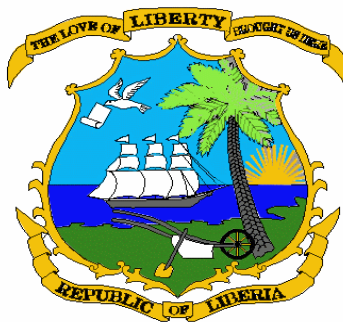


THE



LIBERIA

OFFICIAL

GAZETTE
PUBLISHED BY AUTHORITY

VOL. XVI.

Friday, May 10, 2017

NO.25

EXTRAORDINARY

The Government of the Republic of Liberia announces that the Central Bank of Liberia (CBL), pursuant to its mandate under the Central Bank of Liberia Act of 1999 and its authority under the Financial Institutions Act of 1999, and specifically consistent with Section 55 of the said Central Bank of Liberia Act of 1999 and Section 39 of the Financial Institutions Act of 1999, has issued on May 10, 2017, its Regulations No. CBL/RSD/002/2017 revising Regulations No. CBL/RSD/004/2013 herein under:

**CONCERNING AML/CFT REGULATIONS FOR FINANCIAL
INSTITUTIONS IN LIBERIA**

BY ORDER OF THE PRESIDENT

MARJON V. KAMARA
MINISTER OF FOREIGN AFFAIRS

MINISTRY OF FOREIGN AFFAIRS
MONROVIA, LIBERIA
May 10, 2017

1.0 Introduction and Definitions

This regulation implements internal control requirements which are mandatory for financial institutions (as defined by §1 of the Anti-Money Laundering and Terrorist Financing Act of 2012), pursuant to that law as well as § 4(5) of the Central Bank of Liberia Act (CBL Act) and § 39 of the New Financial Institutions Act of 1999 (New FIA). This Regulation replaces the previous AML/CFT Regulation No. CBL/RSD/004/2013.

- 1.1 This regulation requires financial institutions to adopt and fully implement effective internal AML/CFT control policies and procedures applicable to all customers, products, services, business lines, branches and subsidiaries.
- 1.3 In these regulations the following definitions apply:
 - 1.3.1 **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.
 - 1.3.2 **Express trust** means a 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.
 - 1.3.3 **Payable-through accounts** means correspondent accounts that are used directly by third parties to transact business on their own behalf.
 - 1.3.4 **Politically Exposed Person (PEP):**
 - i. **domestic or foreign PEPs** are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, or important political party officials; or

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

1.3.5 **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 meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.

2.0 AML/CFT Internal Control Obligations for Financial Institutions

2.1 All licensed financial institutions shall adopt and implement written internal AML/CFT policies and procedures to ensure effective compliance with the obligations to report suspicious transactions of any amount, as well as cash transactions (equal to or above the designated threshold amount specified in regulation of the financial intelligence unit "FIU") pursuant to §67.5(2) and (3) of the Act to Establish the Financial Intelligence Unit of Liberia (2012).

2.2 The written internal AML/CFT policies and procedures shall specify detailed reporting procedures in accordance with regulations issued by the FIU, as well as all internal AML/CFT policies and procedures to enable all staff to effectively identify transactions that may be suspicious for money laundering or terrorist financing, pursuant to the Anti-Money Laundering and Terrorist Financing Act of 2012.

2.3 The internal AML/CFT policies and procedures shall:

- cover all AML/CFT obligations stated in this regulation and other relevant laws and regulations
- be approved (signed off/dated) by Senior Management
- distributed to all staff
- specify in detail policies, procedures and obligations of all staff to fully implement AML/CFT preventive measures

- cover all customers/clients, products, services, transactions, business lines, branches and subsidiaries
- be made available for inspection by the Central Bank of Liberia (CBL) or the Financial Intelligence Unit (FIU), upon request.

2.4 Compliance with Obligations by Foreign Subsidiaries and Branches:

2.4.1 Financial institutions shall require their foreign branches and majority-owned subsidiaries to implement the customer identity, customer due diligence and internal control requirements to the extent that domestic applicable laws and regulations of the host country so permit.

2.4.2 If the laws of the country where the branch or majority-owned subsidiary is situated prevent compliance with these obligations, for any reason, the financial institution shall so advise its competent supervisory authority, which may take such steps as it believes to be appropriate to accomplish the purposes of this Regulation.

2.5 Prohibition against relations with shell banks: Establishment of any business relations or executing any transactions with a shell bank are absolutely prohibited.

2.6 Prohibition against anonymous accounts: Opening, establishing or maintaining anonymous accounts are absolutely prohibited. Any anonymous accounts which existed prior to enactment of the AML/CFT and FIU Acts of 2012 shall be closed or subject to effective and thorough CDD/KYC procedures and AML/CFT risk assessment.

2.7 Recordkeeping Obligations

2.7.1 Financial institutions shall maintain all transaction records for a minimum of 5 years from the date the transaction was executed.

2.7.2 Financial institutions shall maintain CDD/KYC documents, records, correspondence and files for 5 years from the date of termination of the relationship with the customer.

2.8 AML/CFT Compliance Officer, training and integrity: Financial institutions shall:

2.8.1 Designate a compliance officer at management level to be responsible for the implementation of, and ongoing compliance with AML/CFT obligations of the financial institution. The AML/CFT compliance officer shall have ready access to all books and records of the institution.

2.8.2 Provide AML/CFT training to all employees on an annual basis, and shall maintain copies of, and make available to the CBL upon request, all training attendance records, training programs and materials for inspection by the CBL;

2.8.3 Implement internal audit arrangements to review and monitor effectiveness of AML/CFT policies, procedures, systems and compliance, as well as initiate corrective actions where compliance deficiencies are identified.

2.9 AML/CFT Risk Assessment of new products, services and technologies

2.9.1 Financial institutions shall conduct AML/CFT risk assessments of all products and services that utilize new technologies which give rise to increase money laundering or terrorist financing risks, particularly where accounts can be established or transactions can be executed in a non-face-to-face manner.

2.9.2 The AML/CFT risk assessments of these products and services shall clearly identify all ML/TF risks, and set forth effective procedures to mitigate them. The procedures to mitigate the ML/TF risks shall be fully implemented and integrated into the internal AML/CFT control policies and procedures shall be updated to include them.

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

3.1 Customer Identity Requirements

3.1.1 Financial institutions shall obtain and maintain documentary records for each client or customer to

verify by reliable and independent source documents (such as a passport, a driver's license, or national identification documents):

- Identity(full name) of the person
- date and place of birth
- address
- contact details (ie., phone, cellphone, email, etc)

3.1.2 The identity records must also be obtained and maintained on all persons acting on behalf of a customer, together with documentation that proves that the person is legally authorized to act in a representative capacity.

3.1.3 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 FIU Acts of 2012. 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.

3.1.4 For legal entities, financial institutions shall obtain and maintain documentary records including:

- 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
- 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, and any additional information and documents necessary to understand the ownership and control of the legal person.

3.1.5 For other contractual legal arrangements (ie., other than recognized legal entities), financial institutions shall obtain and maintain documentary records including the name of all trustees, settlers, and

beneficiaries of express trusts, and other parties with authority to manage, vary or otherwise control the arrangement.

3.1.6 Where there is any suspicion or doubt about the validity of any official identity documentation provided by the customer, the financial institution shall take steps to verify the validity of the documentation with the issuing agency.

3.1.7 Customer identity documentation must be obtained:

- before opening any account for or otherwise establishing a business relationship with a customer (except customers existing before this regulation became effective in which case such documents must be obtained within 1 year of effectiveness of this regulation);
- when carrying out transactions for occasional or walk-in (non-account holder) customers
- when any doubts exist about information proved by an account holder, including the veracity or adequacy of information; or
- there is a suspicion of money laundering or financing of terrorism involving the customer or the customer's account.

3.2 Customers not Physically Present: Financial institutions shall take adequate measures to address the specific ML/TF risks where a customer is not physically present for purposes of identification. 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.

3.3 Beneficial Owner Requirements: Financial institutions shall identify the natural persons who are beneficial owners of legal entities and or natural persons. Where it is not possible to identify them with certainty, the financial institution shall make a responsible determination as to whether to open or continue the account, or classify the account as a high risk account.

3.4 Know Your Customer (KYC) - understanding 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.

3.5 Risk classification

3.5.1 Financial institutions shall classify all client accounts and business relationships with respect to level of risk and perform on-going and enhanced due diligence procedures in accordance with the risk classification.

3.5.2 At minimum, high risk clients must be classified as such and appropriate enhanced due diligence procedures shall be applied and appropriately documented. All clients in high risk categories identified in this Regulation as well as subsequent regulations of the CBL or FIU shall be classified as high risk.

3.5.3 Financial institutions shall additionally classify other clients or accounts as high risk where higher risk designation is appropriate.

3.5.4 New customers: Financial institutions shall implement effective procedures to ensure all new clients are classified by risk level before account opening or executing of transactions.

3.5.5 Clients that established accounts prior to enactment of the AML and FIU acts shall be risk classified no later than 1 year from the date of effectiveness of this regulation.

3.6 High Risk Accounts

3.6.1 Financial institutions shall have appropriate risk management systems to identify customers whose activities may pose a high risk of money laundering and financing of terrorism and shall exercise

enhanced due diligence procedures in respect of such customers.

3.6.2 Client accounts that shall be mandatorily classified as high risk in all cases are:

- casinos
- Politically Exposed Persons (PEPs)
- Any other categories of customers, or customers/transactions connected with countries, products and/or services that the CBL or FIU designate as high risk.

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

- obtaining additional documentation concerning customer identity, verification, purpose of the account and nature of transactions, transaction profile and additional documentation to satisfy the financial institution that it understands the sources of funds involved in transactions and in the account;
- conducting period monitoring of transactions and transaction patterns in the account; and
- documenting the enhanced due diligence procedures applied to the account.

3.8 Additional procedures for PEP accounts: Financial institutions shall:

- Determine whether any clients or beneficial owners are PEPs at account opening, or whether existing clients have become PEPs;
- obtain senior management approval in writing prior to opening an account of a PEP;
- obtain senior management approval in writing to maintain an account of a client that has become a PEP; and
- take all reasonable measures to identify the source of wealth and funds and other assets of the PEP.

3.9 On-going Customer Due Diligence: Financial institutions shall conduct ongoing due diligence with respect to all client relationships which shall include:

- maintaining current information and records relating to the customer and beneficial owner (not older than 2 years);
- ensuring transactions are consistent with documentary evidence provided by the client concerning the purpose and nature of the account, financial activities and risk profile.
- paying 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
- paying 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.

3.10 Wire transfers

- 3.10.1 When executing wire transfers equal to or above 1,000 US dollars or the equivalent in Liberian dollars, financial institutions shall:
- identify and verify the identity of the originator;
 - obtain and maintain the account number of the originator or (in absence of an account number) a unique reference number;
 - obtain and maintain the originator's address or (in the absence of address) the national identity number or date and place of birth; and
 - include the above information in the message or payment form accompanying the transfer.
- 3.10.2 When a financial institution is an intermediary in a chain of payments, all information received with the wire transfer must be re-transmitted.
- 3.10.3 If an institution receives wire transfers that does not contain the complete originator information, they shall take measures to obtain and verify the missing information from the ordering institution

or the beneficiary, or refuse to execute the transfer and report the transaction to the FIU.

3.11 Correspondent Banks

3.11.1 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.

3.11.2 In respect of all correspondent banking relationships, financial institutions shall:

- identify and verify the ownership structure of the correspondent bank;
- collect information on the nature of the institution's banking and other business activities;
- evaluate the institution's reputation and quality of supervision to which it is subject;
- obtain written approval from senior management to establish or continue a correspondent banking relationship;
- evaluate the AML/CFT controls implemented by the institution;
- adopt a written agreement specifying the respective AML/CFT responsibilities of each institution; and
- in the case of a payable-through accounts, ensure that it is possible to obtain client identity information upon request.

3.12 Inability to Fulfill Customer Identification or Know Your Customer Obligations: A financial institution that cannot fulfill the customer identity and due diligence requirements with respect to any customer shall not establish an account for or maintain any business relationship with that customer. Where appropriate, it shall make a report to the CBL and the FIU in accordance with this regulation.

4.0 Compliance Inspections

The CBL or the FIU shall conduct compliance inspections that include examination of documents, records, transactions, as well as internal policies and procedures to determine effectiveness of compliance with AML/CFT and other obligations. The CBL and FIU

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, documents requested by the CBL or FIU shall be provided in a timely manner and without delay.

5.0 Sanctions for Violation of any of the Provisions of this Regulation

The CBL may impose a range of administrative sanctions upon any financial institution as an entity as well as individual persons who violate any provisions of this Regulation. These may include:

- Warning letter;
- CBL Order to take specified corrective action;
- Administrative penalties, including monetary penalties of up to L\$1 million;
- Civil penalties;
- Order to remove employee, officer, director or manager from position in the financial institution;
- Full or partial suspension of financial activities until the violation or deficiency is rectified; and/or
- Permanent revocation of financial license.

6.0 Effective Date

This Regulation takes immediate effect as at the date of its issuance and shall remain in force until otherwise advised by the CBL.

Issued this 10th day of May, A.D. 2017 in the City of Monrovia, Republic of Liberia.