GAZETTE OF ERITREAN LAWS

PUBLISHED BY THE GOVERNMENT OF ERITREA

Vol. 22/2014 No. 1 Asmara, September 8, 2014 Price: 15.00 Nakfa

\

PROCLAMATION NO. 175/2014

The Anti-Money Laundering and Combating Financing of Terrorism Proclamation

PROCLAMATION NO. 175/2014

The Anti-Money Laundering and Combating Financing of Terrorism Proclamation

WHEREAS, money laundering and the financing of terrorism are serious crimes which threaten the peace, security and development of the country and the world at large;

WHEREAS, the Government of Eritrea is committed to protect the well-being of its citizens from terrorism and guarantee their safety in their day-to-day activities;

WHEREAS, it is necessary to ensure that all financial institutions in the country are in the forefront in combating money laundering and terrorism financing; and

NOW, THEREFORE, it is proclaimed as follows:

PART I

PRELIMINARY PROVISIONS

Article 1. Short Title

This Proclamation may be cited as "Anti-Money Laundering and Combating Financing of Terrorism Proclamation No. 175/2014."

Article 2. Definitions

(1) In this Proclamation, unless the context otherwise requires:

(1) **"Bank"** means the Bank of Eritrea, which is the central bank of Eritrea as defined in Proclamation No. 93 of 1997;

(2) **"Beneficial Owner"** refers to the natural person who ultimately owns or controls a customer or account, the person on whose behalf a transaction is being conducted, or the person who ultimately exercises effective control over a legal person or arrangement;

(3) **"Competent Authority"** means any physical person or government body which has a delegated or vested authority, capacity, or power to perform a designated function;

(4) **"Correspondent Banking"** means the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank);

(5) **"Cross-Border Transfer"** means any transfer where the originator and beneficiary persons are located in different countries at the time of initiating the transfer. The term also refers to any chain of transfers that has at least one cross-border element;

(6) **"Customer"** in relation to a transaction or account, includes:

(a) a person in whose name a transaction or account is arranged, opened or undertaken;

(b) a signatory to a transaction or account;

(c) any person to whom a transaction has been assigned or transferred; or

(d) any person who is authorized to conduct a transaction;

(7) **"Domestic Transfer"** means any transfer where the originator and beneficiary persons are located within the same country at the time of initiating the transfer. The term refers to any chain of transfers that takes place entirely within the borders of a single country, even though the system used to effect the transfer may be located in another country;

(8) **"Depository Institution"** means any financial institution authorized to engage in the business of collecting deposits or their equivalents from the public;

(9) **"Financial Institution"** means both any authorized depository and non-depository financial institution;

(10) **"Financing of Terrorism "** means an act by any person who, by any means, directly or indirectly, willfully, provides or collects funds, or attempts to do so, with the knowledge and intention that they would be used in full or in part to carry out a terrorist act by a terrorist or terrorist organization;

(11) **"Freezing"** means prohibiting the transfer, conversion, disposition or movement of funds or other property on the basis of, and for the duration of the validity of, a decision of a judicial or other competent authority. The frozen funds or other property shall remain the property of the persons or entities that held an interest in the specified funds or other property at the time of the freezing, and may continue to be administered by the financial institution;

(12) **"High Risk Categories"** means customers, businesses or transactions that need to be subjected to more regular reviews, particularly against the know-your-customer information held by the bank and the activity in the account. Such categories shall include, but not be limited to:

(a) complex, unusual or large transactions;

(b) relationships or transactions with countries known to have material deficiencies in anti money laundering and terrorist financing strategies;

(c) politically exposed persons;

(d) non-resident customers such as those staying in the country for less than one year or those in short visit or travel; and

(e) companies that have shares in bearer form;

(13) **"Large Cash Transaction"** means a transaction exceeding USD 10,000 or its equivalent in other convertible currencies;

(14) **"Money Laundering"** means the offence provided for in Article 31 of this Proclamation;

(15) **"Money or Value Transfer Service"** shall mean carrying on the business of accepting cash, cheques or any other monetary instrument or other means of storing value, and paying a corresponding sum in cash or in other form to a beneficiary, by means of communication, message, transfer or through a clearing system to which the money or value transfer service belongs;

(16) **"Non-Depository Financial Institution (NDFI)"** means any authorized financial institution which does not collect deposits or their equivalent from the public;

(17) **"Non-Depository Financial Institution Public's Funds (NDFIPF)"** means any authorized financial institution which does not collect deposits or their equivalent from the public, but which does collect funds from the public in some form for its operations, and

which is of a specialized nature and includes insurance companies, pension funds, investment funds as well as others which may be designated by the Bank;

(18) **"Non-Depository Financial Institution Non-Public's Funds (NDFINPF)"** means any authorized financial institution which does not collect deposits or their equivalent from the public and does not collect funds from the public in any form, and engages in one or more specialized financial activities, foreign exchange dealership, factoring and leasing companies, venture capital firms, credit card companies, installment credit and consumer credit institutions, security companies (such as brokers, dealers, investment analyst, investment fund management, investment advisors, underwriters and investment bankers), stocks (shares) and bond exchanges and clearing, settlement and depository institutions, trustees, custodians, and any other which may be designated as NDFINPF by the Bank;

(19) **"Non-Face-to-Face Customers"** are customers who do not present themselves for personal interview when they open accounts with financial institutions such as non-resident customers;

(20) **"Originator"** is a bank account holder or, where there is no account, the person that places an order with the bank or other financial institution to perform a transfer;

(21) **"Payable-Through Accounts"** refers to correspondent accounts that are used directly by third parties to transact business on their own behalf;

(22) **"Person"** means any natural or juridical person;

(23) **"Politically exposed person"** shall mean any person who is or has been entrusted with prominent public functions as well as members of such person's family or those closely associated with him/her.

(24) **"Predicate Offence"** shall mean any offence, which generates proceeds of crime and is punishable with rigorous imprisonment;

(25) **"property"** shall mean assets or funds of every kind, whether movable or immovable, tangible or intangible, and legal documents or instruments in any form, including electronic or digital, evidencing title to or interest in such assets, including but not limited to bank credits, traveler's cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit, and any interest, dividends or other income on or value accruing from or generated by such assets;

(26) **"Proceeds of Crime"** means any property derived or obtained, directly or indirectly, from an offence under Articles 31 and 32 of this Proclamation and includes property converted or transformed, in part or in full, into other property and investment yields from such an offence;

(27) **"Seizing"** means prohibiting the transfer, conversion, disposition or movement of funds or other property on the basis of, and for the duration of the validity of, a decision of a judicial or other competent authority. The seized property shall remain the property of the persons or entities that held an interest in the specified property at the time of the seizure, but shall be administered by the judicial or other competent authority;

(28) **"Senior Management"** means a team of executives at the highest level who have the day-to-day responsibilities of managing a financial institution as defined by the instruments establishing it;

(29) **"Shell Bank"** means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision;

(30) **"Supervisory Authority"** means the Bank which is entrusted with the oversight authority of all financial institutions;

(31) **"Suspicious Transaction"** refers to a transaction which is inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account, or a complex and unusual transaction or pattern of transaction that has no apparent or visible economic purpose;

(32) **"Terrorist Act'** means shall mean an act intended to cause death or serious bodily injury to a civilian, or any other person not taking an active part in the hostilities in a situation of armed conflict, to commit kidnapping or hostage taking, cause serious damage to property, cause serious risk to the safety and health of the public, cause damage to the natural resources, environment, historical or cultural heritage, or to endanger, seize or put under control, cause serious interference or disruption of any public service when the purpose of such act, by its nature or context, is to intimidate a population or to compel a government or an international organization to do or to abstain from doing so;

(33) **"Terrorist"** shall mean any natural person who:

(a) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully;

(b) participates as an accomplice in terrorist acts;

(c) organizes or directs others to commit terrorist acts; or

(d) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act;

(34) **"Terrorist Organization"** shall mean any group of terrorists that:

(a) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully;

(b) participates as an accomplice in terrorist acts;

(c) organizes or directs others to commit terrorist acts; or

(d) contributes to the commission of terrorist acts by group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

(35) **"Transaction with No Apparent or Visible Economic Purpose"** includes:

(a) a transaction that gives rise to a reasonable suspicion that it may involve the laundering of money or the proceeds of any crime and is made in circumstances of unusual or unjustified complexity;

(b) a transaction whose form suggests that it might be intended for an illegal purpose or the economic purpose of which is not discernible;

(c) a customer relationship with the financial institution that does not appear to make economic sense, such as a customer having a large number of accounts with the same bank, frequent transfers between different accounts or exaggeratedly high liquidity;
(d) a transaction in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish plausible reason for immediate withdrawal;
(e) a transaction that cannot be reconciled with the usual activities of the clientele of the financial institution or branch office in question, and in which the reason for the customer's choice of that particular financial institution or branch cannot be ascertained;
(f) a transaction which, without plausible reason, results in the intensive use of what was previously a relatively inactive account, such as a customer's account which shows virtually no normal personal or business related activities but is used to receive or disburse unusually large sums which have no obvious purpose or relationship to the customer or his or her business; or
(g) a transaction which is incompatible with the financial institution's knowledge and experience of the customer in question or with the purpose of the business relationship;

(36) **"Wire Transfer"** refers to any transaction carried out on behalf of an originator through a bank or other financial institution by electronic means with a view to making an amount of money available to a beneficiary at another bank or financial institution. The originator and the beneficiary may be the same person; and

(2) Any expression in the masculine gender shall also include the feminine.

Article 3. Objectives

The objectives of this Proclamation are to:

(a) detect, deter and prosecute offences of money laundering and the financing of terrorism;
(b) maintain public confidence in the financial system;
(c) facilitate co-operation among reporting entities, Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) supervisors, and various government agencies, in particular law enforcement and regulatory agencies; and
(d) sensitize financial institutions to establish and maintain policies and procedures to guard against money laundering and the financing of terrorism.

Article 4. Scope of Application

This Proclamation applies to all financial institutions in Eritrea.

PART II

CUSTOMER DUE DILIGENCNE AND IDENTIFICATION

Section I. Customer Due Diligence of Financial Institutions

Article 5. Customer Acceptance Policy, Procedure, and Compliance Arrangement

(1) Financial Institutions shall establish and maintain internal policies, procedures, and controls to prevent money laundering and terrorist financing, and communicate the same to their employees and the Bank. The said policies, procedures and controls shall at a minimum cover:

(a) explicit criteria for identification and acceptance of customers;
(b) appropriate risk management systems to determine whether a potential customer, an existing customer or beneficial owner is a politically- exposed person or a customer in a high risk category;
(c) record retention techniques, methods and periods;
(d) unusual and suspicious transactions detection techniques, methods and reporting obligations;
(e) measures to be taken to prevent the misuse of technology for the purposes of money laundering or terrorist financing schemes; and
(f) specific risks associated with non-face-to-face business relationships or transactions.

(2) Financial institutions shall develop appropriate compliance management arrangements which at a minimum include:

(a) designation of a compliance officer at the management level; and
(b) ascertain application of all laws related to anti-money laundering and combating terrorist financing: as well as internal policies, procedures and controls when establishing customer relationships and conducting ongoing due diligence.

(3) Financial institutions shall maintain an adequately-resourced and independent internal audit function to test compliance with laws and directives of the Bank, as well as internal policies, procedures and controls.

\Article 6. Customer Identification and Due Diligence

(1) Financial institutions may not keep anonymous accounts or accounts in fictitious ~~names~~ (names)

(2) Financial institutions may not enter into, or continue, correspondent banking relationships with shell banks.

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

(a) establishing business relations with a customer;
(b) carrying out occasional cash transaction with a customer exceeding USD 10,000 or its equivalent in other currencies, and shall include situations where

the transaction is carried out in a single operation or in several operations that appear to be linked or structured;

(c) there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or thresholds provided under this Proclamation; and

(d) they have doubts about the veracity or adequacy of previously-obtained customer identification data.

(4) Financial institutions shall identify the customer, whether regular or occasional, natural or juridical person or legal arrangement, and verify that customer's identity using, as much as possible, reliable independent source documents, data or information.

(5) Identification requirements for natural persons shall include:

(a) given or legal name and all other names used;
(b) identity card or residence permit or passport;
(c) permanent address;
(d) telephone number, fax number, mailing and e-mail address, if available;
(e) date and place of birth;
(f) nationality;
(g) occupation, public position held and/or name of employer, if any;
(h) type of account; and
(i) signed statement certifying accuracy of the information provided.

(6) For customers that are juridical persons or legal arrangements, financial institutions shall:

(a) take reasonable measures to understand the ownership and control structure of the customer and determine who the natural persons that ultimately own or control the juridical person or arrangement are, including those natural persons who exercise ultimate effective control over the juridical person or arrangement;

(b) verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person;

(c) verify the legal status of the juridical person or legal arrangement at a minimum by obtaining proof of incorporation or similar evidence of establishment or existence. Information concerning the juridical person or legal arrangement's shall include:

(i) name;

(ii) legal form;

(iii) some form of official identification number such as tax identification number, if available;

(iv) address which includes country, region/city/town/zonal administration in which the head office is located and, if available, house number, mailing address, telephone number and fax number;

(v) names of the general manager or chief executive officer and of directors, if applicable;

(vi) provisions regulating the power to bind the juridical person or arrangement;

(vii) the resolution of the board of directors, if applicable, or any other authorized body or person that authorizes to open an account; and

(viii) identification of those who have authority to operate the accounts.

(7) In carrying out transactions with any person, a financial institution shall identify the ultimate beneficial owner and take reasonable measures to verify the identity of the beneficial owner using relevant information or data obtained from a reliable source such that the financial institution is satisfied that it knows who the beneficial owner is. A financial institution shall, for all its customers, determine whether the customer is acting on his own behalf or on behalf of another person and, if the customer is found to be another person, it shall take reasonable steps to obtain sufficient identification data to verify the identity of that other person.

(8) Establishment of a financial institution's new business relationship with a politically-exposed person shall be approved by a senior management member of the financial institution.

(9) Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes, a politically-exposed person, continuation of business relationship with such person shall be approved by a senior management member of the financial institution.

(10) Financial institutions shall take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as politically- exposed persons.

(11) Financial institutions shall obtain information on the purpose and intended nature of the business relationship.

(12) Banks shall perform enhanced due diligence on high risk categories of customers, business relationships or transactions.

(13) Financial institutions shall give particular attention to business relationships and transactions with natural and judicial persons from countries which do not or insufficiently apply anti-money laundering and combating terrorist financing laws.

Article 7. Account Monitoring

(1) Financial institutions shall conduct ongoing due diligence measures on existing customers and business relationships, including scrutiny of transactions undertaken throughout the course of that relationship to ensure that:

(a) the transactions being conducted are consistent with the financial institution's knowledge of the customers, their business and risk profile, and where necessary, the source of funds; and

(b) documents, data or information collected under the due diligence process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

(2) Where financial institutions are in a business relationship with a politically-exposed person, they shall conduct enhanced ongoing monitoring.

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

(4) Financial institutions shall examine as far as possible the background and purpose of transactions specified under this Article and set forth their findings in writing.

Article 8. Cross-Border Correspondent Banking

(1) With respect to cross-border correspondent banking and other similar relationships, financial institutions, in addition to performing normal customer due diligence measures, shall:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly- available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

(b) assess anti-money laundering and combating terrorist financing controls of the respondent institution, and ascertain that they are adequate and effective; and

(c) document the respective anti-money laundering and combating terrorist financing responsibilities of each institution;

(2) Where a correspondent relationship involves the maintenance of payable-through accounts, banks shall be satisfied that:

(a) their respondent financial institution has performed all the normal customer due diligence obligations set out in this Proclamation on its customers that have direct access to the accounts of the correspondent financial institution; and

(b) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent bank.

(3) Where a correspondent bank fails to comply with national anti-money laundering and combating terrorist financing laws, financial institutions shall not open an account, commence business relations or perform transaction or shall terminate the business relationship with such correspondent bank and consider making a suspicious transaction report in relation to that correspondent bank.

(4) Financial institutions shall satisfy themselves that respondent banks in foreign countries do not allow business relationship with shell banks.

Article 9. Wire Transfers

(1) For all wire transfers exceeding USD 10,000 or its equivalent in other convertible currencies, ordering banks shall be required to obtain and maintain the originator's:

(a) full name;
(b) account number or a unique reference number; if no account number exists;
(c) complete address; and
(d) date and place of birth.

(2) Banks shall adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information.

Article 10. Exemptions

(1) Identification of a customer does not need to be verified where the customer is itself a regulated bank or other financial institution that is subject to anti-money laundering and combating terrorist financing laws and regulations;

(2) Credit and debit card transactions are exempted from standard customer due diligence, provided that they are not used as payment tools to effect money transfer.

Section II. Keeping Records on Customer's Identification

Article 11. Records on Customer Identification and Maintenance of Records of Transactions

(1) A financial institution shall keep records on customer identification including copies or records of official identification documents like passports, identity cards, driving licenses or similar documents, account files and business correspondence for a period of 10 years after an account is closed to enable it comply with requests from competent authorities.

(2) A financial institution shall maintain, for a period of 10 years, all necessary records of transaction to enable it to comply with information requests from competent authorities.

(3) The records referred to in sub-Article (2) hereinabove shall be kept in sufficient form to permit reconstruction of individual transaction, including the amounts and types of currency involved, if any, so as to provide evidence for prosecution and criminal proceedings.

Article 12. Training Programs

(1) Financial institutions shall establish ongoing employee training programs which at a minimum incorporate:

(a) responsibilities under the financial institution's arrangements for money laundering and terrorist financing prevention;
(b) policies, procedures, controls and practices for obtaining identification evidence, applying "know-your-customer" standard, account monitoring; enhanced due diligence, record keeping and reporting of suspicion of money laundering and terrorist financing;
(c) audit function to ensure the bank's compliance with anti-money laundering and combating terrorist financing laws, directives, and internal policies and procedures;
(d) domestic laws related to money laundering and terrorist financing;
(e) relevant typologies of money laundering and terrorist financing; and
(f) potential risks, including reputational, operational and legal risks for being involved in laundering the proceeds of crime or financing of terrorism.

(2) A financial institution shall provide to the Bank the dates and descriptions of all anti-money laundering and combating terrorist financing staff training events, at the beginning of each financial year of the Bank.

PART III

DETECTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

Section I. Establishment of Financial Intelligence Unit (FIU)

Article 13. Establishment of Financial Intelligence Unit (FIU)

(1) An autonomous Financial Intelligence Unit (hereinafter referred as **"FIU"**) is hereby established to serve as a national authority responsible for receiving, requesting, analyzing and disseminating information concerning money laundering and financing of terrorism, as provided for by this Proclamation.

(2) The head of FIU shall be appointed by the President of the State of Eritrea. The composition, organization, operation and resources of the Financial Intelligence Unit shall be prescribed by Government directive.

Article 14. Powers and Functions of FIU

(1) The functions of FIU shall be to:

(a) receive, analyze and access reports of suspicious transactions issued by financial institutions;

(b) send any reports referred in sub-Article (1)(a) of this Article to the appropriate law enforcement authorities and the supervisory authority where, on the basis of its analysis and assessment, it has determined that there is an element of money laundering or financing of terrorism;

(c) send to the appropriate law enforcement authorities any information derived from an inspection carried out pursuant to sub-Article (2)(a) of this Article if it gives FIU reasonable grounds to suspect that a transaction involves offences of money laundering or terrorist financing;

(d) indentify training requirements and provide such training for any financial institution in respect of customer identification, transaction record keeping, and report obligations and identification of suspicious transactions; and

(e) conduct any investigation into money laundering or terrorist financing in the financial institutions only for the purpose of ensuring compliance of the financial institution with the provisions of this Proclamation.

(2) FIU may also:

(a) enter the premises of any financial institution during ordinary business hours to inspect any record kept in respect of money laundering or financing of terrorism, and ask any questions related to such records, make notes and take copies of whole or any part of the record;