THE

LIBERIA  **OFFICIAL**

GAZETTE

PUBLISHED BY AUTHORITY

VOL. XXVI TUESDAY, AUGUST 11, 2026 NO. 39

E X T R A O R D I N A R Y

THE GOVERNMENT OF THE REPUBLIC OF LIBERIA ANNOUNCES THAT THE CENTRAL BANK OF LIBERIA (CBL) AND FINANCIAL INTELLIGENCE AGENCY (FIA), PURSUANT TO THEIR RESPECTIVES STATUTORY POWERS AND FUNCTIONS UNDER THE ANTI-MONEY LAUNDERING, TERRORIST FINANCING, PREVENTIVE MEASURES, AND PROCEEDS OF CRIME ACT, 2021, THE FINANCIAL INTELLIGENCE AGENCY ACT, 2021, THE AMENDMENT AND RESTATEMENT OF THE ACT ESTABLISHING THE CENTRAL BANK OF LIBERIA, AND OTHER APPLICABLE LAWS, HAVE JOINTLY FORMULATED AND HEREBY ISSUED ON AUGUST 11, 2026, THE BELOW REGULATIONS:

REGULATION NO. CBL/FIA/AML/CFT/001/2026 TITLE:
ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING, COUNTER-PROLIFERATION FINANCING, PREVENTIVE MEASURES, AND PROCEEDS OF CRIME REGULATIONS, 2026

BY ORDER OF THE PRESIDENT

MME. SARA BEYSOLOW NYANTI
MINISTER OF FOREIGN AFFAIRS

MINISTRY OF FOREIGN AFFAIRS
MONROVIA, LIBERIA
AUGUST 11, 2026

Contents

1.0 Introduction 4
Definitions 6
2.0 ROLES AND RESPONSIBILITIES OF THE BOARD OF DIRECTORS 8
3.0 ROLE OF SENIOR MANAGEMENT 10
4.0 AML/CFT Preventive Measures for Financial Institutions 11
4.3 High Risk Customers and Accounts 15
4.5 Politically Exposed Persons (PEP) 16
5.0 Policies and Procedures 17
7.0 Employee Due Diligence (Know Your Employee) 20
8.0 MONITORING OF EMPLOYEE BEHAVIOUR 22
9.0 NON-PROFIT ORGANIZATION (NPO) 23
10.0 TERRORIST FINANCING 24
11.0 AUDIT 25
12.0 COMPLIANCE WITH OBLIGATIONS BY FOREIGN SUBSIDIARIES AND BRANCHES: 25
13.0 HIGHER RISK COUNTRIES 26
14.0 OBLIGATIONS OF TRUSTEES 27
15.0 Record Keeping Obligations 27
16.0 Prohibition against relations with shell banks 28
17.0 Prohibition against Anonymous and Numbered accounts 28
18.0 Suspicious Transactions Monitoring and Reporting 28
19.0 NEW BUSINESS WITH EXISTING CUSTOMERS 28
20.0 RISK-BASED CUSTOMER DUE DILIGENCE and Enhanced Customer Due Diligence 29
21. New Products, Technologies and non-face-to- face business relationships 29
22. AML/CFT Customer Due Diligence/Know Your Customer (CDD/KYC) Obligations 30
23. FINANCIAL INCLUSION MEASURES 35
23.0 Simplified Customer Due Diligence 36
24.0 Inability to fulfill Customer Identification Obligations 37
25.0 Enhanced Due Diligence 37
26. TRANSACTION MONITORING AND REPORTING SYSTEMS 38
27.0 WHISTLE-BLOWING 40
28.0 Ongoing Due Diligence: 40
29. Prohibition of Personal accounts for business purposes 41

30. Tipping off and confidentiality 41
31.0 Trade Finance Customer 42
32.0 Deferral and Timing of Verification: 42
33. Application of CDD to Existing Customers 44
34. Reliance on Third Parties: 45
35. Money or Value Transfer Services (MVTS) 46
36.0 FOREIGN EXCHANGE BUREAUS 47
37.0 Wire transfers 47
38. IDENTIFICATION AND ACCOUNT-OPENING FOR CROSS-BORDER CORRESPONDENT RELATIONSHIPS 50
39.0 TARGETED FINANCIAL SANCTIONS AGAINST TERRORISM AND PROLIFERATION FINANCING 51
40. VIRTUAL ASSETS (VAs) AND VIRTUAL ASSETS SERVICE PROVIDERS (VASPs) 56
41.0 Compliance Inspections 57
42. Enforcement Actions for Violation of any of the Provisions of this Regulation 57
43. Judicial Review 59
44. Effective Date 59
45.0 Annex: 59
Annex 45.2 A Non-Exhaustive List of Domestic PEP 64
Annex 45.3 A Non-Exhaustive List of Foreign PEP 65

1.0 Introduction

This regulation implements Preventive Measures requirements which are mandatory for financial institutions (as defined by §15.3 of the Anti- Money Laundering and Terrorist Financing Act of 2021):

Whereas, §15.1.5 of the AML/CFT Act of 2021, which designates the National AML/CFT Inter-Ministerial Committee (IMC) as the central coordinating body for the formulation of national AML/CFT policies and strategies necessary to achieve the objectives of the anti-money laundering, countering the financing of terrorism and combating the financing of the proliferation of weapons of mass destruction.

Whereas, Part II, § 6(h) of the Amendment and Restatement of the Act Establishing the Central Bank of Liberia of 1999, which mandates the Central Bank to have power and authority to license, regulate, monitor, supervise and resolve all bank-financial institutions operating within Liberia. Furthermore, §106.0(2) and (3) of The Bank-Financial Institutions and Bank-Financial Holding Companies Act of 2025 authorizes the Central Bank of Liberia to issue regulations, guidelines and policies as necessary, to safeguard bank-financial institutions against money laundering and terrorist financing risks, and to collaborate with relevant stakeholders in protecting the integrity of the financial system. Accordingly, this Regulation constitutes an amendment of the CBL AML/CFT Regulation No. CBL/RSD/002/2017, aligning it with the requirements of the Anti-Money Laundering/Countering Financing of Terrorism Act of 2021, and;

Whereas, §67. 3 (1) of the Financial Intelligence Agency (FIA) Act, which empowers the FIA to regulate, supervise, monitor and enforce compliance with AML/CFT obligations as set out in the AML Act of 2021 and Targeted Financial Sanctions Against Terrorist Act of Reporting Entities.

This Regulation repeals and replaces the previous CBL AML/CFT Regulation No. CBL/RSD/002/2017.

1.1 Financial institutions are required to adopt and fully implement effective internal AML/CFT/CPF control policies and procedures applicable to all customers, products, services, business lines, branches and subsidiaries. In addition to the above, financial institutions shall:

a) adopt policies stating its commitment to comply with Anti-Money Laundering (AML'), Combating Financing of Terrorism (CFT') and Countering Proliferation Financing (CPF') obligations under subsisting laws, regulations and regulatory directives and to actively prevent any transaction that otherwise facilitates criminal activities, money

laundering, terrorism financing and financing the proliferation of weapons of mass destruction (ML/TF/PF).

b) Create and implement internal controls and other procedures to deter criminals from using its facilities for ML/TF/PF.

c) adopt a risk–based approach in the identification, assessment and management of their ML/TF/PF risks in line with the requirements of these Regulations.

d) comply without delay with requests made pursuant to current AML/CFT/CPF legislations and provide information to the Central Bank of Liberia ("CBL"), Financial Intelligence Agency ("FIA") and other competent authorities.

e) not in any way prevent the implementation of the provisions of these Regulations and shall co-operate with the regulators and law enforcement agencies in the implementation of a robust AML/CFT/CPF regime in Liberia.

f) render statutory reports to appropriate authorities as required by law and shall guard against any act that will cause a customer or client to avoid compliance with AML/CFT/CPF Legislations.

g) identify, review and record other areas of potential ML/TF/PF risks not covered by these Regulations and report same to the Supervisory Authorities.

h) reflect AML/CFT/CPF Act and Regulations, etc. in their strategic policies.

i) conduct on-going Due Diligence and where appropriate, enhanced Due Diligence on all business relationships and shall obtain information on the purpose and intended nature of the business relationship of their potential customers.

j) ensure that their employees, agents and others doing business with them, clearly understand the AML/CFT/CPF program.

Definitions

In these regulations the following definitions apply:

1.2.1 **Beneficial Owner** is the natural person(s) who ultimately owns or controls a customer/client or the rights to and/or benefits from assets, including an account or property, as well as the person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

1.2.2 **Beneficiary Institution** means the financial institution that receives the funds on behalf of the wire transfer or fund transfer beneficiary.

1.2.3 **Compliance Officer** – means the head of the compliance department/section. The compliance Officer shall be at a managerial level.

1.2.4 **Deferral** means a **temporary delay** in completing the full verification of a customer's identity or beneficial ownership information **after** the commencement of a business relationship or the execution of a transaction, under conditions permitted by law and approved by the CBL.

1.2.5 **Designated Person or Entity** means any natural person, legal person, group, undertaking or entity designated under: UNSCR 1267; UNSCR 1988; UNSCR 1373; UNSCR 1718; UNSCR 2231; successor resolutions; any designation made under Liberian law.

1.2.6 **Express trust** means trust created by the settler, either orally or in a written agreement or deed of trust, by which property is passed from the owner to another person.

1.2.7 Financial institution means any person doing financial transactions consisting in the business of banking, credit, loan making, lending or rendering non-banking financial services; provided that, for the purpose of the BFIA Act of 2025, and unless the context otherwise requires, all officers and branches of a financial institution in Liberia shall be deemed to be one financial institution.

1.2.8 **Freeze** means prohibiting the transfer, conversion, disposition, movement or use of funds or other assets in any manner whatsoever.

1.2.9 **Funds or Other Assets**

means every kind of asset, whether tangible or intangible, movable or immovable, including digital assets, virtual assets, economic resources and any legal documents evidencing ownership.

1.2.10 **Online Transaction** means deposit or withdrawal of cash, fund transfers, payments against goods and services, etc. using different branches of financial institutions through electronic means.

1.2.11 **Ordering Institution** refers to the financial institution that initiates a wire transfer on the instructions of the wire transfer originator for transferring the funds.

1.2.12 **Originator** means the person who allows or places the order to initiate a fund transfer, wire transfer or an online transaction.

1.2.13 **Payable-through accounts** mean correspondent accounts that are used directly by third parties to transact business on their own behalf.

1.2.14 **Politically Exposed Person (PEP):** as defined in the AML/CFT Act of 2021 and to include:

i. **Foreign PEPs:** individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

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

iii. **International PEPs** are those who are or have been entrusted with a prominent public function by an international organization, for example senior management, i.e., directors, deputy directors and members of the board or equivalent functions.

iv. **Family members and close associates** of persons referred to in (i) and (ii).

a) **Family Members**: These are individuals who are related by blood, marriage, or a similar form of partnership. Common examples include:

- **Spouse or partner** (including common-law partners)
- **Children** (including adopted or stepchildren)
- **Parents** (including in-laws)
- **Siblings** (including in-laws)
- **Grandparents, uncles, aunts, nieces, and nephews** may also be considered family depending on the jurisdiction and context.

b) **Close Associates**: These are individuals who are closely connected to a PEP, either socially and/or professionally. Close associates might include:

- **Business partners** or **associates** (individuals involved in joint ventures, partnerships, or financial transactions with the PEP)
- **Key advisers**, such as legal or financial advisers, who may have significant influence over the PEP's decisions
- **Close friends** with whom the PEP has a longstanding relationship or who share financial interests
- **Individuals with significant professional or business relationships** with the PEP

1.2.15 **SENIOR MANAGEMENT means** any person who is an officer of a financial institution including the chief executive officer, managing director, deputy managing director, chief operating officer, company secretary, vice president(s), chief financial officer, chief compliance officer, General Manager and any other person who, alone or together with one or more others, has the authority to commit the bank.

1.2.16 **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 group that is subject to effective consolidated supervision. For purposes of this definition 'physical presence' means a meaningful mind and management located within a country. The simply existence of a local agent or low-level staff does not constitute a physical presence.

1.2.17**Supervisor or Supervisory Authority** means a competent authority responsible for licensing and/or supervising financial institutions, i.e., Central Bank of Liberia (CBL) and the Financial Intelligence Agency (FIA) of Liberia

1.2.18 **Without Delay**

means immediately upon designation and without prior notice to the customer, allowing only the time reasonably necessary to identify the designated funds or assets and execute the freeze.

2.0 ROLES AND RESPONSIBILITIES OF THE BOARD OF DIRECTORS

2.1 The Board shall exercise ultimate oversight responsibility to ensuring the effectiveness of the AML/CFT/CPF compliance program of the Financial Institutions. In this respect, the Board's oversight regarding AML/CFT/CPF shall

align with the best international practices, as well as the CBL's Corporate Governance Regulation as well as the corporate governance standards stipulated in the Bank-Financial Institutions and Bank-Financial Holding Companies ACT of 2025. The Board must ensure that there is documented evidence of its oversight functions, for example, in meeting minutes of the Board or its committees.

a) Key responsibilities of the Board include:

i. Establishing the institution's overall risk appetite and strategy, and ensure that mechanisms, based on Financial Institution risk context, are in place to effectively mitigate risk. These processes shall be documented and retained, consistent with §15.3.16 of the AML/CFT Act of 2021;

ii. Ensuring that appropriate policies, procedures and controls are approved for the management of all ML/TF/PF risks, and that arrangements are in place for the effective reporting of all issues related to the functioning of the risk management framework;

iii. Setting up an independent compliance function and appoint a Compliance Officer at a Senior Managerial Level, who shall be responsible for coordinating, monitoring and facilitating compliance with existing laws and regulations, and improve the bank's compliance policy and procedures;

iv. Reviewing, assessing and testing the effectiveness of the AML/CFT controls and ensure that the risk management policies and strategies are effectively managed.

v. Approving the AML/CFT/CPF compliance program, training program, compliance reports, Internal Risk Assessment Framework, Compliance Charter and reports;

vi. Ensuring that the appropriate measures are adopted for the periodic review and update of AML/CFT/CPF policies, procedures and controls to ensure their continued relevance in line with changes in the Financial Institution risk profiles, amendment of AML/CFT laws and regulations, and to address new and emerging ML/TF/PF risks;

vii. Ensuring the creation of an appropriate ML/TF/PF 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;

viii. Ensuring that all Board members receive the requisite training on AML/CFT/CPF as well as the institution's specific ML/FT/PF risks and controls at least annually. All such trainings shall be documented and retained, consistent with §15.3.16 of the Anti-Money Laundering and Countering Financing of Terrorism Act of 2021;

ix. Ensuring the receipt of regular and comprehensive reports on the Financial Institution's AML/CFT/CPF function from the Compliance Officer 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 Central Bank of Liberia (CBL) and the Financial Intelligence Agency (FIA), on its assessment of the institution's AML/CFT/CPF obligations;

b) The results of compliance testing as well as all self-identified instances of noncompliance with AML/CFT/CPF requirements;

c) Recent changes in AML/CFT/CPF laws and regulations and what implications said changes may have on the Financial Institution;

d) Details of recent significant risk issues and the potential impact on the Financial Institutions; and

e) Statistics of statutory report to the FIA, requests/orders from law enforcement agencies.

3.0 ROLE OF SENIOR MANAGEMENT

3.1 Senior Management of Financial Institution(s) is responsible for the day-to-day implementation, monitoring and management of the FI's AML/CFT/CPF compliance program, including ensuring adherence to established AML/CFT/CPF policies and procedures. Among other things, Senior Management shall ensure that policies and procedures:

a. are risk based, proportional and adequate to mitigate ML/TF/PF risks of the Financial Institution(s);
b. comply with all relevant AML/CFT/CPF laws, regulations and guidelines; and
c. are implemented effectively across relevant business areas or throughout the financial group as applicable.
d. exists for succession planning for the Compliance Officer function.

3.2.1 Senior Management shall review policies and procedures periodically for consistency with the Financial Institution's business model, product and service offerings, risk appetite and all existing AML/CFT&CPF Laws and Regulations.

3.2.2 Attention should be paid to new and developing technologies and Financial Institution(s) shall identify and assess the ML/TF/PF risks arising from new products/services and delivery channels; new business practices, new delivery mechanisms and new or developing technologies for new and pre-existing products; and put measures in place to manage and mitigate such risks. Risk assessments should take place prior to the launch or use of such products/services, channel, business practices and technologies.

3.3 Senior Management shall also ensure that:

i. Comprehensive Business-wide risk assessment is conducted of the Financial Institution, including those for pre-existing customer, products, services, geographic location and delivery channel mechanisms.
ii. All significant recommendations made by internal and external auditors and regulators in respect of the AML/CFT/CPF program are addressed in a timely manner, and or as prescribed by the regulatory/supervisory body;
iii. Relevant, adequate and timely information regarding AML/CFT/CPF matters is provided to the Board;
iv. The Compliance Officer receives appropriate training on an ongoing basis to effectively perform his duties;
v. There is an ongoing employee training program (at least twice a year) which enables employees to have adequate and relevant knowledge to understand and discharge their AML/CFT/CPF responsibilities; and
vi. The Compliance and Internal Audit functions are adequately resourced in terms of personnel, IT systems and budget to effectively implement, administer, monitor and periodically audit the AML/CFT/CPF program, providing independent assurance on the effectiveness of the Financial Institution's AML/CFT/CPF control framework.

4.0 AML/CFT Preventive Measures for Financial Institutions

4.1 Risk Assessment

4.1.1 Financial Institutions shall adopt a risk-based approach for the effective management and mitigation of their money laundering, terrorist financing and proliferation financing risks. The procedures to mitigate the ML/TF/PF

risks shall be fully implemented and integrated into the internal AML/CFT/CPF control policies and procedures shall be updated to include them.

4.1.2 Financial Institution shall establish, document, maintain, and periodically update an enterprise-wide risk assessment of its money laundering, terrorist financing, and proliferation financing risks. Such risk assessment shall remain current and appropriate to the Institution Risk profile.

4.1.3 The enterprise-wide risk assessment shall identify, assess, understand, document, and evaluate the ML/TF/PF risks arising from the institution: a) customers; b) beneficial owners; c) products and services; d) delivery channels; e) transactions; f) geographic exposure; g) business lines; h) correspondent banking relationships; i) Money or Value Transfer Services; j) virtual asset activities, where applicable; k) trade finance activities; l) new products, technologies, and delivery mechanisms; m) outsourcing and third-party reliance arrangements; n) distribution networks; and o) any other activity presenting ML/TF/PF risks.

4.1.4 In conducting its enterprise-wide risk assessment, the Financial Institution shall consider, where applicable: a) the National Risk Assessment; b) sectoral risk assessments; c) guidance issued by the Central Bank of Liberia; d) guidance issued by the Financial Intelligence Agency; e) Financial Action Task Force Recommendations and guidance; f) applicable United Nations Security Council Resolutions; g) typologies, trends, and emerging financial crime risks; h) internal audit findings; i) compliance monitoring results; j) regulatory inspection findings; k) suspicious transaction reporting trends; l) sanctions risks; m) cyber-enabled financial crime risks; and n) any other relevant internal or external information.

4.1.5 The enterprise-wide risk assessment shall: a) be documented in writing; b) be approved by the Board of Directors; c) be reviewed by Senior Management; d) be updated at least annually, or more frequently where significant changes occur; and e) be made available to the Central Bank of Liberia, the Financial Intelligence Agency, and any other competent authority upon lawful request.

4.1.6 Financial Institution shall ensure that the results of the enterprise-wide risk assessment are reflected in: a) customer acceptance policies; b) customer risk classification methodologies; c) Customer Due Diligence measures; d) Simplified Due Diligence measures; e) Enhanced Due Diligence measures; f) ongoing due diligence; g) transaction monitoring systems; h) targeted financial sanctions controls; i) wire transfer controls; j) reliance on third

parties; k) employee training programs; l) internal audit plans; m) allocation of compliance resources; and n) any other AML/CFT/CPF control necessary to mitigate identified risks.

4.1.7 Financial Institutions shall adopt a Risk-based approach and a documented methodology for assessing ML/TF/PF risks that: a) identifies inherent risks; b) evaluates the effectiveness of existing controls; c) determines residual risks; d) assigns appropriate risk ratings; e) documents assumptions and conclusions; and f) supports risk-based decision-making throughout the institution.

4.1.8 Where the enterprise-wide risk assessment identifies material deficiencies, emerging risks, or elevated ML/TF/PF risks, the Financial Institution shall promptly implement appropriate corrective measures, including enhanced internal controls, revised policies and procedures, enhanced due diligence, increased transaction monitoring, additional employee training, or any other risk mitigation measures necessary to address the identified risks.

4.1.9 Financial Institutions shall maintain records relating to the enterprise-wide risk assessment, including supporting methodologies, data sources, assumptions, approvals, periodic reviews, updates, and corrective actions, in accordance with the recordkeeping requirements prescribed under this Regulations.

4.2 Risk Classification

4.2.1 Financial Institution shall establish, implement, and maintain a documented customer risk classification methodology that enables the identification, assessment, classification, monitoring, and periodic review of the money laundering, terrorist financing, and proliferation financing risks associated with each customer and business relationship.

4.2.2 The customer risk classification methodology shall be risk-based, proportionate to the nature and complexity of the Financial Institution's business, and consistent with the enterprise-wide ML/TF/PF risk assessment

4.2.3 Customer risk assessments shall be completed: a) before establishing a business relationship; b) before opening an account; c) before conducting an occasional transaction where Customer Due Diligence is required; d) before establishing a correspondent banking relationship; e) before establishing a business relationship with a Virtual Asset Service Provider, where applicable; and f) whenever otherwise required under these Regulations.

4.2.4 Financial Institutions shall assess customer risk by considering, at a minimum: a) customer type; b) legal form and ownership structure; c) beneficial ownership; d) occupation, profession, or business activity; e) products and services used; f) delivery channels; g) anticipated account activity; h) transaction size, frequency, and complexity; i) source of funds; j) source of wealth, where applicable; k) geographic exposure; l) connections with higher-risk jurisdictions; m) Politically Exposed Person (PEP) status; n) adverse media or other reliable negative information; o) sanctions exposure; p) virtual asset activities, where applicable; q) trade finance activities, where applicable; and r) any other factor identified through the institution's enterprise-wide risk assessment.

4.2.5 Financial Institutions shall classify customers into appropriate risk categories, which shall include, at a minimum: a) Low Risk; b) Medium Risk; and c) High Risk.

4.2.6 The customer risk classification methodology shall clearly establish: a) the risk factors considered; b) the weighting or scoring methodology; c) approval authorities; d) escalation procedures; e) review frequencies; f) documentation requirements; and g) circumstances requiring reclassification.

4.2.7 Financial Institutions shall ensure that customer risk classifications determine the nature, extent, and frequency of: a) Customer Due Diligence; b) Simplified Due Diligence; c) Enhanced Due Diligence; d) ongoing due diligence; e) transaction monitoring; sanctions screening; g) review of beneficial ownership information; and h) any other AML/CFT/CPF control required under these Regulations.

4.2.8 Customer risk classifications shall be reviewed and updated: a) periodically according to the customer's assigned risk category; b) whenever material changes occur in the customer's ownership, control, business activities, products, services, or expected transaction profile; c) following significant or unusual transaction activity; d) upon changes in beneficial ownership; e) following adverse media, regulatory findings, or law enforcement information; f) following changes in applicable sanctions lists; g) where the Financial Institution becomes aware of new ML/TF/PF risks; or h) whenever otherwise required by these Regulations or applicable law.

4.2.9 Financial Institutions shall document the basis for every customer risk classification and maintain evidence supporting the assigned risk rating.

4.2.10 Records relating to customer risk assessments, classifications, periodic reviews, reclassifications, approvals, and supporting documentation shall be

maintained in accordance with the Record Keeping requirements of the AML/CFT Act 2021 and this Regulation.

4.3 High Risk Customers and Accounts

4.3.1 Financial institutions shall have appropriate ML/TF/PF risk management systems to identify customers whose activities may pose a high risk of money laundering, financing of terrorism and financing of proliferation and shall exercise enhanced due diligence procedures in respect of such customers.

4.3.2 The ML/TF/PF risk management system for all licensed commercial banks which shall be used for transaction monitoring and detection shall be automated and effective and such system shall have the capability to detect suspicious and large transactions. Said system shall be documented, reviewed and updated regularly.

4.3.3 The ML/TF/PF risk management system for all other licensed financial institutions used for monitoring may be manual or automated but effective. Said system shall be documented, reviewed and updated regularly.

4.3.4 Accounts for Mandatory Classification

a. Casino;

b. Politically Exposed Persons (PEPs);

c. Non-resident customers;

d. Private/Prestige banking customers;

e. Cross-border banking and business relationships;

f. Legal persons or legal arrangements such as trusts, customer accounts that are personal-assets holding vehicles;

g. Companies that have nominee shareholders or shares in the bearer form;

h. High Net Worth individuals; Religious Leaders;

i. Natural or legal people who do business in precious metals/minerals, petroleum;

j. Designated Non-Financial Businesses and Professions;

k. Any customer deemed high-risk by the Financial Institution;

l. Other high-risk customers as may be determined by the National Risk Assessment findings; and

m. Any other categories of customers, or customers/transactions connected with countries, products and/or services that the Supervisory Authorities designate as high risk (including: MVTS providers, non-face-to-face customers).

4.5 Politically Exposed Persons (PEP)

4.5.1 Financial Institutions shall develop appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person, or a family member or close associate of such PEP. Financial Institutions shall take the following Risk management Procedures for Foreign, Domestic and International PEP:

i. obtain written approval from a designated senior manager before establishing a business relationship with such customer or beneficial owner.
ii. Where a customer has been accepted or has an ongoing relationship with a financial institution and the customer or beneficial owner is subsequently found to be or become a PEP, the financial institution shall obtain senior management approval in updating customers risk profile when continuing the business relationship.
iii. take reasonable measures to identify the source of wealth and source of funds;

4.5.2 PEPs should include, but are not limited to the persons listed in the following:

i. A non-exhaustive list of domestic PEPs is in Annex 45.2
ii. A non-exhaustive list of foreign PEPs is in Annex 45.3
iii. International PEP
iv. Family members and Close Associates of PEP

Additional Procedures for PEP

4.5.3 Where a financial institution deems it appropriate to establish business relationship prior to verification, it shall adopt a risk management procedure relevant for the occurrence of said condition. The procedures shall include measures such as: Limitation of the number, types or value of transactions that may be performed; and

4.5.4 The monitoring of large or complex transactions being carried out outside the expected norms for that type of business relationship.

4.5.5 Financial Institutions are required to ensure that the handling of a client who is no longer entrusted with a prominent public function should be based on a risk-based assessment and not on prescribed time limits.

4.5.6 The provision of sub-section seven (7) above abrogates the requirements of Section 2.12 of the PEP Regulation 2019, which required Financial Institution(s) to apply a Risk-based Approach in the handling of a customer who is no longer entrusted with a prominent public function.

4.5.7 Before making a payout under a life insurance policy, financial institutions shall take reasonable measures to determine whether the beneficiary or the beneficial owner of the beneficiary of a life insurance policy is a politically exposed person. Where higher risks are identified, financial institutions shall inform senior management before the payout of the policy proceeds, conduct enhanced scrutiny on the whole business relationship with the policyholder, and submit a suspicious transaction report to the Financial Intelligence Agency.

5.0 Policies and Procedures

5.1 All financial institutions shall develop and implement written internal Risk-based AML/CFT/CPF policies and procedures for the prevention of money laundering, terrorist financing and proliferation financing and for the management and mitigation of money laundering and terrorists financing risks in accordance with §15.3.12 of the AML/CFT Act of 2021.

5.2 The financial institutions shall develop and implement internal programs for the prevention of money laundering, terrorism financing and proliferation financing and for the management and mitigation of existing and emergent ML/TF/PF risks and such programs shall require regular updates;

5.3 Such programs shall be approved by the Board and senior management and be monitored and enhanced, if and as necessary.

5.4 The program shall be appropriate to all the risks faced by the financial institution including those identified under the national risk assessment process on AML/CFT/CPF and be proportionate to the nature and size of the reporting entities' business, and should at minimum include internal policies, procedures and controls for:

i. All AML/CFT/CPF obligations stated in the AML/CFT Act OF 2021, this regulation and other relevant laws and regulations;
ii. Be approved (signed off/dated) by the Board and Senior Management
iii. Distributed to all staff;
iv. Specify in detail policies, procedures and obligations of all staff to fully implement AML/CFT/CPF preventive measures;
v. Cover all customers/clients, products, services, transactions, business lines, branches and subsidiaries
vi. Developing and keeping the entity's business strategy up to date including the risk appetite.

6.0 Compliance and Compliance Officer: The board shall set up an independent compliance function and appoint a Compliance Officer at a Senior Managerial Level. The Compliance Officer shall be responsible for coordinating, monitoring and facilitating compliance with existing laws and regulations, and improve the bank's compliance policy and procedures. The Compliance Officer and appropriate staff shall have unrestricted and timely access to all books, records and employees of the financial institution as it is necessary to fulfill his/her responsibilities.

6.1 The Compliance Officer shall report directly to the Board of Directors or the Sub-Committee of the Board responsible for risk and compliance to ensure operational independence, on all matters relating to AML/CFT&PF.

6.2 The Compliance Officer must have sufficient authority, independence and seniority to be able to effectively carry out his/her duties in accordance with the AML/CFT Act 2021. The Financial Institution shall ensure that the Compliance Officer possesses the required professional qualification in AML/CFT/CPF Compliance and Risk Management and financial crimes.

6.3 The Compliance Officer shall be removed ONLY by the Board of Directors of the Financial Institution on grounds of: a) conviction of fraud, corruption or other financial crimes or a felony; b) personal or professional misconduct as per requirements of standards set in the Financial Institution Policy/Code of Conduct, c) failure to satisfy the terms and conditions of service or d) other good cause, after due process.

6.4 The duties of the Compliance Officer shall include but are not limited to the following:

i. Ensure the effective implementation of Financial Institution AML/CFT/CPF policies and procedures;
ii. Have an oversight of the AML/CFT/CPF control measures in all relevant business areas for the purpose of establishing a reasonable risk level consistent with the size and complexity of the Financial Institution;
iii. Keep the AML/CFT/CPF program current relative to the institution's identified inherent risks and consider local and international developments in ML/TF/PF;
iv. Receive and vet suspicious (unusual) transaction/activity reports from the staff;
v. Conduct regular risk assessments of the inherent ML/TF/PF risks including timely assessments of new products, services and business acquisition initiatives to identify potential ML/TF/PF risks and develop appropriate control mechanisms;
vi. File suspicious, Electronic Currency, Politically Exposed Persons, Cash Transaction Reports and other relevant regulatory reports with the FIA;
vii. Coordinate, with the specific approval of the Board of Director, the conduct of periodic assessments of AML/CFT/CPF control mechanisms to ensure their continued relevance and effectiveness in addressing changing ML/TF/PF risks, assess operational changes, including the introduction of new technology and processes to ensure that ML/TF/PF risks are addressed;
viii. Regularly review, update and sign off on all account opening packages including new or existing customers at all branches.
ix. Ensure systems and resources, including those required to identify and report suspicious transactions and suspicious attempted transactions, are appropriate in all relevant areas of the institution;
x. Ensure that ongoing training programs on ML/TF/PF are current and relevant and are carried out for all employees, senior management and the Board;
xi. Ensure that systems and other processes that generate information used in reports to Senior Management and the Board are adequate and appropriate, use reasonably consistent reporting criteria, and generate accurate information;
xii. Report pertinent information to the Board and Senior Management regarding the adequacy of the AML/CFT/CPF framework or any associated issues; and

xiii. Serve both as a liaison officer with the CBL and the FIA and a point-of contact for all employees on issues relating to ML/TF/PF.

6.5 Financial Institutions shall assess the working strength of the compliance function and all its sub-divisions on an annual basis and if any deficiency is observed, prompt corrective action shall be considered.

6.6 Financial Institution shall incorporate procedures to record and maintain data of account opening or customer relationships cases rejected by compliance or customer service units; the cases where customers' risk ratings recommended by business units were challenged or revised, and the cases where accounts or customer relationships were closed based on ML/TF/ PF risks.

6.7 Employees of Financial institutions shall be strictly prohibited from disclosing the fact to a customer or any other person that an STR or related information is being or has been reported to the FIA, except if required by law. This ethic shall be incorporated in the appropriate internal policies and be signed by employees and directors at the time of inductions.

7.0 Employee Due Diligence (Know Your Employee)

7.1 Adequate screening and hiring procedures to ensure appropriate and high standards when hiring all employees, whether contractual or permanent or hired through outsourcing. In this respect, financial institutions shall inter alia regularly ensure that:

i. All employees are screened against lists of designated and prescribed individuals, on an ongoing basis, and maintain a proper record of screening. Accordingly, employees shall become disqualified if they are designated or proscribed or associated by any means directly or indirectly.
ii. No employee has been convicted/involved in any fraud/forgery, financial crime; etc.
iii. No employee is or has been associated with any illegal activity concerning banking business, foreign exchange business financial dealing and other business or employment.
iv. Financial Institutions comply with the Fit and Proper Criterion required for shareholders and/or board approval and all senior management appointments.
v. The AML/CFT/CPF performance review of staff shall be part of employees' annual performance appraisals.
vi. Verify the applicant's identity and personal information including employment history and background and consider credit history checks using a risk-based approach;

vii. Develop a risk-based approach to determine when pre-employment background screening is considered appropriate or when the level of screening should be increased, based upon the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which shall include verification of references, experience, education and professional qualifications;

viii. Implement a continuous screening process for certain positions to account for changing circumstances or to conduct a thorough review of employees over time. Internal policies and procedures, such as codes of conduct, ethics, and conflict of interest guidelines, should be established to evaluate employees effectively. For instance, in a financial institution, senior management positions may require ongoing screening to address changes in regulatory requirements or shifts in organizational priorities. Policies like an ethics code and conflict of interest disclosure forms can help identify potential risks and ensure employees align with the organization's values and compliance standards;

ix. Have a policy that addresses appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or employee provided.

x. Verification shall generally include the following:

a) Reference checks
b) Checking the authenticity of academic qualifications
c) Verifying Employment History
d) Police background checks and clearance
e) Integrity checks against each licensed bank-financial institution, non-bank financial institution and the CBL Engaged and Disengaged Database

xi. Financial Institutions shall document and keep evidence of the above processes.

xii. Financial Institutions, where applicable or permitted, shall ensure the laws of the relevant country and similar recruitment policies are followed by its branches, subsidiaries and associate companies abroad, especially in those countries which are not sufficiently compliant with FATF standards.

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

xiv. Financial Institutions shall establish and maintain procedures to ensure high standards of integrity among employees, including the meeting of statutory "fit and proper" criteria of the officers of the Financial Institutions. The standards shall include a code of conduct for all employees and procedures shall allow for regular reviews of employees' performance and their compliance with established rules and standards. It shall also provide for disciplinary action in the event of breaches of these rules.

8.0 MONITORING OF EMPLOYEE BEHAVIOUR

8.1 Financial Institutions shall conduct ongoing monitoring of employees' accounts for potential signs of ML/TF/PF and pay special attention to employees whose lifestyles cannot be supported by their salary or known financial circumstances. Managers shall be encouraged to get to know the employees in their department and investigate any substantial changes in their lifestyles which do not commensurate with their financial position. Internal procedures shall provide for special investigation of employees who are associated with unexplained shortages of funds.

8.2 Financial Institutions shall also subject employees' accounts, including accounts of key senior 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 Compliance Officer. The Compliance Officer's account is to be reviewed by the Internal Audit or a designated Officer by the Management of the Financial Institution. Compliance reports, including findings on the Compliance Officer's account, shall be submitted to the CBL during the bank's quarterly DCT reporting each year.

8.3 The AML/CFT/CPF performance review of staff shall form part of employees' annual performance appraisal.

8.4 Financial Institutions shall provide **on-going Training**, i.e. general and specialized, at least twice a year for all statutory directors, officers, employees and agents relating to money laundering, terrorism financing, and on AML/CFT laws, regulations, measures, policies and procedures of the reporting entity and as required by the AML/CFT Act and this Regulation. The training shall cover relevant scope and depth commensurate with staff functions, experience and grid.

8.5 Financial Institutions shall provide comprehensive training programs for staff covering compliance officers and as part of the orientation programs for new staff and those posted to the front office, banking operations and branch office staff, particularly cashiers, account opening, mandate, marketing, internal control and audit staff;

8.6 Financial Institutions shall render returns on their level of compliance on its education and training programs to the Supervisory Authorities; twice every year, the first return of the year shall cover the latter half of the previous year and shall be submitted on January 15, and the second return, shall be submitted on July 31. The first return of the year shall be submitted along with the training plan (training schedule and estimated training budget).

8.7 An AML, CFT and CPF training program shall be developed under the guidance of the compliance officer in collaboration with top management and shall be approved by senior management and the Board of Directors;

8.8 The basic elements of the AML CFT and CPF training program of Financial Institutions shall include:

i. AML, CFT and CPF Laws and Regulations;

ii. the nature of ML, TF and PF and offences;

iii. ML, TF and PF "red flags" and suspicious transactions, including trade-based money laundering typologies;

iv. reporting requirements;

v. Customer Due Diligence;

vi. risk-based approach to AML, CFT and CPF; and

vii. record keeping and retention policy.

viii. Financial Institutions shall submit its annual AML, CFT and CPF employee training program for the following year to the CBL on January 15 consistent with section 8.5 above.

8.9 Records of the training materials used and documentation of attendance, dates and times that training programs shall be retained in files for the purpose of AML/CFT/CPF supervisory inspections.

9.0 NON-PROFIT ORGANIZATION (NPO)

9.1 These organizations vary widely in size, income, structure, legal status, membership, and scope. Their activities include raising or distributing funds

for charitable, religious, cultural, educational, social, or fraternal purposes, as well as engaging in other forms of "good works." They encompass a broad spectrum, from large regional, national, or international charities to local community-based self-help groups. The category also includes research institutions, churches, clubs, and professional associations. Most of these organizations rely, fully or partially, on charitable donations and voluntary contributions for their operations.

9.1.1 To assess the risk, a financial Institution shall require:

i. Evidence of registration under applicable laws of the home and local operation;
ii. The organization's donor, volunteer and member base;
iii. The organization's purpose, ideology or philosophy;
iv. The geographic areas covered and served (including headquarters and operational areas);
v. The organizational structure of the institution;
vi. Record keeping requirements;
vii. Funding and disbursement criteria (including basic beneficiary information);
viii. Affiliation with other organization, Governments or groups;
ix. Identity of all signatories to the organization's account; and
x. Identity of board members and trustees, where applicable.

9.2 Financial Institutions shall apply CDD measures proportionate to the assessed ML/TF/PF risk, considering the customer's size, nature of activities and geographical risk exposure.

10.0 TERRORIST FINANCING

10.1 Financial Institutions shall, as part of the CDD/EDD process, carry out due diligence against publicly available terrorist lists and monitor on an ongoing basis whether funds are being sent to high-risk countries. A non-profit organization (NPO) should be registered in Liberia and where it is registered outside of the country, then the Financial Institution shall as additional due diligence measures contact the appropriate overseas competent authority to confirm its existence. Financial Institutions shall satisfy themselves as to the legitimacy of the organization by, for example, requesting a copy of the NPO's constitution among other things.

10..2 Financial Institutions that suspect or have reason to suspect that funds or the proceeds of criminal activity are related to terrorist financing, shall report immediately or not later than twenty-four (24) hours, its suspicions to

the FIA. All suspicious transactions, including attempted transactions, are to be reported regardless of the amount involved. This requirement to report suspicious transactions shall apply regardless of whether they are thought, among other things, to involve tax matters.

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

10.4 In processing wire/electronic transfers, Financial Institutions 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.

11.0 AUDIT

11..1 Implement internal audit arrangements to review, test and verify the adequacy, completeness and effectiveness of AML/CFT/CPF policies, procedures, systems and compliance, as well as initiate corrective actions where compliance deficiencies are identified. The reviews shall be performed by an experienced person/entity (Internal and External) with the requisite international credential in anti-money laundering and or anti-fraud systems and an appropriate level of knowledge of the regulatory requirements and guidelines. It is required that the said person shall determine the adequacy, completeness and effectiveness of the AML/CFT/CPF compliance function.

12.0 COMPLIANCE WITH OBLIGATIONS BY FOREIGN SUBSIDIARIES AND BRANCHES:

12.1.1 Financial Institutions shall ensure that foreign branches and subsidiaries observe AML, CFT and CPF measures consistent with the provisions of these Regulations and apply the measures to the extent that domestic applicable laws and regulations of the host country so permit.

12.2 Group-level compliance, audit and anti-money laundering, counter terrorism financing and counter proliferation financing functions shall have the power to request and be provided customer's account and transaction information from parent companies, branches, and subsidiaries as necessary to fulfill their

functions and secrecy and confidential provisions shall be overridden for purposes of the sharing of information.

12.3 Financial groups shall develop and implement policies and procedures for sharing of information within the group for anti-money laundering, counter terrorism financing and counter proliferation financing purposes and for safeguarding the confidentiality and use of the shared information in line with this section, the AML/CFT Act and these Regulations.

12.4 Reporting entities shall require foreign branches and any subsidiaries over which it has control to apply appropriate measures to manage their money laundering and terrorist financing risks and to implement the requirements of the AML/CFT Act and these regulations issued hereunder to the extent that the applicable laws and regulations in the jurisdiction where the foreign branch or subsidiary is domiciled so permit. If such laws prevent compliance with these obligations for any reason, the reporting entity shall advise its competent supervisory authority and apply additional measures to manage the money laundering and terrorist financing risks.

13.0 HIGHER RISK COUNTRIES

13.1 Financial Institutions shall apply enhanced due diligence proportionate to the risk to business relationships and transactions with natural or legal persons (including financial institutions) from countries for which FATF raised such concerns.

13.2 Pursuant to section 15.3.14 of the AML/CFT/ Act of 2021, Financial institutions shall apply specific counter measures against high-risk countries, including the mandatory application of enhanced due diligence measures. These counter measures may include, inter alia-

i. Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or avoiding doing business with limited AML/CFT/CPF compliance,
ii. Requiring financial institutions to review and amend, or if necessary, terminate correspondent relationship with financial institution in the country concerned;
iii. Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions;
iv. Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned;
v. Prohibiting reporting entities from relying on third parties located in the country concerned to conduct elements of the due diligence process;

vi. Conducting any other measure as may be required by the Supervisory Authority.

vii. In considering requests for licensing or approval for the establishment of subsidiaries or representative offices, FIs shall ensure that the country has adequate AML/CFT/CPF systems in place and if not, conduct the appropriate EDD procedures;

viii. Financial Institutions advise their customers that transact with natural or legal persons within that country that there is a high risk of ML/TF/PF. The Financial Institution shall therefore limit business relationships or financial transactions with the identified country or persons in that country.

14.0 OBLIGATIONS OF TRUSTEES

14.1 A trustee must disclose its status to a reporting entity, when as a trustee, before it establishes a business relationship or carries out an occasional transaction above the stipulated threshold.

14.2 A Trustee must provide reporting entities with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship.

15.0 Record Keeping Obligations

15.1 Financial institutions shall accurately and securely obtain and maintain all customers' documentary records for a minimum of seven (7) years from the date of termination of the business relationship.

15.2 Financial institutions shall maintain documentary records including those obtained through CDD/KYC measures such as official identification documents; informational data on the customer, beneficial owner or Domestic and International transactions; business correspondence, results of any analysis undertaken; all other necessary documents as may be requested by the Supervisory Authorities.

15.3 Transaction records maintained by Financial Institutions shall be sufficient to permit the reconstruction of individual transactions so as to provide evidence for prosecution of criminal activity.

15.4 Financial Institutions shall ensure that all customer records, information or transactions are made readily available upon request by the Supervisory Authorities

15.5 Financial Institutions shall maintain reports of suspicious transactions, cash transactions and attempted suspicious transactions for at least seven (7) years.

16.0 Prohibition against relations with shell banks

16.1.1 Establishment of any business relations or executing any transaction with a shell bank is absolutely prohibited.

17.0 Prohibition against Anonymous and Numbered accounts

17.1 Opening, establishing, operating or maintaining an anonymous, numbered or account in fictitious name is absolutely prohibited. Any account in such category that existed prior to the enactment of the AML/CFT and FIA Acts of 2021 shall be closed or subject to effective and thorough CDD/KYC procedures and AML/CFT risk assessment.

18.0 Suspicious Transactions Monitoring and Reporting

18.1 All financial institutions must submit suspicious transactions reports (STRs) as soon as possible but not later than three (3) days to the Financial Intelligence Agency (FIA) if they suspect or have reasons to suspect that any funds, property, or transaction is related to, intended for use in, or linked in any other way to money laundering or its predicate offences, proceeds of crime, or terrorism, terrorist acts or terrorist organizations, or is to be used for terrorism, terrorist acts or terrorist organizations or those who finance terrorism.

18.2 Financial institutions shall have a written Policy Framework that guides and enables their staff to monitor, recognize and respond appropriately to suspicious transactions in addition to the guidance issued by competent authorities.

19.0 NEW BUSINESS WITH EXISTING CUSTOMERS

19.1 If an existing customer closes an account and opens another or enters into a new agreement to purchase products or services, the Financial Institution shall

apply a risk-based approach in the CDD/EDD procedures. This is particularly important given the following instances:

i. if there was an existing business relationship with the customer and identification evidence had not previously been obtained;
ii. or if there has been no recent contact or correspondence with the customer for a period of two years or more; or when a previously dormant account is re-activated.
iii. in line with the conditions stated above, details of the previous account(s) and any identification evidence previously obtained, or any introductory records should be linked to the new account records and retained in accordance with record keeping requirements.

20.0 RISK-BASED CUSTOMER DUE DILIGENCE and Enhanced Customer Due Diligence

20.1 Financial Institutions shall carry on risk-based enhanced customer due diligence for accounts designated above as high risk and this process shall include but not limited to:

i. Customer Identification and Verification of information such as full name, address, date of birth, and identification numbers. For entities, incorporation documents and information on directors and beneficial owners.
ii. Risk Assessment which should focus on assigning risk rating based on predetermined ML/TF/PF risk parameters.
iii. Ongoing Monitoring which should focus on updating customer information and reassessing risk profiles
iv. Enhanced Due Diligence (EDD) which is applying additional scrutiny to high-risk customers, and;
v. Reporting

21. New Products, Technologies and non-face-to- face business relationships

21.1 The rapid advancement and expanded capabilities of new technologies for delivering financial services pose significant challenges for countries and private sector financial institutions in preventing the misuse of these payment products and services for money laundering, terrorism financing, and proliferation financing. Emerging alternatives, such as virtual currencies and

various forms of electronic money, exemplify this shift from traditional financial services. Financial Institutions shall identify and assess the money laundering or terrorist financing risks that may arise in relation to the development and deployment of new products and new business practices, including new delivery mechanisms for products and services; the use of new or developing technologies for both new and pre-existing products; and non-face-to-face transactions or relationships

21.2 The Risk Assessment of all Financial Institutions shall take place prior to the launch of the new products, business practices or the use of new or developing technologies which shall be documented, and appropriate measures shall be taken on an ongoing basis to manage and mitigate such risks;

21.3 Financial Institutions shall have policies and procedures in place to address any specific risk associated with non-face-to-face transactions or business relationships;

21.4 The Policies required to be taken shall be applied automatically when establishing customer relationships and conducting ongoing due diligence; the measures for managing the risks are to include specific and effective CDD procedures that are applicable to non-face-to-face customers.

22. AML/CFT Customer Due Diligence/Know Your Customer (CDD/KYC) Obligations

22.1 Financial institutions shall establish, implement, and maintain adequate and effective customer due diligence policies, procedures and controls, consistent with a risk-based approach, to identify, verify and monitor all customers seeking to establish or maintain a business relationship or conduct occasional transactions with the institution. These procedures shall consist of:

i. Identifying any natural person authorized to act on behalf of the customer, verifying such persons through credible and independent documentation and confirming that the person is authorized thereto, pursuant to the relevant applicable rules.

ii. Identifying the beneficial owner, and taking all reasonable and proportionate measures to verify their identity, using reliable, independent source documents, data or information until the

Financial Institution is reasonably satisfied that they know who the beneficial owner is;

iii. Obtaining and maintaining information on, and understanding, the purpose and nature of the business relationship or the transaction;

iv. For customers that are legal persons or legal arrangements, identifying and understanding the nature of the customer's business activities, ownership and control structure, and the beneficial owner.

22.2 Customer Identity Requirements: Customer identity documentation must be obtained and verified:

i. before opening any account for or otherwise establishing a business relationship with a customer.

ii. when an occasional customer (non-account holder) wishes to carry out transactions equal to or exceeding US$1,000.00 or its Liberian Dollars equivalence at the prevailing approved exchanged rate or as may be determined by the Supervisory Authority from time to time, including where the transaction is carried out in a single or several operations that appear to be linked;

iii. when transactions are carried out in several operations involving smaller amounts totaling the designated threshold stipulated above.

iv. when carrying out occasional transactions that are wire transfers including cross-border and domestic transfers between Financial Institutions and when credit or debit cards are used as payment method to effect money transfer;

v. during acquisition of Prepaid Cards;

vi. when any doubts exist about the veracity or adequacy of previously obtained customer identification information;

vii. whenever there is a suspicion of money laundering, financing of terrorism or financing of proliferation involving the customer or the customer's account.

viii. Financial Institutions shall obtain and maintain documentary records for each client, customer or natural person and verify by means of reliable and independent source documents or information (such as a passport, a driver's license, or national identification documents):

- Legal Identity (full name) of the person
- date and place of birth
- permanent address and/ or residential address
- contact details (i.e.., phone, cellphone, email, social media handle, etc.)
- nationality
- occupation
- public position held and/or name of the employer
- a unique identifier contained in an unexpired official document that bears a photograph of the customer and a signature
- Resident and/or Work Permit (For Non-Liberians)

22.3 The identity records must also be obtained, verified and maintained on all persons purporting to act on behalf of a customer, together with documentation that proves that the person is legally authorized to act in a representative capacity. The above documentation is required to be maintained in documentary form for all clients/customers, including customers which established relations with the financial institution prior to enactment of the AML/CFT and FIA Acts of 2021. Obtaining identity records and documentation for previously existing customers must be completed no later than 1 year from the date of publication of this regulation.

22.4 Financial Institutions shall refer to Annex 43.1 for KYC/CDD/EDD requirements during onboarding and ongoing due diligence

22.5 Financial Institutions shall screen customers at onboarding against all domestic and international sanctions lists (including but not limited to UNSCR, OFAC, EU, ECOWAS)

22.6 For Legal entities, financial institutions shall obtain, verify and maintain documentary records including:

i. the above identity information/data applicable to natural persons in respect of all who serve as directors, founders, those authorized to execute transactions on behalf of the entity, and those who are beneficial owners which own, control or influence the business decisions of the legal entity; and

ii. the corporate name, head office address, documentary proof of official incorporation or similar evidence of legal status and legal form, provisions governing the authority to bind the legal person or legal arrangement, and any additional information and documents necessary to understand the ownership and control of the legal person or arrangement.

22.7 **Beneficial Owner Requirements:** Financial institutions shall identify the natural persons who are beneficial owners of legal entities and or natural persons and take reasonable measures to verify the identity. To determine the beneficial owner of a customer, the financial institution shall:

22.7.1. For customers that are legal persons, obtain and take reasonable measures to verify:

i. The identity of any natural person(s) who ultimately owns or controls a legal entity by directly or indirectly owning more than applicable percentage threshold of the shares or voting rights or ownership interests in the legal person, including through bearer share holdings, trust arrangements or other means; or

ii. if there is doubt under Section **18.7(i) of this AML/CFT&PF Regulation** as to whether the person(s) with controlling ownership interests is the beneficial owners), or where no natural person under **18.7(i)** is identified, the identity of the natural person(s) exercising ultimate effective control over the legal person through other means; or

iii. where no natural persons are identified under **18.7(i) or 18.7(ii) of this Regulation,** the identity of the natural person(s) who holds the position of senior managing official.

22.8 For legal arrangements, obtain and take reasonable measures to verify:

i. For Trusts, the identity of the settlor, the trustee(s), the protector if any, the beneficiaries or where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates, and any other natural person directly or

indirectly exercising ultimate effective control over the trust, including through a chain of control or ownership; and

ii. For other types of legal arrangements similar to Trusts, the identity of the natural persons holding equivalent or similar positions as those indicated above.

22.9 For life and other investment related insurance businesses, in addition to applying regular identification and verification measures to customers and beneficial owners, undertake the following measures as soon as beneficiaries of life or investment-related insurance policies are identified or designated:

I. For beneficiaries that are identified as specifically named natural or legal persons, or legal arrangements, take the name of that person;

II. For beneficiaries that are designated by characteristics or class, or by other means, obtain sufficient information concerning the beneficiaries to satisfy the life or investment related insurance business that it will be able to establish the identity of the beneficiary at the time of the pay-out; and

III. In all cases, verify the identity of the beneficiaries at the time of the pay-out

22.10 Know Your Customer (KYC) – understand and obtain information on the purpose and nature of accounts and transactions: To effectively identify suspicious transactions in fulfillment of the suspicious transaction reporting obligation, in addition to fulfilling customer identity requirements, financial institutions shall obtain and maintain sufficient information and data from each client to have a sufficient understanding of the profile of expected transactions and account activity for the client in view of the client's stated business and sources of income.

22.11 Timing of CDD—establishment of business relationship

22.11.1 Financial Institution(s) shall conduct CDD for a customer before the establishment of business relationship;

22.11.2 However, the CDD may be conducted during the establishment of the business relationship if:

i) this is necessary in order not to interrupt the normal conduct of business;

ii) there is little risk of money laundering or terrorism financing and these risks are effectively managed;
iii) the CDD is completed as soon as practicable after contact is first established with the customer; and
iv) the CDD is conducted in accordance with the policies, procedures, systems and controls on the use of the business relationship even before the customer's identity is verified.

22.11.3 Financial institutions shall, in cases where their supervisory authority permits the establishment of a business relationship with a customer prior to verification, adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship.

23. FINANCIAL INCLUSION MEASURES

23.1 Financial Institutions shall develop and implement internal policies and procedures for persons that are socially and financially disadvantaged to ensure that they have reasonable access to, and equitable usage of tailored banking products, services and facilities aimed at promoting financial inclusion.

23.2 Financial Institutions shall review its Financial Inclusion Policy and/or procedures for persons with social and financial disadvantages at least every two years.

22.3 Financial Institutions shall conduct risk assessments of all products and services applicable to financial inclusion, in accordance with Section 4.0 of this regulation

22.4 Access to basic banking and financial services is essential for most adults. It is therefore crucial that individuals who are socially or financially disadvantaged are not excluded from opening accounts or accessing financial services simply because they lack standard identification documents. In cases where providing such evidence is not feasible, financial institutions must implement internal procedures that accommodate these individuals. This includes offering clear guidance to staff on how to verify the identities of such individuals and outlining the specific checks to be conducted in these exceptional situations.

22.5 If a Financial Institution determines that a customer cannot reasonably provide the required detailed proof of identity, the institution should take the following steps:

i. Accept a letter or statement from a responsible individual who knows the customer and can confirm their identity, including their permanent address.
ii. Verify the identity of the guarantor providing the confirmation.
iii. Provide basic, low-risk account services to the customer.
iv. Allow a 90-day grace period for the customer to obtain his/her Liberian Citizen ID Card.
v. Discontinue any ongoing activities for the customer if they fail to provide the required information within the stipulated grace period.
vi. Submit a Suspicious Transaction Report (STR) to the Financial Intelligence Agency (FIA) if unusual activity or ML/TF/PF risks are suspected.

22.6 A Financial Institution shall submit an annual report on financial inclusion activities undertaken during a stated year, to the Central Bank of Liberia by January 31 of the ensuing year.

23.0 Simplified Customer Due Diligence

23.1 Financial Institutions shall perform CDD measures proportionate to the level of risks involving the customers, their businesses and their transactions, and shall perform EDD where the ML/TF/PF risks are higher pursuant to §15.3.1 of the AML/CFT Act of 2021.

23.2 Financial Institutions may apply simplified customer due diligence measures where lower risks have been identified through the National and/or Sectorial Risk Assessment, or the Financial Institution's risk assessments.

23.4 The simplified customer due diligence measures shall commensurate with the lower risk factors, but not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios and shall at minimum include:

a) Reducing the frequency of updating customer identification information;
b) Reducing the degree of on-going monitoring and scrutinizing transactions;
c) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship.

24.0 Inability to fulfill Customer Identification Obligations

24.1 Where a financial institution is unable to verify the identity of the customer and beneficial owner(s) or comply with other CDD measures set out in these regulations, it shall refrain from opening the account or commencing the business relationship or carrying out the transaction, or it shall terminate the business relationship.

24.2 In such cases, the Financial Institution shall consider filing a suspicious transaction report to the Financial Intelligence Agency (FIA). A Financial Institution shall also consider submitting a suspicious transaction report to the FIA when the customer refuses to provide information required by Law.

24.3 Where a Financial Institution suspects money laundering, terrorism financing or proliferation financing and reasonably believes that conducting CDD measures could tip off the customer, it shall:

- Cease the CDD process; and
- File a Suspicious Transaction Report (STR) with the FIA.

25.0 Enhanced Due Diligence

25.1 Enhanced due diligence procedures shall apply to all customers and customer accounts classified as high risk. These procedures shall include:

i. obtaining additional documentation concerning customer identity, verification, purpose of the account and nature of transactions, volume of assets, transaction profile and additional documentation to satisfy the Financial Institution that it understands the sources of funds involved in transactions and in the account;
ii. update more regularly the identification data of the customer and beneficial owner;

iii. obtain additional information on the intended nature of the business relationship;
iv. obtain information on the reasons for intended or performed transactions;
v. obtain information on the source of funds or source of wealth of the customer;
vi. conducting periodic monitoring of transactions and transaction patterns in the account; and increasing the number and timing of controls applied and selecting patterns of transactions that require further examination;
vii. requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standard;
viii. documenting the enhanced due diligence procedures applied to the account.

25.2 Financial Institution(s) are required to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. If and when the Financial Institution(s) determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it is required to perform enhanced due diligence, which should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of the payout.

26. TRANSACTION MONITORING AND REPORTING SYSTEMS

26.1 Financial Institutions shall adopt appropriate procedures for the identification of unusual transactions patterns and activities that are not consistent with the customer's risk profile.

26.2 Financial Institutions shall implement processes to analyze transactions patterns and activities to determine if they are suspicious and meet the required threshold for reporting.

26.3 Transaction monitoring systems can differ in scope and sophistication, ranging from automated, complex systems that integrate customer data with core banking applications to simpler setups, depending on the size, volume, and complexity of the business operations. Regardless of the system's sophistication, maintaining up-to-date customer information is essential for identifying unusual activities effectively.

26.3.1 Monitoring can be conducted in two ways:

i. In real-time, where transactions or activities are reviewed as they occur or just before they are executed.
ii. Post-event, through an independent review of the transactions or activities a customer has already completed.
iii. Financial Institutions shall also have systems and procedures in place to deal with clients who have not had contact for some time, such as dormant accounts or relationships, to be able to identify future reactivation and unauthorized use of said account
iv. When designing monitoring arrangements, it is crucial to consider the frequency, volume, and size of customer transactions in relation to the assessed risks associated with the customer, product, and delivery channels. Monitoring systems should facilitate trend analysis of transaction activities, including tracking transactions involving parties in high-risk countries or jurisdictions, to detect unusual or suspicious business relationships and transactions. These systems must enable the Compliance Officer to oversee and report significant customer relationships and activities—either individually or on a consolidated basis across the financial group—to the Board and senior management. Additionally, they should identify activities that deviate from the institution's understanding of the customer, their business, and their risk profile.
v. The parameters and thresholds used to trigger alerts for unusual transactions or activities must be tailored to align with the FI's money laundering, terrorism financing, and proliferation financing (ML/TF/PF) risk profile, as well as the complexity and scale of its operations. While standard parameters provided by vendors may be utilized, the Financial Institution must validate and demonstrate to the Central Bank of Liberia that these parameters are suitable for its specific risk exposure. The monitoring system should undergo testing at least annually to ensure the parameters function effectively and remain relevant. Based on the testing results, adjustments may be necessary. All findings, analyses, and proposed changes must be documented, including:

    a. The reasoning behind the review of parameters and thresholds;

b. Details of the testing process, including any assumptions made and the analysis of results; and

c. The specific modifications made to the parameters and thresholds.
d. Periodic training for the effective usage of Automated or Manual Tools before launch and after system modification

27.0 WHISTLE-BLOWING

27.1 Financial Institutions shall establish whistle-blowing policies that, at a minimum, include the following:

i. Provide written guidance to employees, ensuring they fully and always cooperate with regulators and law enforcement agencies.
ii. Include provisions for directors, officials, and employees to report any breaches of the institution's AML/CFT/CPF compliance program to the Compliance Officer.
iii. Specify that if the breach involves the Compliance Officer, employees must report the matter to a designated higher authority, such as the Internal Auditor.
iv. Clearly inform employees in writing that such reports must be kept confidential and assure them of protection against victimization for reporting.

27.2 Financial Institutions shall establish secure reporting mechanisms for suspicious activities such as hotlines and suggestion boxes.

28.0 Ongoing Due Diligence:

28.1 Financial Institutions shall conduct ongoing due diligence with respect to all client relationships and transactions which shall include:

i. ensure that documents, data and information related to the CDD processes are kept up-to-date and relevant on an ongoing basis, by undertaking reviews of existing records, particularly for high-risk categories of customers. They shall also consistently scrutinize and examine transactions undertaken by customers to ensure that they are consistent with their knowledge of their customers, their businesses and

their risk profile, including where necessary, the source of their funds;

ii. maintain current information and records relating to the customer and beneficial owner (not older than 2 years);

iii. ensure transactions are consistent with documentary evidence provided by the client concerning the purpose and nature of the account, financial activities and risk profile;

iv. pay special attention to and examining the background circumstances of all complex, unusual large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose; and

v. pay special attention to business relations and transactions with persons, including legal persons and arrangements, from or in countries that do not or insufficiently apply the relevant international standards to combat money laundering and the financing of terrorism.

28.2 In fulfillment of the above, Financial Institutions shall develop or acquire automated monitoring tools to monitor all transactions aimed at detecting suspicious transactions by their customers in real time or by the close of business day.

29. Prohibition of Personal accounts for business purposes

29.1 Financial Institutions shall not allow personal accounts to be used for business purposes except proprietorship, small businesses and professions where essential documents are not available and the financial institutions are satisfied with KYC profile of the account holder, purpose of relationship and expected turnover of the account keeping in view financial status and nature of business of that customer.

30. Tipping off and confidentiality

30.1 Financial institutions and their staff shall maintain confidentiality in respect of all investigations and any suspicious transaction report that may be filed with the FIA. This action is in compliance with the provisions as stipulated in Section 15.3.22 of the AML/CFT Act 2021 which criminalizes "tipping off". Tipping off refers to the act of doing or saying anything that might alert or give information to someone else that he/she is under suspicion of ML/TF/PF.

30.2 In cases where financial institutions have a suspicion of money laundering or terrorism financing and have reasonable grounds to

believe that performing the CDD measures will tip-off the customer, they shall not pursue the CDD measures, and shall instead file a suspicious transaction report with the FIA.

31.0 Trade Finance Customer

31.1 Financial Institutions shall undertake CDD measures of trade finance customers as prescribed in these regulations and ensure monitoring of such customers with regard to ML/TF/PF risks.

32.0 Deferral and Timing of Verification:

32.1 Financial Institutions shall obtain and verify the identity of the customer, beneficial owner and occasional customer before, during the course of establishing a business relationship or when conducting transactions on their behalf.

32.2 Financial Institutions may grant deferral only when the customer requesting a deferral of CDD documentation provides a **formal written commitment** to the Financial Institution, indicating clearly the **reason (s) for the deferral** and the specific timeframe within which the outstanding documents shall be submitted.

32.3 Financial Institutions are permitted to complete the verification of the identity of the customer or beneficial owner following the establishment of the business relationship only where:

i. The customer's identity has been primarily identified and verified using reliable and independent source documents.
ii. A risk assessment indicates that the relationship or transaction is low-risk at the point of onboarding. High risk customers or business relationships are strictly prohibited from participating in deferral arrangements.
iii. A written Senior Management approval is obtained and documented for the deferral.
iv. This can be done not later than two (2) weeks;
v. It is essential not to interrupt the normal business conduct of the customer in cases such as non-face-to-face business.

32.4 Examples of other circumstances where it may be essential not to interrupt the normal conduct of existing business are:

i. Securities: In the securities industry, companies and intermediaries may need to perform transactions rapidly, based on market conditions and customer contact, before identity verification is completed.

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

32.5 Where a Financial Institution deems it appropriate to establish business relationship prior to verification, it shall adopt a risk management procedure relevant for the occurrence of said condition. The procedures shall include measures such as:

i. Limitation of the number, types or value of transactions that may be performed; and
ii. The monitoring of large or complex transactions being carried out outside the expected norms for that type of business relationship.

32.6 Financial Institutions shall maintain a register of all deferred documentation cases, including the following details:

i. Customer name and identification number
ii. Reason for deferral
iii. Customer's risk rating
iv. Approval Authority
v. Date of deferral and completion

32.7 The register shall be made readily available to the Central Bank of Liberia upon request.

32.8 Financial Institutions shall submit quarterly reports of all deferred cases to the Central Bank of Liberia within fifteen (15) days after the end of each quarter. Failure to submit such reports within the prescribed timeframe shall constitute non-compliance and may attract administrative sanctions as provided under section 41 of this regulation. The Central Bank of Liberia reserves the right to conduct verification or request additional information on any deferred case reported.

32.9 Financial Institutions that misuse, extend or rely on deferral provisions without valid justification, or that fail to complete customer due diligence (CDD) within the stipulated timelines, shall be considered in breach of this Regulation. Such institutions shall be subject to enforcement actions, including administrative sanctions under Section 41, mandatory corrective measures and possible restrictions on the use of deferral provisions until compliance is fully restored.

32.10 Financial Institutions shall be prohibited from conducting CDD on their customers and/or beneficial owners where there is the risk of tipping off.

32.11 Financial Institutions shall take reasonable steps to ensure that they understand the nature of the business of legal persons and arrangements before or during the course of establishing a business relationship or conducting transactions on their behalf.

33. Application of CDD to Existing Customers

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

33.2 The appropriate time for Financial Institutions to conduct CDD for existing customers is the following non-limitative cases, when-

i. A transaction of significant value occurs;
ii. A customer's risk profile changes significantly;
iii. There is a material change in the way that the account is operated; or
iv. The institution becomes aware that it has insufficient information about an existing customer.

33.3 Financial Institutions shall properly identify the customer in accordance with the criteria contained in these regulations and the customer identification records shall be made available to the compliance officer, other appropriate staff and competent authorities.

33.4 Financial Institutions shall block accounts without valid identity documents (after serving one-month prior notice) for all debit transactions/withdrawals, irrespective of mode of payment, until the

subject regulatory requirement is fulfilled. However, debit block from the accounts shall be removed upon submission of valid identity document and verification of the same.

34. Reliance on Third Parties:

34.1 A Financial Institution that relies on third party reporting entities to undertake customer due diligence procedure on its behalf shall:

i. understand that the ultimate responsibility for customer identification and verification shall be with the financial institution relying on the third party;
ii. ensure that adequate Know-Your-Customer (KYC) Provisions are applied to the third party in order to obtain account information for competent authorities;
iii. ensure that all CDD information that has been obtained by the third party is sent to the financial institution as soon as practicable or that copies of documents obtained as part of the customer due diligence process are either provided or can be made readily available upon request without delay;
iv. ensure that arrangements with third party institutions are documented and can be made available for review by competent supervisory authority, upon request.
v. ensure that third-party intermediaries used for Customer Due Diligence procedures is:
   a. subject to adequate AML/CFT/CPF regulation, supervision or monitoring;
   b. has measures in place to comply with the CDD requirements set out in these regulations;
   c. subject to record keeping requirements issued pursuant in these regulations as well as the AML/CFT Act of 2021.

34.2 For Financial Institutions that rely on third party that is part of the same financial group, Financial Institutions may consider that the requirements of the criteria above are met in the following circumstances:

i. the group applies CDD and record-keeping requirements, in line with programs against Money laundering, terrorist financing and proliferation financing;
ii. the implementation of those CDD and record-keeping requirements and AML/CFT/CPF programs is supervised at a group level by a competent Supervisory authority; and

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

34.3 Such measures shall ensure that the identity documentation procedures are no less effective than where the customer appears in person, and should require additional documentary evidence, or supplementary measures to verify or certify the documents supplied, or certified confirmation from a trusted financial institution (at which the client maintains a client relationship or the previous financial institution at which the client had a relationship) or equally reliable documentary evidence.

35. Money or Value Transfer Services (MVTS)

35.1 All natural and legal persons performing money or value transfer service (MVTS Operators) shall be licensed by the CBL and shall be subject to the provisions of these regulations and relevant laws and regulations.

35.2 MVTS Operators shall ensure that none of their employee(s) or branches, payment booths and agents are involved in conducting or facilitating any sort of unauthorized/illegal money transfer service (illegal MVTS- Hundi Hawala) directly or indirectly;

35.3 MVTS Operators shall maintain a current list of their agents, branches, franchises, payment booths, currency exchange booths etc. and render quarterly returns to the CBL;

35.4 In addition to the requirement specified in this regulation, MVTS Operators shall gather and maintain sufficient information about their agents and correspondent operators or any other operators or institutions they are or likely to do business with.

35.5 MVTS Operators shall ensure effective systems for monitoring and ensuring compliance with AML/CFT/CPF obligations, controls and preventive measures to identify and mitigate ML/TF/PF risk posed to and from their entities as per their business and operational model. In fulfillment of this, the MVTS Operators shall at minimum:

i. Assess their agents' and correspondent operator's AML/CFT/CPF controls and ascertains that such controls are adequate and effective;
ii. Obtain approval from the CBL before establishing relationships with their correspondents;

iii. Document and maintain a checklist of the respective AML/CFT/CPF responsibilities of each of their agents and correspondent operators;
iv. Take appropriate measures to monitor all transfers for the purpose of detecting those which lack the originator and beneficiary information;
v. Prohibit transactions with designated persons and entities in line with the obligations set out in the relevant United Nations Security Council resolutions, Liberians laws and other relevant authorities;
vi. In the case of wire transfers, the MVTS operators shall comply with the applicable wire transfer obligations in these regulations;

35.6 In the case of a MVTS provider that controls both the ordering and the beneficiary sides of a wire transfer, the MVTS provider shall:

i. Take into account all the information from both the ordering and beneficiary sides in determining whether an STR shall be filed.
ii. File an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Agency (FIA).

35.7 Financial Institutions are prohibited from engaging in any transaction, including wire transfers, for the benefit of a person or entity designated under the UNSCRs 1267 and 1373 and their successor resolutions, or controlled directly or indirectly by the designated persons or entities, or for persons and entities acting on behalf of or at the direction of designated persons or entities; and required to freeze immediately and without delay, and within 24 hours, all the funds related to the designated person or entity when attempting to conduct any financial transaction.

36.0 FOREIGN EXCHANGE BUREAUS

36.1 Financial Institutions shall conduct EDD procedures with forex bureau in accordance with these Regulations. Satisfactory evidence of identity must include receipt of a certified copy of the applicant's operating license (Categories A or B) before the establishment of a business relationship.

37.0 Wire transfers

37.1 When executing wire transfers equal to or above the designated amount of $1,000 US dollars or the equivalent in Liberian dollars, Financial Institutions shall obtain, verify and maintain the following:

i. The full name of the originator;
ii. obtain and maintain the account number of the originator or in the absence of an account number, a unique reference number;
iii. The originator's address or national identity number or customer identification number or date and place of birth;
iv. the name of the beneficiary;
v. 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; and
vi. include the above information in the message or payment form which shall accompany or remain with the transfer throughout the payment chain.

37.2 Ensure that cross-border wire transfers of a value below the threshold specified in sub-section (1) of Section 37, include the name of the originator and the beneficiary, and both the originator and the beneficiary account number or a unique transaction reference number which permits traceability of the transaction. In such case, the ordering financial institution is not required to verify the information, unless there is suspicion of ML/TF.

37.3 **For Domestic wire transfers in the amount of (One Thousand United States Dollars) 1,000 USD or its equivalent in Liberian** dollars, full originator information shall be made available to the beneficiary financial institution and appropriate authorities by other means; and

37.4 For Cross-border, where several individual cross-border wire transfers of **(One Thousand United States Dollars**) $1,000 USD or its equivalent in Liberian dollars, from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain the required and accurate originator information (originator's account number or unique reference number) and full beneficiary information that is traceable within the beneficiary's Jurisdiction.

37.5 A Financial Institution generating a wire transfer: Financial Institutions as Ordering institutions (whether domestic or cross-border wire transfer), shall:

a) Identify and verify the originator (if it has not already done in accordance with these Regulations) and obtain details of beneficial owner(s) of funds; and
b) Record adequate details of the wire transfer so as to permit its reconstruction, including the date of the wire transfer, the type and amount of currency involved, the value date, the purpose and details of the wire transfer beneficiary and the beneficiary institution, and relationship between originator and beneficiary, as applicable, and in addition, apply to Record keeping requirements pursuant to §15.3.16 of the AML/CFT Act of 2021 and all CDD requirements contained in these regulations;

37.6 A Financial Institution receiving a wire transfer shall verify the identity of the beneficiary, if the identity has not been previously verified, and record this information, as per the relevant record keeping requirements.

37.7 Beneficiary institutions shall adopt risk-based internal policies, procedures and controls for identifying and handling in-coming wire transfers that are not accompanied by complete originator or beneficiary information. The incomplete originator or beneficiary information may be considered as a factor in assessing whether to execute or terminate the transaction, and in assessing whether the transaction is suspicious and merits reporting to the FIA.

37.8 Financial Institutions shall restrict or prohibit relationships or transactions with institutions that fail to meet the standards specified under this wire transfer section.

37.9 A Financial Institution Processing an Intermediary element of a wire transfer: Financial Institutions as Intermediary Financial Institutions, shall:

i. Ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it;
ii. Keep a record of all the information received from the ordering financial institution or another intermediary financial institution, for at least seven years from the day of the transaction;
iii. Take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or beneficiary information; and

37.10 Beneficiary and intermediary Financial Institutions shall adopt effective risk-based policies and procedures for determining when to execute, suspend or reject a wire transfer lacking required originator or beneficiary information; and reasonable measures and appropriate follow up actions to be taken no later than 24 hours.

37.11 For every wire transfer, Financial Institutions shall take freezing action and prohibit transactions with persons and entities designated as terrorists or with terroristic activities under any relevant United Nations Security Council Resolutions, Liberian laws and other relevant authorities;

37.12 Requirements for Domestic or cross-border wire transfers shall not apply to transfers executed as a result of credit card or debit card transactions, provided that the credit card or debit card number accompanies the transfer resulting from the transaction, nor shall they apply to transfers between financial institutions acting for their own account.

37.13 In accordance with Section 27.0 of Regulation No. CBL/RSD/2022 Concerning Regulation for the Licensing and Supervision of Money Remittance Entities, financial institutions shall submit to the Anti-money Laundering and Countering Financing of Terrorism (AML/CFT) Unit of the Central Bank of Liberia (CBL) the following returns:

a) a weekly report concerning inbound or outbound transfers;

b) monthly report of funds received for remittance but not yet remitted as well as funds received from abroad but not yet disbursed and,

c) quarterly reports consisting of a statement of total funds transferred and received from abroad.

38. IDENTIFICATION AND ACCOUNT-OPENING FOR CROSS-BORDER CORRESPONDENT RELATIONSHIPS

38.1 In addition to performing normal customer due diligence measures as contained in these regulations and the AML/CFT Act of 2021, Financial Institution shall carry out the following before entering or continuing with, cross border correspondent banking and similar relationships:

i. Gather sufficient information about the respondent institution to understand the nature of its business, and determine its reputation and the quality of supervision that it is subject to

and whether it has been investigated, subject to regulatory action or has had other action taken against it relating to money laundering or financing of terrorism;

ii. evaluate the quality of AML, CFT and CPF controls implemented by the respondent institution;

iii. obtain written approval from senior management to establish or continue a correspondent banking relationship;

iv. adopt a written agreement specifying the respective AML/CFT/CPF responsibilities of each institution; and

v. in the case of a payable-through accounts, ensure that it is possible to obtain client identity information upon request.

38.2 Financial Institutions shall apply enhanced due diligence when establishing or continuing correspondent relationship with Banks/ Financial Institutions, pertaining to high-risk countries;

38.3 Financial Institutions are prohibited from entering any business relations with correspondent banks that are shell banks, executing any transactions for or through a shell bank or permitting its accounts to be used by a shell bank. Additionally, Financial Institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

38.4 In a case where a Financial Institution is availing correspondent banking services from a Bank/ Financial Institution abroad, the CDD measures specified above shall be applied, as considered necessary to mitigate ML/TF/PF risks.

39.0 TARGETED FINANCIAL SANCTIONS AGAINST TERRORISM AND PROLIFERATION FINANCING

39.1 This Part establishes mandatory requirements for the implementation of Targeted Financial Sanctions (TFS) against terrorism, terrorist financing, proliferation financing and financing of the proliferation of weapons of mass destruction in accordance with:

i. the Anti-Money Laundering, Countering the Financing of Terrorism, Preventive Measures and Proceeds of Crime Act, 2021;

ii. the Targeted Financial Sanctions Against Terrorism Act;

iii. applicable United Nations Security Council Resolutions (UNSCRs):

a) Terrorism and Terrorist Financing: 1267, 1333, 1373, 1452, 1526, 1617, 1735, 1822, 1904, 1988, 1989, 2083, 2133, 2170, 2178, 2199, 2253, 2368, 2462 and
b) Proliferation Financing (Iran and DPRK): 1718, 1737, 1747, 1803, 1874, 1929, 2094, 2231, 2270, 2321, 2371, 2375, 2397

iv. other applicable laws of Liberia; and
v. the Financial Action Task Force (FATF) Recommendations.

39.2 **Screening Obligations**

Reporting Entities shall:

i. screen all customers, beneficial owners, authorized signatories, directors, trustees, settlors, protectors, beneficiaries, shareholders and controllers:
ii. before establishing a business relationship;
iii. before conducting an occasional transaction;
iv. before processing wire transfers;
v. before paying insurance proceeds;
vi. before processing trade finance transactions;
vii. before executing virtual asset transactions.
viii. conduct continuous screening throughout the business relationship.
ix. screen all transactions in real time.
x. screen all existing customers immediately whenever sanctions lists are updated.

39.3 **Sanctions Lists**

Reporting Entities shall screen against, at a minimum:

i. United Nations Security Council Consolidated List;
ii. Domestic Terrorist List;
iii. Domestic Proliferation List;
iv. Lists circulated by the Financial Intelligence Agency;
v. Lists circulated by the Central Bank of Liberia;
vi. any additional lists designated by competent authorities pursuant to law.

39.4 **Freezing Obligations**

Where a Reporting Entity identifies funds or assets owned or controlled directly or indirectly by a designated person or entity, it shall immediately:

i. freeze all funds and other assets;
ii. prohibit any dealing in such funds;
iii. prohibit any movement, withdrawal, transfer or disposal;
iv. prohibit making any funds available directly or indirectly;
v. prohibit providing financial services;
vi. prohibit processing transactions; and
vii. preserve all frozen assets until otherwise authorized by law.

39.5 No Prior Notice

i. A Reporting Entity shall not notify the customer or any third party before implementing a freeze.
ii. Implementation of the freeze shall not constitute tipping-off.

39.6 Reporting Requirements

a) Immediately after freezing assets, the Reporting Entity shall notify:
   i. the Financial Intelligence Agency;
   ii. any other competent authority designated by law.

b) The report shall include:
   i. customer identity;
   ii. account numbers;
   iii. amount frozen;
   iv. description of assets;
   v. transaction history;
   vi. beneficial ownership information;
   vii. supporting documentation.

39.7 False Positives

Where a sanctions screening alert is determined to be a false positive, the Reporting Entity shall:

i. document the analysis;
ii. retain evidence supporting the decision;
iii. continue monitoring;
iv. make the records available to supervisors upon request.

39.8 **Ongoing Monitoring**

Reporting Entities shall continuously monitor:

i. changes in ownership;
ii. changes in beneficial ownership;
iii. sanctions updates;
iv. new designations;
v. attempted transactions;
vi. indirect ownership;
vii. control relationships.

39.9 **Prohibition on Circumvention**

No Reporting Entity shall knowingly:

i. facilitate avoidance of sanctions;
ii. restructure transactions to evade sanctions;
iii. provide substitute services;
iv. assist designated persons through nominees;
v. provide indirect access to the financial system.

39.10 **Proliferation Financing Sanctions**

Reporting Entities shall implement targeted financial sanctions relating to proliferation financing pursuant to applicable United Nations Security Council Resolutions, including successor resolutions concerning:

i. Democratic People's Republic of Korea (DPRK);
ii. Iran; and
iii. any other jurisdiction or person designated by the United Nations Security Council.

39.11 **Internal Policies**

Every Reporting Entity shall establish written policies addressing:

i. sanctions governance;
ii. automated screening systems;
iii. escalation procedures;
iv. manual review procedures;
v. asset freezing;
vi. reporting;
vii. unfreezing;
viii. recordkeeping;
ix. staff responsibilities;
x. sanctions risk assessment.

These policies shall be approved by the Board of Directors.

39.12 **Independent Testing**

The internal audit function shall annually review the effectiveness of the sanction's compliance program including:

i. sanctions screening systems;
ii. list management;
iii. false positive management;
iv. governance;
v. reporting;
vi. freezing procedures;
vii. quality assurance.

39.13 **Recordkeeping**

Reporting Entities shall maintain for not less than seven (7) years:

i. sanctions screening results;
ii. alerts;
iii. investigations;
iv. freezing orders;
v. reports submitted to competent authorities;
vi. correspondence;
vii. audit reports.

39.14 **Staff Training**

Reporting Entities shall provide annual training covering:

i. terrorist financing;
ii. proliferation financing;
iii. sanctions screening;
iv. UNSCR obligations;
v. asset freezing;
vi. reporting obligations;
vii. typologies;
viii. sanctions evasion methods.

Training records shall be retained for supervisory review.

40. VIRTUAL ASSETS (VAs) AND VIRTUAL ASSETS SERVICE PROVIDERS (VASPs)

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

40.2 Virtual Asset Service Provider (VASP) refers to any natural or legal person that offers services related to virtual assets (digital assets like cryptocurrencies or tokens) and their transactions. Said legal or natural person 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, which involves moving virtual assets from one address or wallet to another;
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 the issuance, offering, or sale of a virtual asset (e.g., initial coin offerings).

40.3 The rise of virtual assets (VAs), including virtual currencies, has introduced innovative investment opportunities and payment infrastructures that enable new ways of creating and transferring value. However, transactions involving VAs are often anonymous and difficult to trace, making them vulnerable to misuse for money laundering, terrorism financing, and proliferation financing. Additionally, VAs is frequently traded on exchange platforms that remain unregulated in certain jurisdictions, leaving customers at risk of losing their investments if a Virtual Asset Service Provider (VASP) shuts down or ceases operations, without any regulatory safeguards in place.

40.4 Financial Institutions shall identify and assess the ML/TF/PF risks that may be associated with the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies such as virtual assets and virtual asset service providers for both new and pre-existing products.

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

40.6 Financial Institutions shall identify and assess the ML/TF/PF risks arising from virtual assets activities and the activities or operations of VASPs.

40.7 Financial Institutions should adopt a risk-based approach, tailoring their measures to prevent or mitigate money laundering, terrorism financing, and proliferation financing (ML/TF/PF) in proportion to the level of risk they identify based on their assessments.

40.8 Financial Institutions shall take adequate steps to identify natural or legal persons that carry out VASP activities without the requisite license or registration.

40.9 Financial Institutions shall submit STRs on identified VASP activities to the FIA immediately or not later than 24 hours.

40.10 Proliferation Financing (PF), as defined by the FATF, refers to the provision of funds or financial services that are, wholly or partially, used to support activities such as the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their delivery systems. This includes related materials, such as technologies and dual-use goods intended for illicit purposes, in violation of national laws or applicable international obligations.

41.0 Compliance Inspections

41.1 The Supervisory Authorities shall conduct independent and/or joint compliance inspections that include examination of documents, records, transactions, as well as internal policies and procedures to determine the effectiveness of compliance with AML/CFT/CPF and other obligations. The Supervisory Authorities shall have complete access to all documentation, data, records, transaction records, client and correspondence files to carry out such inspections. Inspections may be conducted with or without prior notice, and all information, data, and documents requested by the CBL or FIA shall be provided in a timely manner and without delay.

42. Enforcement Actions for Violation of any of the Provisions of this Regulation

42.1 The Supervisory Authorities may impose a range of enforcement actions that are effective, proportionate, and dissuasive on financial institution(s).

In determining the appropriate enforcement action, the Supervisory Authorities shall consider the nature, gravity, duration, frequency, and impact of the violation, whether the violation was intentional or negligent, the institution's compliance history, and the extent of cooperation with supervisory authorities.

The Provision of this Section 39(1&2) shall not affect or otherwise diminish the criminal, civil or other sanctions available under applicable law to Supervisors, as the case may require.

Supervisory Authorities may impose one or more of the following measures:

i. Written warning, reprimand, or directive requiring specified corrective action within a prescribed period;
ii. Administrative monetary penalties in accordance with the approved CBL and FIA Monetary Sanctioning Regime for Non-Compliance with AML/CFT Requirements for Financial Institutions, including additional penalties for continuing violations;
iii. Civil penalties and enforcement measures as provided by law;
iv. Restrictions on, or suspension of, specific products, services, business activities, transactions, branches, or operations until identified deficiencies are remedied;
v. Suspension, removal, disqualification, or prohibition of any director, officer, manager, compliance officer, employee, or other responsible person from holding office or performing specified functions within a financial institution;
vi. Revocation, suspension, or restriction of any license, authorization, registration, or approval granted to the financial institution; and
vii. Any other supervisory, remedial, or enforcement measure authorized under applicable laws and regulations.

All enforcement actions under these Regulations shall not preclude the referral of any matter to law enforcement authorities for investigation or prosecution where there is evidence of money laundering, terrorist financing, proliferation financing, or any other criminal offence. Supervisory Authority shall have the authority and/or obligation to publish their enforcement actions.

42.2 See the approved Central Bank of Liberia's Anti-Money Laundering & Countering the Financing of Terrorism Sanctioning Regime Framework for Non-Compliance with AML/CFT Requirements for Financial Institution

43. Judicial Review

All persons or Institutions, who have been subjected to any of the range of enforcement actions, including the imposition of sanction(s) such as administrative/monetary sanctions as contained in this regulation and/or the AML/CFT Act of 2021, may file a petition for a judicial review to a Court of Competent Jurisdiction(s) in accordance with the laws of Liberia.
All Petition(s) must be filed within 10 calendar days as of the date of the imposition of the sanction(s). Any failure to file Judicial Review within the timeline provided herein shall amount to a forfeiture of said rights.

44. Effective Date

This Regulation takes immediate effect as at the date of its issuance and shall remain in force until otherwise advised by the National AML/CFT Inter-Ministerial Committee of Liberia..

Issued this day of----, A.D. 20 in the City of Monrovia, Republic of Liberia.

45.0 Annex:

45.1: Minimum Identification Documents to be obtained for Specific Customers (in addition to the CDD requirements in these regulations)

No.	Customer Type	Minimum Documentations/Information to be obtained
1.	Salaried Accounts	Obtain and verify: i. the employment information including: Employment letter or contract; ii. Employer name, address and contact details iii. Salary slips or evidence Of salary deposit pattern iv. Determine other sources of funds or wealth for high-risk customers Enhanced due diligence should apply when: v. The customer is a Politically Exposed Person, Senior Public Official or High-ranking employee of a state-owned enterprise

		vi. The account receives offshore or irregular salary payments vii. the salary deposits do not match the declared employment profile
2.	Students	i. Admission Letter ii. Student ID Card iii. Proof of Residence
	Joint Account	i. Copy of applicable valid identity document for each joint account holder; ii. CDD measures on all of the joint account holders shall be performed as if each of them is individual customer
3.	Sole Proprietorship	i. Copy of the applicable valid identity document; ii. Business registration iii. TIN iv. Declaration of sole proprietorship on business letterhead v. Account opening requisition on business letterhead
4.	Small Businesses and Professions	i. Copy of applicable valid identify documentation of the account holder/s ii. Business registration iii. TIN iv. Certificate or proof of membership of the trade bodies, etc. wherever applicable v. Proof of source of funds/income
5.	Partnership	i. Copy of the applicable valid identity document of all partners and authorized signatories ii. Attested copy of 'Partnership Deed' duly signed by all partners of the firm iii. Business registration certificate iv. Authorization letter
6.	Corporate Company	The identity of a corporate company shall comprise of: i. Registered corporate name and any trading names used; ii. Registered address and any separate principal trading addresses; iii. Directors, owners, shareholders iv. The nature of the company's business v. Tax Identification Number (TIN) etc.
7.	Public Registered companies/ customers listed on stock exchange	i. The Board Resolution or other authority for a representative to act on behalf of the company ii. Phone calls may be made to the CEO of the company to intimate him of the application to open

		the companies' account, in a case where the principal owners, controllers or signatories need to be identified; iii. The identity of the directors of a quoted company may be verified iv. Due diligence shall be conducted where the account or service falls within the category of higher risk business
8.	Private Companies (where the applicant is an unquoted company and none of the principal directors or shareholders already have an account with the FI)	i. Certificate of incorporation or registration, evidence of the company's registered address and the list of shareholders, directors or signatories; ii. Obtain information on the company through a third party or available and credible public sources and make reasonable attempts to verify.
9.	Higher Risk Business Applicant (any business relationship where third party funding and transactions are permitted or where a high-risk business applicant is seeking to enter a full banking relationship)	i. For established companies that are incorporated for 18 months or more, a set of the latest report and audited accounts shall be produced; ii. Enquiry of the business through available sources that are credible; iii. A certified copy of the resolution of the Board of Directors addressed to the financial institution to open an account with clear instructions about the signatories; iv. The memorandum and articles of association of the company; and v. Any other document that the financial institution shall deem necessary including evidence of source of funds
10.	Higher risk business relating to private companies	i. Identification evidence shall be obtained for the principal beneficial owner of the company and any other person with principal control over the company's assets; ii. Verify the identity of the beneficial owner or settlors; iii. Where the principal beneficial owners or controllers have changed, FIs are required to verify the identities of the new owners; iv. Identify directors who are not principal controllers and signatories to an account; v. Visit the place of business to confirm the existence of such business premises and the nature of the business conducted;

		vi. Where changes are observed in the nature of the business transacted or the profile of payment, FIs are to make further checks to establish the cause; vii. Periodic enquiries shall be made to establish changes to controllers, shareholders or the original nature of the business or activity. viii. Specific KYC/CDD attention shall be given to international business companies registered in an offshore jurisdiction and operation out of a different jurisdiction
11.	Foreign Financial Institutions	FIs shall obtain and verify the existence and regulated status by: a) Checking with the home country's central bank or relevant supervisory body; b) Checking with another office, subsidiary, branch or correspondent bank in the same country; c) Obtaining evidence of its license or authorization to conduct financial and banking business from the institution itself; d) Additional information on banks all over the world may be obtained from various international publications and directories or any of the international business information services such as Swift KYC registry, etc.
12.	Designated Non-Financial Businesses and Professions (DNFBPs)	FI's shall obtain the following, in addition to the CDD requirements: i. Certificate of registration; ii. Constitution; iii. Identity of signatories and verify new ones if there is a modification;
13.	MVTS Operators	i. In addition to the CDD requirements stated in these regulations, said customers shall submit valid licenses to the financial institutions before establishing business relationships
14.	NGOs/NPOs/Charities	Identify and verify the identity of: i. the institution ii. members of the governing body or committee iii. President iv. Board members v. Treasurer vi. All signatories vii. Certified copies of all registration documents/certificate of incorporation; memorandum & article of association

		viii. Obtain and confirm the name and address of the organization (in the case of a registered charity) ix. Information on Donors if that's the stated source of funds
15.	Trust, Clubs, Societies and Associations etc.	i. Copy of applicable valid identity document of: a) All members of governing body/Board of Directors/Trustees/Executive committee b) All signatories c) Settlor, the trustee, the protector (if any) and the beneficiaries; ii. Declaration from Governing Body/Board of Trustees/ Executive committee/ purpose and source of funds etc. iii. Certified copies of the following: a) Business registration/instrument of Trust b) By-laws/Rules & regulations c) Resolution/any documentation that captures the governing body/board of trustees/executive committee, if it is the ultimate governing body authorizing any person(s) to open and operate the account
16.	Minor Accounts	i. Birth certificate ii. Passport photo of the minor iii. Obtain and verify the identification and home address of the parent or guardian of a minor
17.	Embassies, Consulates, career and established members of embassies, high commissions, other diplomatic and expatriate officials (such as UN, African union, etc.)	i. Applicant's letter of request (showing official position or status and duration of stay in host country); ii. Letter of introduction from the relevant Diplomatic mission or international organization; iii. Relevant pages of the applicant's international passport.
18.	Non-Resident Accounts/ Overseas correspondence, examination bodies, foreign companies executing approved contracts in Liberia, foreign professional bodies	A. For overseas correspondence and other examination bodies: i. Letters of request from applicant; ii. Memorandum and articles of the overseas company; iii. Letter of accreditation; B. For Foreign companies executing approved contracts: i. Contract agreement/document; ii. Applicant's letter of request

		iii. Memorandum and articles of association of the company. C. For foreign Professional bodies i. Applicant's letter of request ii. Memorandum and articles of the overseas iii. Letter of accreditation from the ministry of education; iv. Power of attorney to the agent in Liberia; FI's shall do the following for all listed customers at minimum: v. Obtain and verify identification directly form the customer's embassy or reputable FI in the applicant's home country or country of residence; vi. Obtain and verify an applicant's permanent residential address which shall be notarized; vii. All Non-resident accounts in the above category shall on completion of the contract be closed and the balance, if any, transferred to the customer's account in country of residence, after provision of proper documentation.
19.	Non-Resident Liberians	i. Name, date of birth ii. Permanent residential address (in host country) directly through a reputable financial institution Validate sources of funds via work ID's, pay slips or bank statements
20.	Foreigners/ Resident non-Liberians	i. Obtain and verify the valid Resident Permit on non-Liberians; ii. A recently arrived foreigner shall provide permanent home address

Annex 45.2 A Non-Exhaustive List of Domestic PEP

A non-exhaustive list of persons performing prominent public function for which domestic PEP designation is a must:

I. Legislature
   a. Members of the House of Representatives
   b. Members of the Senate
   c. Secretary of the Senate
   d. Chief Clerk of the House of Representatives
   e. Comptrollers, Procurement Officers, Departmental Directors, Project Managers.

II. Judiciary
   a. Chief Justice and Associate Justices of the Supreme Court

b. Judges of Circuit Courts and circuit-level specialized courts
c. Stipendiary and Associate Magistrates
d. Court Administrator
e. Comptrollers, Procurement Officers, Departmental Directors, Project Managers.

III. Executive
   a. President of Liberia
   b. Vice President of Liberia
   c. Cabinet Ministers, Deputy Ministers and Assistant Ministers, Comptrollers,
      Procurement Officers, Departmental Directors, Project Managers
   d. Members of the Board of Directors, Head, Deputy Head, and Department Head of Autonomous Agency
   e. Head, Deputy Head, and Department Head of State-Owned Enterprises
   f. Chairpersons, Commissioner, Deputy Heads, and Department Heads of Independent Commissions
   g. Ambassador-At-Large, Ambassador, Consul General, Consular Officer; Head,
      Deputy Head, Department Head of foreign mission, institution and organization
   h. Head, Deputy, Department Head and Top-ranking officers (from the rank of Captain where applicable) of Law Enforcement and Investigation Agencies including but not limited to Liberia National Police, Liberia Immigration Service, Liberia Drug Enforcement Agency, National Security Agency, etc.
   i. Chief of Staff, Deputy Chief of Staff and Officers of the Armed Forces of Liberia (AFL)
   j. Custom Officers of the Liberia Revenue Authority

Annex 45.3 A Non-Exhaustive List of Foreign PEP

A non-exhaustive list of persons performing prominent public function for which foreign PEP designation is a must:

I. Ambassador-At-Large, Ambassador, Consul General, Consular Officer, Economic Officer of foreign mission
II. Head, Deputy Head, Department Head of multi-national, bilateral and regional institution and organization
III. Head, Deputy Head, Department Head of United Nations, United Nations Agencies, United Nations Missions, international relief agencies, international non-profit or non- governmental organizations