6. 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 transactions against the designated lists of persons and entities and to ensure that the lists being screened against are up to date.
7. Screening measures shall consider:
 - i. Continuous risk-based screening of customer records;
 - ii. Immediate screening of one-off or occasional transactions before the transaction is completed;

- iii. Procedures to screen payment messages; and
 - iv. Procedures to screen payment details on wire/electronic transfers and payment transactions and remittances to reasonably ensure that originator, intermediary and beneficiary details are included on the transfers.
8. 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 and reporting suspicious or positive matches to the FIC.

2.10 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, His Majesty's Treasury, Canada, the European Union, AU or 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 concerning 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 and payment transactions, 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.

2.11 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/CPF 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 shall 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.
 - v. Verification shall generally include the following:
 - a. Checking the authenticity of academic qualifications
 - b. Verifying Employment History
 - c. Police background checks
 - d. 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 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 recruitment standards of integrity among employees, including the meeting of statutory "fit and proper" criteria of the officers of the AI.
8. AI shall develop a code of ethics which shall be accessible to all employees. The code of ethics shall have disciplinary procedures and dissuasive and appropriate sanctions in the event of breaches of these rules.
9. The code of ethics shall include:
 - 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.

2.11.1 MONITORING OF EMPLOYEE CONDUCT

1. AIs shall monitor employees' accounts for potential signs of ML/TF/PF and also pay particular attention to employees whose lifestyles cannot be supported by their salary or known financial circumstances. AMLRO shall investigate observed 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/CPF procedures as applicable to other customers' accounts. This is required to be performed under the supervision of the AMLRO.
3. The AMLRO's account is to be reviewed by the Internal Auditor or any other Senior Officer designated by the Management of the AI.
4. Compliance reports shall include a lifestyle audit and findings on employees accounts, and 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.
5. The AML/CFT/CPF performance review of employees shall be part of employees' annual performance appraisal.

2.12 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/CPF tasks. Indeed, the establishment of such an employee training programme is not only considered 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 employees/areas such as reporting officers; new employees (as part of the orientation programme for those posted to the front office); banking operations/branch office employees (particularly cashiers, account opening, mandate, and marketing employees); internal control/audit employees and managers.
3. AIs are required to submit their annual AML/CFT/CPF 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 shall 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/CPF 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/CPF Reporting requirements;
 - v. Customer due diligence;
 - vi. Risk-based approach to AML/CFT/CPF regime;
 - vii. Record keeping and retention policy;
 - viii. Fraud and
 - ix. Any other relevant AML/CFT/CPF 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 ongoing training plan.
8. AIs shall submit a 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/CPF interactive programmes organised by BOG and/or FIC, and failure to attend shall attract administrative sanctions.

2.13 WHISTLEBLOWER POLICY

1. AIs shall develop a whistleblower policy. 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/CPF 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 victimisation for making them.

2.14 FRAUD MANAGEMENT

1. Bank of Ghana’s Directives titled “Inspection and Internal Audit Report for Banks” dated 15/4/87 and “Bank Frauds” dated 11/5/88, and BSD/33/2007 require all banks to submit

reports of all fraud incidents and defalcation to the BOG. The purpose is to help the BOG identify emerging fraud trends and notify the banking sector of same, making recommendations where necessary to help combat fraud and mitigate the effect on the banking sector.

2. Fraud is one of the predicate offences of money laundering and must be considered as part of the AI's AML/CFT/CPF compliance regime. AIs are to ensure that effective systems and policies are in place to detect and curb fraud activities.
3. An AMLRO, as part of its responsibilities, shall ensure that AI puts in place fraud mitigation controls.
4. At a minimum;
 - i. AIs shall develop policy and procedures on fraud management, which shall be approved by the Board. The policy and procedure shall include:
 - a. Detection
 - b. Prevention
 - c. Reporting and
 - d. Remedial actions.
 - e. The Board of Directors' oversight in fraud management, i.e. frequency of fraud report submission
 - f. Role of audit function in fraud management
 - ii. AIs shall acquire or develop a fraud detection tool. The fraud detection tool may vary in scope or sophistication depending on the size, volumes and complexity of the business operations.
 - iii. The fraud detection tool shall at a minimum be embedded with
 - a. Threshold limits
 - b. Customer profile
 - c. Features of products and services
 - iv. AIs shall ensure that employees are routinely assigned other roles.
 - v. AIs shall organise fraud awareness training for employees
 - vi. AIs shall organise a fraud awareness campaign for customers.
 - vii. AIs shall immediately report any fraud incident to BOG upon detection and file a fraud report through the Online Reporting Analytic Surveillance System (ORASS) as and when fraud occurs.
 - viii. AIs shall constitute an investigation team and generate a fraud investigation report to Management and Board.
 - ix. AIs shall submit the investigation report together with remedial action(s) to BOG promptly.

- x. AIs shall submit monthly fraud reports to the BOG through the prescribed channel.
- xi. AIs shall follow through on all fraud incidents reported to the Law Enforcement Agencies and Competent Authorities and update the BOG by submitting an updated Fraud Report through the prescribed channel.

2.15 RECORD KEEPING

1. AIs shall keep books and records (both hardcopy and electronic) with respect to customers and transactions as set out in section 32 of Act 1044

2.15.1 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 keep all records obtained through CDD measures, account files and business correspondence and results of any analysis undertaken for at least five (5yrs) years following the termination of the business relationship or after the date of the occasional transaction.
3. 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.
4. The above requirements apply regardless of whether the account or business relationship is ongoing or has been terminated.
5. 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, identification document and financial instruments (i.e. Cheques, Withdrawal/Deposit slips etc.).
6. AIs shall maintain records of the identification data, account files and business correspondence in accordance with section 32 of Act 1044.
7. AIs shall ensure that all customer-transaction records and information are made available on a timely basis.
8. AIs shall ensure that all CDD information and transaction records are available swiftly to competent authorities.

2.16 STATISTICS

1. AIs shall maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT/CPF systems. This shall include statistics on the CTRs, ECTRs, STRs reported, and those not reported with reasons. These statistics shall be easily retrievable whenever there is a request from competent authorities. Where there are discrepancies in the statistics provided to BOG or FIC, the AI would be expected to provide justification to such.

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

3.0 ESTABLISHMENT OF BUSINESS RELATIONSHIP

1. 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 claim 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/EDD information shall be the sole prerogative of the National Identification

Authority (NIA) for individuals' resident/working in Ghana and the competent authority responsible for the registration and licensing of legal persons and legal arrangements.

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;
 - c. during a one-off transaction(s);
 - d. third party;
 - e. when series of linked transactions take place.
2. AIs shall verify the identity of account holders when conducting transactions on their own account using a risk-based approach in line with the AI's AML/CFT/CPF policy.
3. Once identification procedures have been satisfactorily completed and the business relationship established, AIs shall maintain and keep records 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 claim to be.
2. AIs shall verify the identity of the person acting on behalf of another and obtain and verify the identities of the other persons involved.
3. AIs shall take appropriate steps to verify directors and/or all signatories with a controlling

interest in 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 a 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 regard 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 an 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 (prospective customer) to provide satisfactory identification evidence within a reasonable time frame of ninety (90) days may lead to a suspicion that the applicant is engaged in ML/TF/PF. The AI shall therefore make an STR/SAR to the FIC based on the available information on the applicant.
 5. AIs shall have in place written and consistent policies for 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 RISK-BASED APPROACH TO CUSTOMER IDENTIFICATION AND VERIFICATION

2. 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 authority and keep evidence of same.
3. AIs shall take a risk-based approach to the KYC/CDD requirements for all customers, verify the customer's records during the relationship and keep records of same.

3.8 RISK-BASED CUSTOMER DUE DILIGENCE

3.8.1 LOW RISK/SIMPLIFIED DUE DILIGENCE (SDD)

1. With a risk-based approach, where the identified ML/TF/PF risks are low, AIs shall apply SDD. SDD shall be proportionate 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 a 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; and
 - ii. Pensioners, social benefit recipients or customers whose income originates from their spouses'/partners' employment.
5. For customers who do not have photo identification or have limited identification documentation or those who are socially or economically vulnerable such as the persons with disability, elderly, minors, 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.

3.8.1.1 MINIMUM 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 and/or prescribed level by regulation and that systems are in place to identify linked transactions which, when aggregated, exceed the threshold.

3.8.1.2 FINANCIAL INCLUSION

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

1. AIs shall have financial inclusion policy and procedures 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 excluded from opening accounts or obtaining other financial services merely because they do not possess evidence to identify themselves. In

circumstances where they cannot reasonably do so, the internal procedures of the AIs shall make allowance for such persons by way of providing appropriate procedures in line with the AIs policy to employees on how to undertake due diligence.

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(guarantor) 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 Ghana Card of the guarantor;
 - iii. offer basic low risk account services;
 - iv. have a 90-day deferral for the customer to obtain the Ghana Card;
 - v. where the customer does not supply the required information as stipulated above, the AI shall give the customer an additional 30-day deferral before the decision to discontinue the business relationship is made. and
 - vi. where the AI suspects any unusual or ML/TF/PF risks, the AI shall file an STR to FIC and terminate the business relationship.

3.8.2 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 and as stated in the NRA or sectoral risk assessment.
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 as stated in the National Risk Assessment;

- iv. When establishing correspondent banking relationships;
 - v. Where a customer has been identified as a PEP; 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 Majesty's Treasury (UK), UNSCRs, FATF, AU and ECOWAS.

3.8.2.1 MINIMUM 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 and 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. AIs, in addition to undertaking EDD measures, shall obtain and maintain records of;
 - i. additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating
 - ii. additional information on the intended nature of the business relationship.
 - iii. information on the source of funds or the source of wealth of the customer.
 - iv. information on the reasons for intended or performed transactions.
 - v. the approval of senior management to commence or continue the business relationship.
 - vi. enhanced monitoring of the business relationship, transaction by increasing the number and timing of monitoring applied, and selecting patterns of transactions that need further examination.
 - vii. require the first payment to be carried into the customer's account to be subjected to due diligence measures.

3.8.2.2 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.

3.8.3 MINORS / STUDENTS

1. For customers who are minors i.e. below the age of eighteen (18) and are not in the tertiary education system, AI shall establish a business relationship through the trust of a parent.
2. For customers who are students and in the tertiary education system (i.e., University/ Training Schools). AI shall establish business with the customer and subject the customer to required due diligence procedures.

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

1. FATF defines a 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 thus 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 winds up 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 such as virtual assets and virtual asset service providers.
5. AIs shall undertake risk assessment prior to the launch, use of such VA/VASP or establishment of business relationship with customers in such products, practices and technologies.
6. AIs shall take appropriate measures to manage and mitigate the risks.
7. AIs shall identify and assess the ML/TF/PF risks emerging from virtual assets activities and the activities or operations of VASPs.
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 proportionate with the risk identified.
9. AIs shall take steps to identify natural or legal persons that carry out VASP activities and put in place measures to mitigate any ML/TF/PF risks associated with such activities.
10. AIs shall report SAR/STR on identified VASP activities to the FIC within 24 hours.

PUBLIC

REGULATORY REPORTING OBLIGATIONS

1. AIs shall submit the underlisted reports and returns to the Bank of Ghana and FIC as indicated in Appendix F of this guideline.
 - a. Compliance Report (Half-year and end-of-year)
 - b. Self-Risk Assessment Questionnaire
 - c. Data Capture Return
 - d. Engaged Staff (BOG Opinion)
 - e. Disengaged Staff
 - f. Fraud and Defalcation Return
 - g. Employee Education Training Programme
 - h. Independent Audit Report
 - i. Updated PEP List
 - j. CTR/ECTR
 - k. Suspicious Transaction Report
 - l. PEP Transaction Report
 - m. Any other report or return as prescribed by the competent authority.
2. AIs shall adhere to the reporting deadlines and submissions to relevant authorities.
3. Bank of Ghana shall apply administrative sanctions as required under section 93 (3) of Act 930.

SANCTIONS FOR NON-COMPLIANCE

Failure to comply with the provisions contained in this Guideline and other AML/CFT/CPF Legislations shall attract appropriate administrative sanctions as prescribed in the BOG/FIC Administrative Sanctions/Penalties for Accountable Institutions (2022), Act 1044 and Act 930.

APPENDIX A - DEFINITION OF TERMS

Terms	Definition
<i>Accountable Institution</i>	All Bank of Ghana licensed institutions
<i>Account Address</i>	All addresses for the purposes of exchange, trading, VA transfers of cryptocurrencies and/or virtual assets.
<i>Applicant for Business</i>	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.
<i>Batch transfer</i>	A batch transfer is a transfer comprising a number of individual wire/electronic transfers and payment transactions that are being sent to the same Bank of Ghana licensed institutions, but may/may not be ultimately intended for different persons.
<i>Beneficial owner</i>	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.
<i>Beneficiary AI</i>	All Bank of Ghana licensed institutions which receive the wire/electronic transfer and payment transactions or domestic transfer and payment transactions from the ordering AI or financial institution directly or through an intermediary and make funds available to the
<i>Beneficiary</i>	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.
<i>Business Relationship</i>	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.
<i>Business Entity</i>	Business entity includes: <ul style="list-style-type: none"> (a) a firm, (b) an individual licensed to carry out a business, (c) a limited liability company, or (d) a partnership, (e) company limited by guarantee, and (f) public listed companies

<i>Cross-border transfer</i>	<p>Cross-border transfer means any wire/electronic transfer and payment transactions where the originator and beneficiary institutions are located in different jurisdictions.</p> <p>This term also refers to any chain of wire/electronic transfers and payment transactions that has at least one cross-border element.</p>
<i>Designated categories of offences</i>	<p>Designated categories of offences means:</p> <ul style="list-style-type: none"> • participation in an organised criminal group and racketeering; • terrorism, including terrorist financing, proliferation financing; • trafficking in human beings and migrant smuggling; • sexual exploitation, including sexual exploitation of children; • illicit trafficking in narcotic drugs and psychotropic substances; • illicit arms trafficking; • illicit trafficking in stolen and other goods; • corruption and bribery; • fraud; • counterfeiting currency; • counterfeiting and piracy of products; • environmental crime; • murder, grievous bodily injury; • kidnapping, illegal restraint and hostage-taking; • robbery or theft; • smuggling; • tax evasion • extortion; • forgery; • piracy; and • insider trading and market manipulation; • any other similar offence or related prohibited activity punishable with imprisonment of not less than twelve (12) months; • any activities that occurred in another country which constitute an offence in that country and which would have constituted an unlawful activities had it occurred in Ghana; and • a contravention of a law in relation to a serious offence which occurs in the country or elsewhere.

Designated non-financial businesses and professions	<p>Designated non-financial businesses and professions means:</p> <ul style="list-style-type: none"> • Casinos (which also includes internet casinos). • Real estate agents. • Dealers in precious metals. • Dealers in precious stones. • Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to “internal” professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat ML/TF/PF. • 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: <ul style="list-style-type: none"> i. acting as a formation agent of legal persons; ii. acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; iii. providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; iv. acting as (or arranging for another person to act as) a trustee of an express trust; v. acting as (or arranging for another person to act as) a nominee shareholder for another person.
<i>Domestic transfer</i>	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 and payment transactions may be located in another jurisdiction.
<i>Existing Customer</i>	An account holder with an AI.
<i>The FATF Recommendations</i>	The Financial Action Task Force Recommendations refers to the internationally endorsed global standards against ML/TF/PF
<i>Financial institutions</i>	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.

<i>Funds Transfer</i>	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.
<i>High Net Worth</i>	High Net Worth means individuals who have been classified by the AIs as High Net Worth person per the internal policies and procedures.
<i>Legal arrangement(s)</i>	Legal arrangement means a trust or partnership or other entity created between parties which lacks separate legal personalities.
<i>Legal person(s)</i>	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.
<i>MVTS</i>	<p>Money or value transfer services (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other store of value and the payment of corresponding sum in cash or other form to a beneficiary by means of communication, message, transfer or through a clearing network to which the MVTs provider belongs.</p> <p>Transaction perform by such services can involve one or more intermediaries and final payment to a third party and may include any payment methods.</p> <p>Such MVTS can also be referred to as Money Service Business (MBV) or Money Transfer Operators (MTO)</p>
<i>Non-profit Organizations/ Non-governmental Organizations</i>	The term non-profit organization/non- governmental organizations refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of good works. (FATF definition)
<i>Originator</i>	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 and payment transactions.

<i>One-off Transaction</i>	A one-off transaction means any transaction carried out other than in the course of an established business relationship, that is, a single, unusual, online or customized transaction that meets a specific requirement or transaction purpose. It may be between an AI and a customer who do not usually do not do business with each other. It is important to determine whether a customer 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.
<i>Payable through account</i>	Payable through account refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.
<i>Personal Assets Holding Vehicle</i>	Legal structure/entity set up by an individual or family to hold, manage and protect personal assets such as real estate, investments, art and private businesses.
<i>Physical presence</i>	means the physical location of the AI and its' management in a country.
<i>Private/Prestige Banking</i>	Exclusive banking service offered to customers with an asset worth of at least Ghs50,000.00
<i>Proceeds</i>	Proceeds refer to any property derived from or obtained, directly or indirectly, through the commission of an offence.
<i>Property</i>	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.
<i>Religious Leader</i>	In this Guideline refers to: i. a founder of a faith/religious denomination, ii. member of the executive/council at the national, regional or area of the religious denomination/faith
<i>Risk</i>	All references to risk in this Guideline refers to the risk of money laundering and/or terrorist financing.
<i>Settlor</i>	Settlers 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
<i>Shell bank</i>	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.
<i>Simplified Due Diligence</i>	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

<i>Source of Funds</i>	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.
<i>Source of Wealth</i>	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.
<i>Suspicious Activity</i>	A suspicious activity is any activity undertaken by a prospective or existing customer for which the AI knows, suspects, or has reasonable grounds to suspect that it may be connected to unlawful activities, i.e. illicit financial activity.
<i>Suspicious Transaction</i>	A suspicious transaction is any transaction, attempted transaction, or pattern of transactions for which an AI knows, suspects, or has reasonable grounds to suspect that it may be connected to unlawful activities, regardless of the amount, origin, or destination. 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.
<i>Terrorist</i>	It refers to any natural person who: <ul style="list-style-type: none"> i. commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; ii. participates as an accomplice in terrorist acts; iii. organizes or directs others to commit terrorist acts; or iv. contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

<i>Terrorist act</i>	<p>A terrorist act includes but are not limited to:</p> <p>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.</p>
<i>Terrorist financing</i>	<p>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.</p> <p>This includes those who provide or collect funds or other assets with the intention that they shall be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts.</p>
<i>Terrorist financing offence</i>	<p>A terrorist financing (FT) offence refers not only to the primary offence or offences, but also to ancillary offences.</p>

<i>Terrorist organization</i>	<p>Refers to any group of terrorists that:</p> <ul style="list-style-type: none"> • commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; • participates as an accomplice in terrorist acts; • organizes or directs others to commit terrorist acts; or • contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act
<i>Trustee</i>	<p>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.</p> <p>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.</p>
<i>Unique identifier</i>	<p>A unique identifier refers to any unique combination of letters, numbers or symbols that refer to a specific transaction or an activity.</p>
<i>Wire/Electronic transfer and payment transactions</i>	<p>The term wire/electronic transfer and payment transactions 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.</p>

APPENDIX B - INFORMATION TO ESTABLISH IDENTITY

MINIMUM REQUIREMENTS FOR VERIFICATION AND KYC/CDD FOR NEW AND EXISTING CUSTOMERS		
FOR NEW CUSTOMERS, A 90-DAY DEFERRAL SHALL BE APPLIED TO DOCUMENT REQUESTS/ACQUISITIONS WHERE APPLICABLE DURING THIS 90-DAY PERIOD, A POST-NO-DEBIT SHALL BE PLACED ON THE ACCOUNT		
Customer Type	Customer Sub-type	Identification / Verification Requirements
Individuals	Ghanaian Citizen	<p>Ghana Card KYC Data Set</p> <p>Additional minimum requirements</p> <p>Proof of Residential Address</p> <ol style="list-style-type: none"> GPS Address, or Tenancy Agreement, or Any other relevant document issued by an authorized government agency or institution with Customer's address on it.
	Ghanaians Living Abroad	<p>Ghana Card KYC Data Set</p> <p>Additional minimum requirements</p> <p>Proof of Residential Address (local)</p> <ol style="list-style-type: none"> GPS Address, or Tenancy Agreement, or Any other relevant document with Customer's address on it <p>Proof of Residential address (foreign)</p> <ol style="list-style-type: none"> Utility Bill in customer's name, or Tenancy Agreement, or Any other relevant document issued by an authorized government agency or institution with the customer's address on it.
	Foreigners with Permanent Residence in Ghana	Non- Citizen Card KYC Data Set

		<p>Additional minimum requirements</p> <p>Proof of Residential Address (local)</p> <ol style="list-style-type: none"> GPS Address, or Tenancy Agreement, or Any other relevant document with Customer's address on it. <p>Proof of Residential address (foreign)</p> <ol style="list-style-type: none"> Utility Bill in customer's name, or Tenancy Agreement, or Any other relevant document issued by an authorized government agency or institution with Customer's address on it.
	Students (Tertiary Education System)	<p>Ghana Card KYC Data Set</p> <p>Additional minimum requirement</p> <ol style="list-style-type: none"> Introductory letter (school / parent / Guardian) Student ID Card <p>Proof of Residence</p> <ol style="list-style-type: none"> GPS Address Tenancy / Hostel Agreement Any other relevant document issued by an authorized government agency or institution with the Customer's address on it.
	Minors (Through Trust of Parent)	<p>Ghana Card KYC Data Set of Parent/Guardian</p> <p>Additional Requirements (Minor's Details)</p> <p>Full Name</p> <p>Date of Birth</p> <p>Birth Certificate</p> <p>Parent / Guardian</p> <p>Proof of Address Residential</p> <ol style="list-style-type: none"> GPS Address, or Tenancy Agreement, or

		<p>iii. Any other relevant document issued by an authorized government agency or institution with the customer's address on it.</p>
	Refugees and Asylum Seekers	<p>Non- Citizen Card KYC Data Set</p> <p>Additional minimum requirement;</p> <p>References / letter from Ministry of Interior or an appropriate government / international agency</p> <p>Proof Residential Address (local)</p> <ul style="list-style-type: none"> i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized government agency or institution with the Customer's address on it. <p>Proof of Residential address (foreign)</p> <ul style="list-style-type: none"> i. Utility Bill in customer's name, or ii. Tenancy Agreement, or <p>Any other relevant document issued by an authorized government agency or institution with the customer's address on it.</p>
	Foreign Diplomats	<p>Diplomatic Card / Diplomatic Passport</p> <p>Additional minimum requirement</p> <p>Reference/Letter from</p> <ul style="list-style-type: none"> i. Ministry of Foreign Affairs and Regional Integration and or ii. Embassy / Consulate Office <p>Proof of Residential Address (local)</p> <ul style="list-style-type: none"> i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document issued by an authorized

		<p>government agency or institution with the customer's address on it.</p> <p>Proof of Residential address (foreign)</p> <ol style="list-style-type: none"> Utility Bill in the customer's name, or Tenancy Agreement, or Any other relevant document issued by an authorized government agency or institution with the customer's address on it.
	Dependents of Foreign Diplomats	<p>Diplomatic Card / Diplomatic Passport of the Diplomat</p> <p>Additional Requirements (Dependents Details):</p> <ol style="list-style-type: none"> Full Name Date of Birth Passport Details <p>Proof of Address Residential (local) of the Diplomat</p> <ol style="list-style-type: none"> GPS Address, or Tenancy Agreement, or Any other relevant document issued by an authorized government agency or institution. <p>Proof of Residential address (foreign) of applicant</p> <ol style="list-style-type: none"> Utility Bill in the customer's name, or Tenancy Agreement, or Any other relevant document issued by an authorized government agency or institution with the customer's address on it.

Customer Type	Customer Sub-type	Identification/Verification Requirement
Sole Proprietorship / UBO	Sole Proprietorship / UBO	<p><i>Ghana Card KYC Data Set</i></p> <p><i>Additional Minimum Requirement</i></p> <ol style="list-style-type: none"> Full name of Business Full Registered Business Address Registration Number/MMDA License/Permit/Certificate Country of Registration Date of Business Registration Nature of Business <p>Proof of Residential/Business Address</p> <ol style="list-style-type: none"> GPS Address, or Tenancy Agreement, or Any other relevant document issued by an authorized government agency or institution with the customer's address on it.

Client Type	Client Sub-type	Identification/Verification Requirement
Legal Entities	Ghanaian Owned Companies and their Directors / Shareholders / Ultimate Beneficiary Owner (UBO)	<p>Ghana Card KYC Data Set for each Director/Shareholder/Ultimate Beneficiary Owner/Signatories</p> <p>Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner</p> <ol style="list-style-type: none"> Certificate of Incorporation <p>Proof of Residential Address for each Director/Shareholder/UBO</p> <ol style="list-style-type: none"> GPS Address, or Tenancy Agreement, or Any other relevant document issued by an authorized government agency or institution with the customer's address on it
	Foreign Owned Companies and their Foreign Directors and	Non- Citizen Card KYC Data Set

	Shareholders/UBO	<p>Additional minimum requirement for each Director / Shareholder / Ultimate Beneficiary Owner/ Signatories</p> <ol style="list-style-type: none"> Certificate of Incorporation GIPC certification Relevant Industry license <p>Proof of Corporate/Residential Address (local) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner</p> <ol style="list-style-type: none"> GPS Address, or Tenancy Agreement, or Any other relevant document with the customer's address on it. <p>Proof of Residential address (foreign) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner</p> <ol style="list-style-type: none"> Utility Bill in the customer's name, or Tenancy Agreement, or Any other relevant document
--	------------------	--

Client Type	Client Sub-type	Identification/Verification Requirement
Public Registered Companies (Directors / Shareholders / UBO)	Local Directors / Shareholders with Controlling interest	<p>Ghana Card KYC Data Set for each Director/Shareholder/Ultimate Beneficiary Owner/ Signatories</p> <p>Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner/ Signatories</p> <ol style="list-style-type: none"> Certificate of Incorporation <p>Proof of Residential Address for each Director/Shareholder/UBO/ Signatories</p>

		<ul style="list-style-type: none"> i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document with the customer's address on it
	Foreign Directors/Shareholders with Controlling interest	<p>Non- Citizen Card KYC Data Set</p> <p>Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner/ Signatories</p> <ul style="list-style-type: none"> i. Certificate of Incorporation <p>Proof of Corporate/Residential Address (local) for each Foreign Director / Shareholders / Ultimate Beneficiary Owner/ Signatories</p> <ul style="list-style-type: none"> i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document with the customer's address on it. <p>Proof of Residential address (foreign) for each Foreign Director / Shareholder / Ultimate Beneficiary Owner/ Signatories</p> <ul style="list-style-type: none"> i. Utility Bill in the customer's name, or ii. Tenancy Agreement, or iii. Any other relevant document with the customer's address on it
	Local UBO	<p>Ghana Card KYC Data Set for each Director/Shareholder/Ultimate Beneficiary Owner/ Signatories</p> <p>Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner/ Signatories</p> <ul style="list-style-type: none"> i. Certificate of Incorporation <p>Proof of Residential Address for each</p>

		Director/Shareholder/UBO/ Signatories <ul style="list-style-type: none"> i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document with the customer's address on it
	Foreign UBO	Non- Citizen Card KYC Data Set Additional minimum requirement for each Director/Shareholder/Ultimate Beneficiary Owner/ Signatories <ul style="list-style-type: none"> i. Certificate of Incorporation Proof of Corporate/Residential Address (local) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner/ Signatories <ul style="list-style-type: none"> i. GPS Address, or ii. Tenancy Agreement, or iii. Any other relevant document with the customer's address on it. Proof of Residential address (foreign) for each Foreign Director/Shareholder/Ultimate Beneficiary Owner/ Signatories <ul style="list-style-type: none"> i. Utility Bill in the customer's name, or ii. Tenancy Agreement, or iii. Any other relevant document with the customer's address on it

Client Type	Client Sub-type	Identification/Verification Requirement
-------------	-----------------	---

Government	State Owned Enterprise (SOE)	Minimum Requirements i. Ghana Card KYC Data Set for all Directors and Account Signatories ii. Board Resolution iii. Details of Address of Government
	Ministries, Departments and Agencies	
	Regulatory Bodies /Agencies	
	Public Institutions (E.g. Universities, Hospitals)	
	Foreign Government – Embassies/Consulate	Minimum Requirements i. Diplomatic Card/Passport of account signatories ii. Reference/Introductory Letter iii. Details of Address
	Foreign Government – Development Organisation	
	International Development Organisations – (E.g. UN, WHO, Africa Development Bank etc.)	

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

Customer Type	Customer Sub-type	Identification/Verification Requirement
Non-Profit Organisation (NPO) / Clubs and Societies	Non-Profit Organisation (NGO)	Minimum Requirements i. Board Resolution ii. Certificate of Incorporation (from Municipal Assembly, institution responsible for registration of companies, where applicable)
	Religious Organisation/Bodies	
	Charities /Foundations	

		<ul style="list-style-type: none"> iii. Copy of license/registration from a Regulatory Authority, where applicable iv. Ghana Card/Non-Citizen Card KYC Data Set for Directors/ Account Signatories (At least two (2)) v. Details of Business Address vi. Nature of Business
	Clubs	Minimum Requirements
	Societies/ Associations	<ul style="list-style-type: none"> i. Board Resolution ii. Constitution iii. Ghana Card KYC Data Set for Account Signatories iv. Details of Business Address v. Nature of Business

Customer Type	Customer Sub-type	Identification/Verification Requirement
Trust	Trust	Minimum requirement <ul style="list-style-type: none"> i. Certified copy of Trust Deed and supplemental Trustee, or Equivalent constitutive document detailing purpose and structure of the Trust. ii. Details of settlors, trustee and beneficiaries and authorised signatories in the Trust. iii. Where signatories are not identified in the Trust Deed, a certified copy of the authorised signatories' list shall be provided. iv. Ghana Card KYC Data Set for; <ul style="list-style-type: none"> a. Settlors (Donor / Grantors) b. Trustees c. Beneficiaries 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 institutions issued by the Bank of Ghana 2025 and available on the Bank of Ghana Website.

PUBLIC

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/CPF 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/CPF 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/CPF 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, shall 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) shall 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 and payment transactions as categories which are considered as high-risk, or which require specific due diligence measures. In addition, AIs shall 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/CPF 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)

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/CPF 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/CPF 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/CPF compliance programme to adequately address its risk profile, as identified by the risk assessment. Management shall understand the AI's AML/CFT/CPF risk exposure and develop the appropriate policies, procedures, and processes to monitor and control AML/CFT/CPF 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/CPF 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/CPF profile, management shall provide a more robust AML/CFT/CPF compliance programme that specifically monitors and controls the high-risk s that management and the board have accepted.

CONSOLIDATED AML/CFT/CPF COMPLIANCE RISK ASSESSMENT

AI that implement a consolidated or partially consolidated AML/CFT/CPF compliance programme shall assess risk both individually within business lines and across all activities and legal entities. Aggregating AML/CFT/CPF 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/CPF risk exposures, the bank shall continually reassess its AML/CFT/CPF risks, review its risk rating of customers and communicate with business units, functions, and legal entities. The identification of an AML/CFT/CPF 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/CPF compliance programme controls risks associated with the AI's products, services, customers, entities, and geographic locations; therefore, an effective risk assessment shall be an ongoing process, not a one-time exercise. Management shall update its risk assessment to identify changes in 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/CPF risks within a two-year cycle.

PUBLIC

APPENDIX E - MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING “RED FLAGS”

INTRODUCTION

Monitoring and reporting of suspicious transactions is key to AML/CFT/CPF 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”

1. 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 with correspondents that have been identified as high-risk.
- c. Large transaction activity involving monetary instruments such as traveler’s cheques, bank drafts, money order, particularly those that are serially numbered.
- d. 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.
- e. Employees' lavish lifestyle that is inconsistent with reported income.

2. 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.

3. 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 foreign exchange 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.
- x. 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.

4. 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.

5. 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).

6. 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 organisation, for which there appears to be no logical economic purpose or for which there appears to be no link between the stated activity of the organisation and other parties in the transaction.
- c. 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.
- d. The stated occupation of the customer is inconsistent with the type and level of account activity.
- e. Funds transfer does not include information on the originator, or the person on whose behalf the transaction is conducted, the inclusion of which shall ordinarily be expected.
- f. Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and channel funds to a small number of foreign

beneficiaries.

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

7. 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.

8. Proliferation Financing Red Flags

- a. Large number of individuals making payments into the same account without an adequate explanation
- b. An account operated in the name of an off-shore company with structured movement of funds.
- c. Large transaction activity involving monetary instruments such as traveler's cheques, bank drafts, money order, particularly those that are serially numbered.
- d. The customer is a research body/NPO/Charity connected with a high-risk

jurisdiction of proliferation concern.

- e. When customer is involved in the supply, sale, delivery or purchase of dual-use, proliferation sensitive or military goods, particularly to high-risk jurisdictions.
- f. When customer or counterparty, or its address, is the same or similar to that of an individual or entity found on publicly available sanctions lists.
- g. When customer's activities do not match with the business profile provided to the reporting entity.
- h. When a customer is unable to provide information on the BOs or the transactions relating to the BOs.
- i. When customer uses complicated structures to conceal connection of goods imported / exported, for example, uses layered letters of credit, front companies, intermediaries and brokers.
- j. When a freight forwarding/customs clearing firm being listed as the product's final destination in the trade documents.
- k. Project financing and complex loans, where there is a presence of other objective factors such as an unidentified end-user.
- l. The transaction(s) involve the shipment of goods inconsistent with normal geographical trade patterns i.e. where the country involved does not normally export or import or usually consumed the types of goods concerned.
- m. Over/under invoice of dual-use, proliferation-sensitive or military goods, trade transactions.
- n. The transaction(s) related to dual-use, proliferation-sensitive or military goods, whether licensed or not.

APPENDIX F - STATUTORY RETURNS

TYPE OF REPORT	RECIPIENT BODY	CHANNEL	FREQUENCY
Compliance Report This shall include but not limited to the following keys areas <ol style="list-style-type: none"> Employees AML/CFT/CPF Training Additional AML/CFT/CPF Risk Assessment Additional Procedures and Mitigants New Technologies/Products, Non-face-to-face Transactions Reliance on Intermediaries or Third-Party Service Providers Update on appointment / re-designation / dismissal / resignation / retirement Monitoring of Employee Conduct Fraud activities Review of Risk Assessment Conducted Review of AML/CFT/CPF policy/framework Record Keeping Procedures Update on AML/CFT/CPF Software/Application Statistics of STRs, CTRs and ECTRs submitted to the FIC during the review period Other relevant compliance activities 	BOG & FIC	To BOG through ORASS To FIC via info@fic.gov.gh and compliancemails@fic.gov.gh	HALF YEARLY (not later than the 15 th day of the month after the half year); and END OF YEAR (not later than the 15 th day of the month after the end of year)

Employee Education & Training Programme	BOG & FIC	To BOG through ORASS To FIC via info@fic.gov.gh and compliancemails@fic.gov.gh	YEARLY (not later than 31st December of every financial year)
Independent Audit Report on AML/CFT/CPF Compliance Function The report may include but not limited to the following areas: <ol style="list-style-type: none"> 1. Review of AML/CFT/CPF programme for the year 2. Board/employees training 3. Review of AML/CFT/CPF policy & Risk Assessment Framework 4. Filing of CTRs/STRs/ECTRs 5. Transaction Monitoring Systems 6. KYC/CDD/EDD on customers 7. Review of AMLROs account 8. Due diligence on new employees 9. Any other AML/CFT/CPF related activity 	BOG & FIC	To BOG through ORASS To FIC via info@fic.gov.gh and compliancemails@fic.gov.gh	YEARLY (not later than the 15 th day of the month after the end of the year)
Annual AML/CFT Self Risk Assessment Questionnaire	BOG	ORASS	YEARLY (not later than the 15 th day of the month after the end of the year)
Quarterly Returns (Data Capture)	BOG	ORASS	QUARTERLY (not later than the 15 th day of the month after the end of the quarter)
Updated PEP List	FIC	info@fic.gov.gh and compliancemails@fic.gov.gh	QUARTERLY (not later than the 15 th day of the month after the end of the quarter)
PEP Transactions	FIC	GoAML	As and When
Fraud and Defalcation Report	BOG	ORASS	As and When
Disengaged Staff Return	BOG	ORASS	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. Banks and Specialised Deposit Taking Act, 2016 (Act 930)
5. Foreign Exchange Act 2007 (Act 723) and Regulations
6. Whistle Blower Act, 2006 (Act 720)
7. Criminal and Other Offences Act, 1960 (Act 29)
8. Payment System and Services Act, 2019(Act 987)
9. Corporate Governance Directive 2018 for Banks, Savings and Loans Companies, Finance Houses and Financial Holding Companies
10. Central Bank of Trinidad and Tobago Anti-Money Laundering Guideline, 2018
11. Red Flag Indicators for Proliferation Financing, 2020 - Financial Monitoring Unit, Government of Pakistan
12. The Financial Action Task Force (FATF) Recommendations
13. Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems