HCBE -AML &CFT POLICY

REVISED JANUARY

2024

HOUSING AND COMMERCE BANK OF ERITREA SHARE COMPANY

APPROVED BY THE BOARD OF DIRECTORS

Berhane Ghebrehiwet

Secretary and GM

TABLE OF CONTENTS

PREAMBLE

Money Laundering (ML) is a serious threat to the financial system that leads to a serious security, political, economic and social problems. This has been widely recognized at the international level and concerted efforts are on track to fight these ultra-criminal activities. Consequently, aligned to these international efforts, The State of Eritrea in 2014 has issued the proclamation 175/2014 Anti-Money Laundering and Combating Financing of Terrorism Proclamation, and Bank of Eritrea has also issued a Directive 01/2014 on Customer Due Diligence and Identification. The State of Eritrea has amended proclamation No. 175/2014 and has issued Proclamation No.181/2018.

HCBE following these developments has revised its 2020 Anti-Money Laundering Policy (AML), system and controls, including sound due diligence procedures so as to align with the aforementioned proclamation and international standards. This revised edition is updated to include recent developments in AML and to be in line with international standards as well as industry best practices. This policy encompasses the basic tenets of the Anti-Money Laundering policy; Know Your Customer (KYC), Trade Based Money Laundering (TBML), Customer Due Diligence Policy (CDD), Responsibility of Compliance Office and Suspicious Activity Reporting policy.

HCBE's Board of Directors and Management are striving for continuous improvement of the Bank AML/CFT policy, procedure and staff capabilities to prevent the bank and/or its infrastructure from being used by criminals. The Bank has laid down appropriate guidelines regarding whom it shall accept, or more precisely, whom it shall not accept as its customers as also suitable set of "Know Your Customer" norms and formalities for accepting a customer. It is important for all staff members to be conversant and be absolutely familiar with the Money Laundering (ML) process as they must be vigilant all the times and should any of the aspects involved in ML process appear to be directed to our business, they must be able to read the danger, signal and report any suspicious activity. When unusual activity is detected, the bank attending officer will immediately (within 24 hours) submit an Unusual Activity Report (UAR) to the

bank's compliance officer. Submission of an UAR will be confidential and must be reported in writing with supporting documents. The Compliance Officer is responsible for reviewing the attending officer's UAR, and determines if a suspicious activity report (SAR) should be filed.

The Compliance officer following the decision will file the SAR to the Financial Intelligence Unit (FIU) for further investigation and litigation. All supporting evidences for the SAR will be maintained for a minimum of ten (10) years, and will be securely stored. The CO, through the Controller, will report to the Board of Directors the number of SARs filed each month, along with a brief summary as to the amount of the suspicious activities and why they were deemed that way.

OBJECTIVE

- To ensure Housing and Commerce Bank of Eritrea Share Company comply with State of Eritrea Proclamation No.175/2014 and 181/2018 on Anti money laundering and Combating Financing of Terrorism, and Bank of Eritrea Directive No.01/2014 on Customer Due Diligence and Identification.
- To protect Housing and Commerce Bank of Eritrea Share Company from becoming vehicle for, or victim, of illegal activities, including money laundering, perpetrated by its customers.
- To ensure Housing and Commerce Bank of Eritrea share company have adequate practices and procedures in place, including strict "Know-Your-Customer" rules; that promote high ethical and professional standards in the Bank and prevent the Bank being used, intentionally or unintentionally, by criminal elements.
- To ensure that they have adequate management information systems to provide the management and compliance officer, with timely information needed to identify, analyze and effectively monitor higher risk customer accounts.
- To ensure Housing and Commerce Bank of Eritrea meets the local and international standards on know your Customer (KYC) and Customers Due Diligence principles.

DEFINITIONS

Money laundering: is the process whereby criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities thereby avoiding prosecution, conviction and confiscation of the criminal funds.

In simple words, it is a process through which Dirty Money is converted to Clean Money. Money Launderers clean the funds so that they are no longer traceable to any underlying criminal activities. It also covers the monies which are legally obtained to fund terrorism or crimes.

Bank: means the Housing and Commerce Bank of Eritrea Share Company

Customer Due Diligence (CDD): Identifying the customer (including borrowers, lenders, investors, service providers, suppliers and contractors, and other party involved in a transaction), and verifying their identity on the basis of documents, data or information obtained from reliable and independent sources. And/or
Identifying the beneficial owners (where there is a beneficial owner who is not the customer) and taking adequate measures on risk sensitive basis, to verify their identity, so that the bank is satisfied that they know who the beneficial owner is. This includes measures to understand the ownership and control structure of the legal person, trust or similar legal arrangement; and obtain information on the purpose and intended nature of the business relationship.

Financing of Terrorism: is defined as an act by any person who by any means, directly or indirectly, willfully, provides or collects funds, or attempts to do so, with the intention that they should be used or in the knowledge that they are to be used in full or in part to carry out terrorist act, by a terrorist, or by a terrorist organization.

Financial Intelligence Unit: an autonomous authority established to receive, analyze and access reports of suspicious transaction issued by financial institutions, and send the report to the appropriate law enforcement authorities as per the proclamation 181/2018.

Large Cash Transaction: means a transaction exceeding USD 10,000 or its equivalent in other convertible currencies.

Proceeds of crime: shall mean any funds or property derived or obtained, directly or indirectly from an offence converted or transformed, in part or in full, into other property and investment yields.

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.

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 complex or unusual pattern of transaction that has no apparent or visible economic purpose.

Trade Based Money Laundering (TBML): TBML as defined by FATF in 2006, the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin and finance their activities.

Terrorist Act: 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.

Transaction with n o apparent / visible economic purpose may i n c l u d e : -

(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) Transaction which, without credible 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

(f) A transaction which is incompatible with the Bank knowledge and experience of the customer in question or with the purpose of the business relationship.

KNOW YOUR CUSTOMER POLICY (KYC)

In order to prevent and detect criminal activity, the Bank needs to develop an awareness of its customer base. It will help the bank to identify suspicious activity and be an effective tool in the fight against money laundering and other criminal activities.

CUSTOMER ACCEPTANCE POLICY (CAP)

The Customer Acceptance Policy enumerates explicit guidelines on the following aspects of customer relationship in the bank.

1. Opening account or transaction in anonymous or fictitious name(s)are prohibited;
2. Transaction on/or behalf of a 'SHELL' Bank/company are prohibited.
3. Opening account to any person or entity barred by international law is prohibited.
4. Not to open an account or close an existing account where the branch is unable to verify the identity and/or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data/information furnished to the bank.
5. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

6. Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder.
7. Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations available on the sanction's platforms including UN SDN List and OFAC List among others along with the Circulars furnished by the Bank of Eritrea and other Eritrean Agencies.

KYC Policy on Companies and Firms

The Bank needs to be vigilant against business entities being used by individuals as a front for maintaining accounts with banks. The Bank may examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk Perception; as in the case of a public company, the bank should focus on those who have 25% and above ownership of the Company.

KYC Policy on Politically Exposed Persons (PEPs)

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, important political party officials.
Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, 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. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

The Bank should gather sufficient information on any person/customer of this category intending to establish a relationship, checks all the information available

on the person in the public domain. The decision to open an account for PEP should be taken at a senior level and should be subjected to monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

Profile Based on Categorization

The Bank should prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his client's business and their location etc. For the purpose of risk categorization, individuals and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk.

Illustrative examples of low-risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulatory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.

Customers who are likely to pose a higher-than-average risk to the bank may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Enhanced due diligence measures are to be applied based on the risk assessment, thereby requiring intensive due diligence for higher risk customers, especially those for whom the sources of funds are not clear.

Customer Identification Policy

The Bank must ensure customer due diligence:
1) While establishing a banking relationship,
2) While carrying out a financial transaction,
3) When the Bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information.

MINIMUM IDENTIFICATION REQUIREMENTS FOR COMMERCIAL / CURRENT ACCOUNTS:

1. Articles and Memorandum of Association (Articles of Incorporation),
2. Business License (Activity License),
3. Board resolution authorizing the opening of the new account,
4. Certificate of Incorporation
5. UBO Information (In case of public companies)

MINIMUM IDENTIFICATION REQUIREMENTS FOR CONSUMER / SAVING ACCOUNTS:

One of the following forms of identification required with a picture,

1. For Nationals; Eritrean National ID Card, Residence Proof
2. For Foreigners; Diplomat ID, Work Permit, Residence Permit
3. Passport

TRADE BASED MONEY LAUDERING

Trade Based Money Laundering is based upon abuse of trade transactions and their financing. Techniques of TBML adopted by criminals vary from simple to complex. Simple techniques include 'over/under invoicing' of goods, multiple invoicing of goods, 'over/under shipment of goods and falsely described goods. Combinations of several simple techniques have been regarded as complex.

1. The Bank needs to establish and strengthen domestic cooperation and information sharing to combat TBML.
2. The Bank should arrange TBML focused training program to familiarize staffs with typologies and red flags so as to enhance their capacity to combat TBML.

CUSTOMER DUE DILIGENCE

Customer due diligence is an essential element of effective KYC procedures. The Bank can effectively control and reduce its risk only if it has an understanding of the normal and reasonable activity of the customer so that it has the means of identifying transactions that fall outside the regular pattern of activity. However,

the extent of monitoring will depend on the risk sensitivity of the account. The ongoing due diligence may include the following:

1. Verification of details of a potential entity, its management and operations.
2. A continuous good faith of efforts – in line with the advised procedures
3. Measure of prudence, responsibility and diligence that are expected from a reasonable and prudent staff under the circumstances.

The Bank management and staff should pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

The Bank management may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions, which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the Bank. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts have to be subjected to intensified monitoring. Bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

High risk Accounts: means customers, businesses or transactions that need to be subjected to more regular reviews, particularly against the KYC information held by the bank and the activity in the account. Such categories shall include, but not limited to:

(a) Businesses commonly used to launder proceeds of crime (i.e. cash intensive businesses)
(b) Relationships or transactions with countries known to have material deficiencies in their anti-money laundering and terrorist financing strategies,
(c) Politically exposed Domestic Persons and Politically Exposed Foreign Persons
(d) non-resident customers such as those staying in the country for less than one year or those in short visit or travel, along with walk-in customers.
(e) Companies that have shares in a bearer form,

DRIC (DECLARATION REGARDING IMPORTATION OF CASH)

- DRIC should be obtained from those who import Foreign Currency equivalent to or more than USD 10,000 or more into Eritrea.
- Where DRIC is applicable but not provided by the customer, reason should be evidenced on the transaction. For unconvincing reason or where customer fails to provide DRIC on next transaction STR should be raised.

UNUSUAL ACTIVITY REPORT (UAR)

In the event that a customer's transaction or behavior is unusual and could potentially be related to the commission of a money laundering or terrorist financing offence, immediately complete an Unusual Activity Report (UAR) and submit it to HCBE's Compliance Office. The UAR must be submitted to HCBE's Compliance Office within 24 hours of identifying the unusual activity.

SUSPICIOUS ACTIVITY REPORT (SAR)

A suspicious transaction is a transaction which leads you to suspect that money laundering or terrorist financing is occurring. It is generally 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.

SUSPICIOUS INDICATORS

- Cash brought in from countries with a high level of corruption or political instability.
- Amount, denomination, currency do not fit the customer's background
- No explanation given for the origin of the cash, incomplete, unlikely or partly incorrect explanation
- No supporting documentation in relation to the origin of funds or owner
- Cash exchange done without identifying the individual
- Pattern of transactions has changed since business relationship was established.

SUSPICIOUS ACTIVITY REPORTING

- Ensure your suspicion is not mere guess; you must have reasonable grounds to suspect that a money laundering or terrorist financing offence is occurring.
- Raise UAR as soon as possible with all details and copies of all applicable documents; forward it immediately to the Compliance Office.
- SAR should be raised even for attempted transactions: attempted transactions are those where customer did not complete when due diligence details/support documents requested
- Your suspicion should remain confidential
- When a transaction is suspected having links to terrorism financing: Immediately block the transaction (process it in the system but should not be transmitted)
- Transaction will remain frozen till instruction received from the Compliance Office.
- Managers, and employees are obliged, personally to report any unusual transaction aiming at money laundering (including terrorist financing)

HOLDING RECORDS

- Records should be kept and made available to Financial Intelligence Unit (FIU) for investigation for a minimum of ten (10) years.
- The objective for records keeping is to ensure that the Bank is able to provide the basic information to reconstruct the transaction undertaken, at the request of the Financial Intelligence Unit.

RESPONSIBILITY OF COMPLIANCE OFFICE

1. Developing and reviewing the Bank's AML/CFT policy in line with best practices and internationally acceptable standards and recommending any changes to the bank board of directors.
2. Developing Housing and Commerce Bank of Eritrea’s internal AML/CFT procedures and ensuring that copies are made available to staff to keep them fully aware of the dangers posed by money laundering and terrorist financing, and other financial crimes.

3. Ensuring that Housing and Commerce Bank of Eritrea's employees are fully aware of the Bank's AML/CFT policy and related procedures, and their individual obligations to the Bank, so that they are equipped and well informed about new changes and developments.
4. Responding to all internal and external enquires regarding the prevention of financial crimes including money laundering terrorist financing, and other compliance related matters.

TRAINING PROGRAM

- Training program should be conducted on regular basis to all Staff on 'KYC'& 'AML' policy so as to make the Management and staff conversant and be absolutely familiar with the Anti-Money Laundering (AML) process as they must be vigilant all the times.

- Records should be kept of all formal training conducted. These records have to include the names and other relevant details, dates and locations of the training.

ANNUAL INTERNAL AUDIT REVIEW

HCBE's internal audit department performs annual assessment of the Bank's AML/CFT compliance framework and reports its findings to the Chief Compliance Officer (CCO), the Chief Executive Officer and the Board of Directors.

The audit team performs a robust review and identifies gaps if any. The audit team delivers its findings based on the severity of the issue as observation, Minor issue and Major issue.

- Observation – an opportunity for a process improvement of potential future impact that doesn't have a current risk impact.

- Minor Issue – a discrepancy or gap that can easily be addressed and doesn't have a serious impact.

- Major Issue – a serious discrepancy and gap that requires immediate attention and poses severe risks to the AML program.

LAW ENFORCEMENT REQUESTS

From time to time, Eritrean law enforcement agencies may make a request to obtain documentation and or information in relation to their own investigations.

All requests from law enforcement must be made via a judicial court in the jurisdiction in which the Bank is duly registered. The request must clearly display the signature of the judge granting the request of the law enforcement agency.

REVIEW AND UPDATE OF POLICY

The implementation and updating of the Policy shall be ensured by the Strategic Management Team. This policy shall be reviewed and, if necessary, updated at least annually.