

FEDERAL GOVERNMENT OF SOMALIA

MINISTRY OF FINANCE

Anti-Money Laundering and Countering the Financing  
of Terrorism Governance and Compliance Regulations



OCTOBER, 2019

## Table of Contents

<b>PART 1: INTRODUCTION .....</b>	<b>4</b>
1.1 MANDATE OF THE FRAME .....	4
1.2 SCOPE OF THE REGULATIONS.....	4
1.3 PURPOSE OF THE REGULATIONS.....	4
<b>PART 2: THE NATIONAL ANTI-MONEY LAUNDERING COMMITTEE.....</b>	<b>4</b>
2.1. MANDATE OF NAMLC.....	4
2.3 MEMBERS OF NAMLC.....	5
<b>PART 3: MANDATE OF AML/CFT TASKFORCE .....</b>	<b>5</b>
3.3. MEMBERS OF AML/CFT TASKFORCE .....	5
<b>PART 4: THE FINANCIAL REPORTING CENTER (FRC) .....</b>	<b>6</b>
4.1. MANDATE OF FRC.....	6
4.2. REPORTING MECHANISM.....	6
4.3. AML/CFT RISK ASSESSMENT.....	6
4.4. INTERNATIONAL ENGAGEMENT AND COOPERATION ON AML/CFT MATTERS.....	7
<b>PART 5: THE CENTRAL BANK OF SOMALIA AND OTHER REGULATORY BODIES.....</b>	<b>7</b>
5.1. THE ROLE OF CENTRAL BANK .....	7
5.2. THE ROLE OF OTHER REGULATORY BODIES.....	7
5.3. COLLABORATION BETWEEN CSB, OTHER REGULATORY BODIES AND FRC .....	7
<b>PART 6: COMPLIANCE PROGRAMS.....</b>	<b>8</b>
6.1. PROGRAM OBJECTIVES.....	8
6.2. AML/CTF COMPLIANCE POLICIES AND PROCEDURES.....	8
6.3. DESIGNATION OF COMPLIANCE OFFICER .....	9
6.4. UNDERSTANDING RISK.....	F9
6.5. ML/TF RISK ASSESSMENT AND MITIGATION PROCEDURES.....	10
6.6. EMPLOYEES DUE DILIGENCE.....	10
6.7 STAFF SKILLS TRAINING AND AWARENESS.....	11
6.8 CUSTOMER DUE DILIGENCE (CDD).....	11
6.9. ENHANCED CUSTOMER DUE DILIGENCE (ECDD).....	13
6.10 POLITICALLY EXPOSED PERSONS (PEPS) .....	13
6.11. ON-GOING MONITORING .....	14
6.12. CUSTOMER IDENTIFICATION FOR PERSONAL ACCOUNTS OR TRANSACTIONS .....	14
6.13. IDENTIFICATION FOR LEGAL ENTITY.....	15
6.14. THIRD PARTY NATURAL PERSON.....	15
6.15. THIRD-PARTY LEGAL PERSON .....	15
6.16. OBTAINING AND RECORDING INFORMATION REGARDING BENEFICIAL OWNERS .....	15
6.17. INTERNAL CONTROLS .....	16
6.18. NGOS, NPOS AND CHARITIES' ACCOUNTS .....	16
6.19. CORRESPONDENT BANKING RELATIONSHIPS.....	17
<b>PART 7: REPORTING AND RECORD KEEPING REQUIREMENTS.....</b>	<b>18</b>
7.1. SUSPICIOUS TRANSACTIONS REPORTING (STRS).....	18
7.2. LARGE CASH TRANSACTIONS (LCTRS) REPORTING .....	18
7.3. ELECTRONIC FUNDS TRANSFER REPORTING.....	19
7.4. INCOMING AND OUTGOING WIRE TRANSFERS REQUIREMENTS.....	19
7.5. RECORD KEEPING REQUIREMENTS .....	20
7.6. TIPPING-OFF OFFENCES.....	20
<b>PART 8: ENFORCEMENT.....</b>	<b>21</b>

**PART 9: COOPERATION WITH LAW ENFORCEMENT ..... 22**

**PART 10: REVISION AND AMENDMENTS..... 22**



## Regulation 1: INTRODUCTION

### 1.1 MANDATE OF THE REGULATION

The enactment of the Anti-Money Laundering and Countering the Financing of Terrorism Act, 2016 has provided Somalia the necessary instruments in the fight against money laundering and terrorist financing. To avoid ambiguity and provide a further clarification, Article 52 of AML/CFT Act, mandates the Ministry of Finance to issue this regulation as a reference for the better implementation of this Act. The Ministry of Finance is also responsible for the overall administration of the Somalia sanctions regime. This regulation incorporates the necessary components of the AML/CFT Act, FATF Recommendations and other international best practices on Anti-Money Laundering and the Countering the Financing of Terrorism (AML/CFT). The adherence to the standards sets by this regulation will be monitored by the Financial Reporting Centre in collaboration with the Central Bank of Somalia and other regulatory bodies through on-site examinations and off-site analysis of data. In order to adopt this regulation. The Ministry of Finance shall seek approval from the National Anti-Money Laundering Committee.

### 1.2 SCOPE OF THE REGULATION

This AML/CFT regulation shall apply to the government institutions required under the AML/CFT Act to regulate designated industries and other industries deemed vulnerable for money laundering and terrorist financing. This regulation describes the structure of the AML/CFT regime in Somalia such as the role and authority of the nominated government institutions, compliance requirements, reporting and record keeping and enforcement mechanisms.

### 1.3 PURPOSE OF THE REGULATION

This regulation set out the ground rules and shall be a source for all regulations issued by all government institutions for institutions and professions subject to this Act. The Regulations outline the AML/CFT regime and provides clarifications for government institutions how they shall comply and adjust their own regulations. It also provides an outline of unified approach across all areas of government in the implementation of the AML/CFT Act.

## Regulation 2: THE NATIONAL ANTI-MONEY LAUNDERING COMMITTEE

### 2.1. MANDATE OF NAMLC

- a) The National Anti-Money Laundering Committee (NAMLC) is established by Article 24 of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Act of 2016 and has oversight responsibility of the AML/CFT regime in Somalia.
- b) The Committee's core mandate is to develop a national AML/CFT strategy, provide funding for capacity building of member institutions of NAMLC, set strategic priorities for the Financial Reporting Centre (FRC), establish information sharing gateway amongst member institutions of NAMLC and enhance the effectiveness of domestic coordination.



## 2.3 MEMBERS OF NAMLC

The National Anti-Money Laundering and Countering the Financing of Terrorism Committee (NAMLC) is chaired by the Minister of Finance and includes the Ministers of Justice, National Security, Commerce & Industry, and the Governor of the Central Bank, the Attorney General, the Director of the National Intelligence Service Agency and the Director of the FRC who is secretary to the Committee.

## Regulation 3: MANDATE OF AML/CFT TASKFORCE

NAMLC established an AML/CFT Taskforce with core focus on operationalizing the statutory functions and responsibilities of NAMLC outlined in Article 25 of the AML/CFT Act of 2016 as well as enforcing NAMLC directives. The mandate and strategic objectives of the AML/CFT Taskforce have been designed to ensure the implementation of the law in a coordinated manner and on the basis of institutional cooperation.

3.1. The main duties and objectives of the AML/CFT Taskforce shall be:

- a) Promote the AML/CFT regime in Somalia (through Task Based Implementation);
- b) Realise the Strategic Objectives set out by NAMLC, through co-operation, co-ordination and information exchange;
- c) Identify the capacity gaps in member institutions to combat Money-Laundering and Financing of Terrorism;
- d) Identify, analyse and mitigate risks, threats and methods of AML/CFT;
- e) Review and uphold the laws, policies and institutional regulations for combating ML/TF;

3.2. Propose and adopt appropriate mechanisms for collaboration and cooperation among the Task-Force members in the combat against ML/TF:

- a) Review and propose appropriate mechanisms for preventing and combatting ML/TF in the Federal Member States;
- b) Discuss and issue directives the role of Non-State Actors such as religious organisations, civil society, media and the private sector in the combat against ML/TF;
- c) Consider and propose appropriate institutional arrangements for training and capacity-building on AML/CFT for key AML/CFT agencies and other public officers generally adopt international or regional best practices in the combat against ML/TF;
- d) Consider proposals for technical assistance for the institutions involved in preventing and combating ML/TF;
- e) Prepare reports on the necessary legal, political and institutional reforms necessary for an effective combat against ML/TF.

## 3.3. MEMBERS OF AML/CFT TASKFORCE

AML/CFT Taskforce is chaired by Director of Financial Reporting Centre and includes Deputy Governor of the Central Bank / Director of Licensing & Supervision, Deputy Director General of National Intelligence & Security Agency, Deputy Attorney General, Director General of the Ministry of Internal National Security, Director General the Ministry of Finance / Director of Customs, Director General of the Ministry of Commerce and Industries and Director General of the Ministry of Justice.



## Regulation 4: THE FINANCIAL REPORTING CENTER (FRC)

### 4.1. MANDATE OF FRC

- a) The FRC established by Article 20 of AML/CFT Act, 2016 shall be operationally independent and autonomous. The FRC shall report its activities to the National Anti-Money Laundering and Countering the Financing of Terrorism Committee (NAMLC).
- b) FRC serves as Somalia Financial Intelligence Unit (FIU) and shall adopt the principles of a hybrid-style FIU, combining appropriate administrative, enforcement and judicial functions. The FRC's mandate is to collect, collate and analyse financial information and share relevant results with designated Somalia police officers. These police officers will then conduct investigations and if they find evidence of an offence, pass the results to designated Somali prosecutors. If these prosecutors determine that there are grounds for prosecution, the evidences will be presented to a Somali court of law presided by a judge trained on financial and terrorist financing crimes.
- c) FRC may request information, including documents and records from any reporting entity or government institution to ensure compliance with the AML/CFT Act. Government institutions and reporting entities shall make these documents and records available to the FRC upon request and within period not exceeding 14 days. In event of non-compliance with the FRC's request, FRC shall escalate this to National Anti-money Laundering Committee for an appropriate action.

### 4.2. REPORTING MECHANISM

- a) FRC shall develop an appropriate reporting guidelines and procedures for the reporting entities to submit their mandatory reports.
- b) FRC shall organise and provide AML/CFT compliance training programs for the reporting entities to comply with the reporting of AML/CFT requirements.
- c) FRC shall recommend and implement standards for individuals nominated for the roles of chief compliance officer by the reporting entities (and continued professional development (CPD) on the requirements of AML/CFT).
- d) FRC shall develop in collaboration with Ministry of Finance and National Intelligence Service an appropriate reporting guidelines and procedures for cross- border transport of cash or bearer negotiable instruments.

### 4.3. AML/CFT RISK ASSESSMENT

- a) FRC shall be the national agency responsible for coordinating the AML/CFT national risk assessment. Currently, the national risk assessment is in progress with the support of the World Bank, the program assessment will be shared with the AML/CFT stakeholders.
- b) FRC shall issue alerts to guide government institutions as well as reporting entities on money laundering, terrorist financing and related predicate offences indicators, trends, typologies and threats.



#### 4.4. INTERNATIONAL ENGAGEMENT AND COOPERATION ON AML/CFT MATTERS

- a) FRC shall be the focal point for Somalia to represent in national, regional and global meetings, forums, and organizations that focus on money laundering and terrorist financing.
- b) FRC may enter Memoranda of Understanding and other agreements with its counterparts to support and improve the effectiveness and implementation of the national anti-money laundering and combatting the financing of terrorism regime.

#### Regulation 5: THE CENTRAL BANK OF SOMALIA (CBS) AND OTHER REGULATORY BODIES

##### 5.1. THE ROLE OF CENTRAL BANK

- a) The Central Bank of Somalia (CBS) is the regulator responsible for licensing and supervising the financial institutions subject to the AML/CFT Act.
- b) CBS shall issue guidelines and circulars that set forth in detail the AML/CFT obligations and procedures in line with this regulation; AML/CFT regulation for Financial Institutions and the AML/CFT law.
- c) CBS shall issue guidelines that identify minimum documentation required for the financial institutions.

##### 5.2. THE ROLE OF OTHER REGULATORY BODIES

- a) Any regulator responsible for registering or licensing institutions or professions subject to the AML/CFT Act shall issue guidelines that set forth detailed the AML/CFT obligations and procedures in line with these regulations, AML/CFT regulations and AML/CFT law. Regulators shall consult with the FRC to promote consistency when developing guidelines.

##### 5.3. COLLABORATION BETWEEN CSB, OTHER REGULATORY BODIES AND FRC

- a) CBS, other Regulatory bodies and FRC shall develop a regulation to effectively control and monitor ML/TF risks
- b) CBS and other regulatory bodies shall share the inspection or audit reports with the FRC in the respect with AML/CFT related topics.
- c) CBS and other regulatory bodies shall enforce the AML/CFT compliance provisions in consultation with FRC.
- d) Any regulations issued by regulatory bodies, in the interest of improving AML/CFT regulations shall be in line with this regulation.



## Regulation 6: COMPLIANCE PROGRAMS

### 6.1. PROGRAM OBJECTIVES

A compliance program is developed to outline the procedures and responsibilities of a reporting entity towards the AML/CFT Act. The program shall also be designed to be an important tool to inform and guide the actions of reporting entity's employees, managers, and affiliate agents ensuring their compliance with AML/CFT requirements.

6.1.2. The main objectives of the AML/CTF compliance program may include:

- a) To identify, mitigate and manage the risk reporting entities may reasonably face that the provision of financial services at or from an establishment in Somalia might (whether inadvertently or otherwise) involve or facilitate money laundering; or the financing of terrorism;
- b) To identify, mitigate and manage the risk a business may reasonably face that the provision of designated services at or from a permanent establishment in a foreign country might (whether inadvertently or otherwise) involve or facilitate money laundering; or financing of terrorism
- c) To develop as a reporting entity, a written program comprising the AML/CFT Act requirements relating to customer Identification and verification in accordance with the Act and relevant regulations,
- d) To ensure that reporting entities take such action that complies with such requirements as specified in the AML / CTF Act and regulations in relation to the provision of reporting entities of our designated financial services; and
- e) To ensure that reporting entities implement to meet their regulatory AML/CFT obligations.

### 6.2. AML/CTF COMPLIANCE POLICIES AND PROCEDURES

Reporting entities shall have risk-based compliance policies and procedures indicating the commitment to comply with this regulation and AML/CFT Act 2016 to prevent money laundering and counter terrorist financing. For best practice, reporting entities need to develop AML/CTF compliance program with emphasis on:

- a) Developing effective Know Your Customer (KYC) information and incorporate KYC information in their employee training programs;
- b) Identifying and reporting suspicious and large cash transactions to the FRC and comply with the FRC's instructions in accordance with Article 14 of the AML/CFT Act;
- c) Developing a Risk Management Program evaluating the level of the customer risk, products, services, geographic locations, and delivery channels as well as transactions;
- d) Establishing effective disclosure requirements for customers;
- e) Having a designated compliance officer at the management level whose designation is verified by the FRC;
- f) Obtaining an external audit in accordance with generally accepted auditing standards;

- g) Developing an adequate training program on AML/CFT to inform employees, and agents and shall be on ongoing basis.

### 6.3. DESIGNATION OF COMPLIANCE OFFICER

The designated compliance officer can be a senior manager of the reporting entity who reports to the Board of Directors. Senior management and the Board should avail the necessary resources and make a commitment to support the Compliance Officer. The Compliance officer should have adequate knowledge about money laundering and terrorist financing, the trends and the dynamics of the related criminal offences. The duties of the reporting entity's compliance officer may include, but are not limited, to the following:

- a) Ensure that the compliance program is constantly updated to reflect developments in money laundering and terrorist financing typologies and legislation and regulations;
- b) Ensure that employees are trained regarding their duties in terms of the compliance program;
- c) Provide guidance and advice to employees and agents in respect of AML/CFT compliance;
- d) Receive Suspicious Transactions Reports (STR) from branches and agents;
- e) Carry out confidential enquiries in respect of STR's to determine if there is actual suspicion;
- f) Submit STRs and Large Transactions Reports (LCTRs) to the FRC in accordance with procedures as prescribed in the FRC guidelines.
- g) Liaise with, receive disclosures, and submit any reports required by the FRC and other relevant competent authorities, and
- h) Is responsible for the implementation of the reporting entity's compliance program: policies and procedures, staff training, risk assessment, conduct periodic and effective reviews.

### 6.4. UNDERSTANDING RISK

A risk assessment is an analysis of potential risks and vulnerabilities that could expose the reporting entity to ML/TF activities. This regulation may assist entities to identify inherent risks so that they may develop mitigation measures to deal with exposed risks. The outcome of the risk assessment process and action taken should reflect the reality of the business, be documented and as a best practice include risk elements applicable to the reporting entity. The risk that is attached to a service may be used to facilitate money laundering or terrorism financing represents a 'business risk'. Prior to providing a designated service to a customer, a reporting entity will consider its ML/TF risks regarding the items specified below:

- a) Its customer types;
- b) The types of designated products and services it provides;
- c) The delivery channels with its products or services; and the foreign jurisdictions with which it deals;
- d) The ML/TF risk which the customer would pose if the reporting entity provided a service to the customer, including risks related to:
  - i. Beneficial owners of the customer;
  - ii. Whether the customer, or any beneficial owner of the customer is a politically exposed person (PEP);



- iii. The source of funds and source of wealth of the customer and each beneficial owner of the customer;
- iv. Whether the reporting entity will be able to adequately understand the business or occupation of the customer; and
- v. The control structures of the customer.

#### 6.5. ML/TF RISK ASSESSMENT AND MITIGATION PROCEDURES

6.5.1. The risk assessment process will include:

- a) An assessment of the risk associated with the type of the individual customer and the nature of their business and source of income;
- b) An assessment of the anticipated volume of activity and anticipated size of transactions;
- c) An assessment of the nature of funds to be utilized during the transaction (cash, checks etc.);
- d) Determine the risk related to customer product or service offered to the customer, geographic location and delivery channels used.
- e) A search of the customer's name in the sanctions lists and other relevant databases.

6.5.2. Before any transaction with any customer is conducted, the reporting entity must determine associated risks by gathering KYC information.

6.5.3. When customer is identified as a high-risk customer, a reporting entity must conduct enhanced and ongoing monitoring of the customer's business relationship for the purpose of:

- a) Determining whether the transactions or activities are consistent with "what you know" about that client.

#### 6.6. EMPLOYEES DUE DILIGENCE

6.6.1. The reporting entity shall put in place appropriate risk- based systems and controls to screen any prospective employee who, if employed, may be in a position to facilitate the commission of money laundering or financing of terrorism offences in connection with the provision of a designated service by their business.

6.6.2. Risk- based systems and controls enable the reporting entity to support and manage its employees to ensure their compliance. The pre-employment screening procedure may include:

- a) Provide two letters of references from persons who know potential employee minimum three years;
- b) Undertaking a background check including clearance letter of good conduct from the Somali Police Force; and

6.6.3. Relevant employees are required to sign a written agreement signifying their adherence to the AML/CTF program and attending periodic training for updating their risk awareness skills.



6.6.4 Employees will report any violations of the Program to the Compliance Officer. Alternatively, employee or staff member may also report the violation to the senior management of the reporting entity. Such reports will be confidential, and the employee will suffer no retaliation for making them.

6.6.5. Employee accounts will be subjected to the AML/CTF procedures as customer accounts and will be reviewed by the Compliance Officer.

## 6.7 STAFF SKILLS TRAINING AND AWARENESS

6.7.1. The reporting entities shall implement ongoing training program for their staff, agents and management. Training materials and list of participants must be documented to ensure and implementation of regulatory requirements thereby following entity's own policies and procedures relating to AML/ CFT.

6.7.2. Effective employee training enhances their skills to understand new trends in money laundering and financing of terrorism techniques and methods.

6.7.3. Employees shall be instructed to interview customers paying regard to the following:

- a) Residence and the nature of employment of the customer;
- b) Amount of funds being transferred and to whom;
- c) Use of the websites of the FRC and other competent authorities;
- d) Access to general media reports;
- e) How to identify red flags and signs of money laundering or terrorist financing that arise during the employee performing their duties; and what to do once the risk is identified.
- f) Whether there is a suspicion the customer has contacts or association with a group designated as terrorist organization.

6.7.4. Employees are made aware of the disciplinary consequences for customer and employee non-compliance with the AML/CTF Act which may result in re-training, dismissal or civil and/or criminal penalties being pursued.

## 6.8 CUSTOMER DUE DILIGENCE (CDD)

The reporting entities shall conduct ongoing and enhanced due diligences CDD measures when a customer conducts business activity not aligned with their normal business activity; fails to provide additional information or other ID rightly bearing same information i.e. names, address information etc.

6.8.1. The AML / CTF program shall include appropriate systems and controls to determine in what circumstances any further KYC information or beneficial owner information should be collected, updated or verified in respect to the customer or beneficial owners of a customer, in order to enable the review and update of KYC information and beneficial owner information for the purposes of ongoing customer due diligence.



- 6.8.2. Reporting entities shall establish and maintain a written Customer Identification Program (CIP). This will mean the collection of reliable CIP information from each customer, utilize risk-based measures to verify the identity of each customer, record customer identification information and verification methods and results.
- 6.8.3. Collection of further KYC information in respect of customers, for ongoing customer due diligence purposes occurs when one of the following situations arises:
- a) Red flag signs, which demand customer due diligence;
  - b) Situations described below under Additional KYC information;
  - c) Customers suspected to be of a high or medium risk.
- 6.8.4. Update existing KYC information in respect of customers for ongoing customer due diligence purposes when one of the following situations arises:
- a) Customer information is updated for each new service;
  - b) Customer ID is verified when recorded ID has expired;
  - c) Customer information is verified once every two years and we have a system in place which tells us when customer information needs updating or verification.
- 6.8.5. Customer due diligence measures shall be undertaken by reporting entities to achieve the following:
- a) Identify the customer and verify that customer's identity using reliable, independent source documents, data or information;
  - b) Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner such that the Financial Institution is satisfied that it knows who the beneficial owners are and it understands the ownership and control structure of the customers in case of legal persons, business entities or non-profit organizations;
  - c) Verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person;
  - d) Understand and as appropriate obtain information on the purpose and nature of the business relationship;
  - e) Conduct on going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Financial Institution' knowledge of the customer, their business and risk profile, including where necessary the source of funds.
- 6.8.6. A reporting entity shall perform the following CDD measures to identify and verify the identity of their customers when:
- a) Establishing a new business relationship;
  - b) A new customer carrying out a transaction equal to or exceeding the threshold of USD \$10,000 or the equivalent in any currency;
  - c) Sending or receiving cash of any amount, or any transaction of any amount where money laundering or terrorist financing is suspected;
  - d) The reporting entity has doubts about the veracity or adequacy of previously obtained customer identification data;
  - e) Identify whether a third-party individual (s) is involved in the transaction;
  - f) Obtain information on the purpose and intended nature of the business relationship.

## 6.9. ENHANCED CUSTOMER DUE DILIGENCE (ECDD)

- 6.9.1. A reporting entity shall apply enhanced due diligence measures when:
- a) It determines under its risk-based systems and controls that the AML /CTF risk is high; or
  - b) A designated service is being provided to a customer who is or who has a beneficial owner who is, a foreign politically exposed person; or
  - c) A suspicion has arisen for the purposes of article 14 of the AML/CFT Act; or
  - d) The reporting entity is entering into a transaction with another party physically present in, or with a corporation incorporated in, a prescribed foreign country.
- 6.9.2. An appropriate risk-based systems and controls shall undertake enhanced customer due diligence as follows:
- a) Seek information from the customer or from third party sources in order to clarify and update KYC information already collected from the customer and update beneficial owner information already collected from the customer regarding the beneficial owners of the customer
  - b) Undertake detailed analysis of customer's KYC and beneficial owner information. Carry out measures to identify customer's and beneficial owner's source of wealth.
  - c) Verify KYC information and beneficial owner information in accordance with the Customer Identification Program and beneficial owner identification requirements
  - d) Undertake detailed analysis and monitoring of the customer's transactions including: The purpose, reasons for, and nature of transactions; and level of transaction behaviour.
  - e) Certain high risk customer transactions require senior management approval including; to continue a business relationship; whether a transaction should be processed.

## 6.10 POLITICALLY EXPOSED PERSONS (PEPS)

In accordance with AML/CFT, Act, a Politically Exposed Person (PEP) is defined as an individual who is or has been entrusted with a prominent public function in the Federal Republic of Somalia or in other countries, for example, heads of state or of government, ministers, members of parliament, senior judges, senior defence and law enforcement officers, senior state-owned entities and enterprises, political party officials, and senior staff of governmental and non-governmental organizations. Also, senior foreign representative and ambassador. All family members of such persons and close associates who have business or financial relationships with such persons are also included herein. Politically exposed persons (PEPs) require enhanced CDD measures, which may involve:

- 6.10.1. In relation to Politically Exposed Persons (PEPs) and their family members or close associates, the reporting entities shall establish appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a PEP, and if so, apply the following ECDD measures:



- a) Obtain approval from senior management before establishing or continuing a business relationship with such a person or beneficial owner.
- b) Identify the sources of wealth, sources of funds, and obtain information from individuals identified as PEPs;
- c) When business relations continue, apply enhanced on-going monitoring to the business relationship.

6.10.2. Procedures for determining whether a customer or beneficial owner is a PEP, Shall include:

- a) Seeking relevant information from the customer or beneficial owner.

#### 6.11. ON-GOING MONITORING

The monitoring process is necessary to identify transactions that may be suspicious. Such a process must be able to detect complex, large transactions or unusual transaction patterns, which have no apparent business or lawful purpose. Equally, low-value international financial transactions must also be carefully monitored as they could be as an attempt by terrorist financiers to scatter the funds and hide the real purpose of the transactions.

6.11.1. On an ongoing basis and prior to approving money transfer transactions, the Compliance Officer sets out:

- a) To request additional information or supporting documentation on any specific order regardless of the amount or stage of transaction;
- b) To randomly check and scan transactions by size, frequency and destination to identify activities that may look suspicious;
- c) To scrutinize transactions by customers for possible structuring;
- d) To aggregate transactions and analyze activities that may give rise to a suspicion and determine follow up, closer monitoring, documentation, and filing of STR if deemed reportable;
- e) To compare what is a 'norm' for a customer and determine if there is any deviation from the normal transaction pattern, and question the customer if necessary;
- f) To make use of good common sense and sound judgment to sort out transaction data and build customer activity transaction profiles and patterns.

#### 6.12. CUSTOMER IDENTIFICATION FOR PERSONAL ACCOUNTS OR TRANSACTIONS

612.1. A reporting entity shall ascertain the identity of their individual customers and in the case of Legal entities. The reporting entity shall ensure that the customer is the person he/she claims to be.

6.12.2. Reporting entities shall verify the identity of customer who is acting on behalf of a personal customer.



### 6.13. IDENTIFICATION FOR LEGAL ENTITY

- 6.13.1. For legal persons, the following information should be obtained:
- a) The person representing the entity must be identified;
  - b) On behalf of the reporting entity is only acceptable in the instances where the reporting entity has a written agreement between them prior to identifying or verifying information for a customer on behalf of the reporting entity;
  - c) Name, legal form and proof of existence of the legal persons (revised; legal entity).
  - d) The principal place of business of the legal person;
  - e) Resolution of the Board of Directors to open an account and identification of those individuals who have authority to operate the account and names of relevant persons holding senior management positions;
  - f) Mailing and registered address of legal person;
  - g) Nature and purpose of the business;
  - h) The identity of the beneficial owner;
  - i) Verify and obtain information regarding beneficiary ownership;
  - j) Verify whether individual owners and executive officers are Politically Exposed Persons.

### 6.14. THIRD PARTY NATURAL PERSON

- 614.1. When determination is made that a third party is involved in the transaction, ask customer detailed information about the third party.
- 614.2. Retain records about the third party.
- 6.14.3. Retain records about relationship between the customer and third-party individual.

### 6.15. THIRD-PARTY LEGAL PERSON

For natural persons representing a legal entity, Reporting Entities shall verify the identity by using reliable, independently sourced documents or information.

- 6.15.1. The Reporting Entities shall identify any person acting on behalf of the customer is authorized to do so and shall be verified through documentary evidence including specimen signature confirming the customer is legal person.
- 6.15.2. Monitor the business relationship on an on-going basis and examine any transactions carried out to ensure they are consistent with their knowledge of the customer, commercial activities and risk profile, and where required, the source of funds.
- 6.15.3. For legal persons, understanding and documenting the ownership and control structure of the customer.

### 6.16. OBTAINING AND RECORDING INFORMATION REGARDING BENEFICIAL OWNERS

Reporting entities shall take reasonable measures to obtain information from beneficial owners and identify and verify the identity of the beneficial owners.



- 6.16.1. In the cases where reporting entity decides that the customer is acting on behalf of beneficial owner, then they should take reasonable measures to verify the identity of the beneficial owner by using relevant information or data obtained from a reliable source such that the reporting entity is satisfied with the identity of the beneficial owner.
- 6.16.2. In the cases, Where the customers are other legal entities, the reporting entity should take reasonable measures to know the ownership and control structure of the customer, including the natural person who ultimately owns or controls the entity as detailed below:
- a) With respect to such legal entities, identification should be made of each natural person that:
    - i. Owns or controls directly or indirectly of the legal entity;
    - ii. The senior management of the legal entity; or
- 6.16.3. With respect to legal arrangements, identification should be made of the settlor, trustee, protector, and beneficiary or of persons in similar positions.
- 6.16.4. For Non-Governmental Organizations (NGOs) and non-profit organizations (NPO) (such as societies, charities etc.) the reporting entity shall also satisfy itself as to the legitimate purpose of the organization, including by reviewing its charter or governing document.

#### 6.17. INTERNAL CONTROLS

- 6.17.1. Reporting entities must ensure to set up proper internal controls to assess the following:
- a) When to execute, reject, or suspend a wire transfer lacking required originator or beneficiary information and considering reporting to the FRC.
  - b) When to take suitable follow-up action which may include terminating or restricting business relationships.

#### 6.18. NGOS, NPOS AND CHARITIES' ACCOUNTS

- 6.18.1. When establishing relationship with Non-Governmental Organizations (NGOs), not-for-Profit Organizations (NPOs) and Charities, the reporting entities should conduct EDD to ensure that these accounts are used for legitimate purposes and the transactions are matching with the objectives and purposes of the entity. The individuals who are authorized to operate the accounts and members of their governing body are subject to enhanced CDD.
- 6.18.2. Information obtained from NGOs/NPO and Charities organizations should be monitored and reviewed on ongoing basis, their authorized personnel, members of their governing body including executive officers should be periodically updated.

- 6.18.3. When discrepancies are noticed management must be alerted. And if necessary, STR may also be filed by the reporting entities' compliance Officer.
- 6.18.4. Reporting entities are obligated to follow NGO/NPO and Charities organization's regulatory guidelines. Enhanced due diligence including obtaining and verifying relevant information about Directors and officers of the organization must be met before relationship is established.
- 6.18.5. Timing of identifying customer and gathering information must take place before accounts or any transactions are conducted. In cases, where potential customer refuse, provide inconsistent information or resists to offer detailed information, Reporting Entities may file Suspicious Transaction Report, even if information on hand is incomplete.

#### 6.19. CORRESPONDENT BANKING RELATIONSHIPS

- 6.19.1. Reporting entities shall take the following measures, before agreeing to a cross-border correspondent banking relationship or other similar relationships:
- a) Collect enough information about the respondent bank to understand the nature of its major business activities.
  - b) Know the risks related to their geographic location or jurisdiction of correspondence.
  - c) Evaluate the money laundering and financing of terrorism prevention and detection measures and controls implemented by the respondent bank.
  - d) Assess the integrity of the respondent institution and the quality of supervision to which it is subject, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action in the respondent's country.
  - e) Establish documentation with respect to AML/CFT responsibilities of each bank.
- 6.19.2. Acquire approval of senior management, before establishing new correspondent banking relationship. Reporting entities shall take extra precautions when establishing or continuing relationship with correspondent banks or other financial institutions which are in jurisdictions that have been identified by FATF for having inadequate AML/CFT standards in the fight against money laundering and financing of terrorism.
- 6.19.3. Reporting entities shall not establish or continue a correspondent or business relationship with a shell bank and they must satisfy themselves that respondent financial Institutions do not allow their accounts to be used by these shell banks.
- 6.19.4. The above obligations shall be applied by reporting institutions to cross border correspondent banking and similar relationships established in accordance with the AML/CFT Act 2016.



## Regulation 7: REPORTING AND RECORD KEEPING REQUIREMENTS

The Anti-Money Laundering and Countering Financing of Terrorism Act imposes certain obligations upon reporting entities. The reporting requirements include suspicious and large cash transactions as well as wire transfers made by reporting entities. Reporting entities are also obligated to retain records obtained from the customers.

### 7.1. SUSPICIOUS TRANSACTIONS REPORTING (STRS)

- 7.1.1. Suspicious transactions require the application of enhanced customer due diligence and the following procedures shall be taken:
  - a) clarify, update or obtain the customer's KYC information from the customer or third party source;
  - b) Determine the nature of the customer's ongoing business with the reporting entity ;
  - c) Undertaking detailed analysis of the customer's KYC information;
  - d) Review the customer's past transactions and monitor future transactions; and
  - e) Determine whether there is an actionable and / or verifiable suspicion that may be reported to FRC.
- 7.1.2. Reporting entities shall comply with the provisions of AML/CFT Act, any regulations issued by their regulator and AML/CFT regulations issued by the Ministry of Finance to implement appropriate internal policies, procedures and controls.
- 7.1.3. Reporting entities shall monitor all unusual large transactions, and patterns of transactions, which have no apparent economic or lawful purpose.
- 7.1.4. The completed STRs shall be in the format obtained from the FRC within thirty days from the day detected or formed a suspicion of any transaction or attempted transaction.
- 7.1.5. Incomplete STRs filed by reporting entities shall result in requests for additional information and/or clarity. Repeated non-compliance to meeting STR reporting standards could be subject to appropriate penalties.
- 7.1.6. The employees and directors of the reporting entities are strictly prohibited to disclose to the customer or any other quarter the fact that a STR or related information is being or has been reported. This requirement may be included in the compliance and training programs of reporting entities.

### 7.2. LARGE CASH TRANSACTIONS (LCTRS) REPORTING

- 7.2.1. Reporting entities shall report to the FRC transactions or series of transactions that meet the threshold amount of USD \$10,000 or the equivalent in any currency (withdrawals, deposits or transfer) as per Art. 14 of the AML/CFT Act, 2016.
- 7.2.2. Reporting entities shall report the full details of Large Cash Transaction Report (LCTR) to the FRC, within fifteen working days.
- 7.2.3. Reporting entities shall submit completed LCTR forms; as prescribed in the LCTR form, incomplete LCTR forms submitted to FRC, shall be returned to provide additional information.

### 7.3. ELECTRONIC FUNDS TRANSFER REPORTING

- 7.3.1. Reporting entity should verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with the record keeping requirements of these guidelines.
- 7.3.2. In case of cross border wire transfers equal to or exceeding USD \$10,000 or its equivalent in other currencies, Financial Institutions shall obtain necessary supporting documents, in addition to the information obtained.
- 7.3.3. The financial institution shall not implement the wire transfer and rather consider submitting a STR report to the FRC if it is unable to comply with these requirements.
- 7.3.4. To prevent the increase of the risk associated with money laundering or terrorism financing, Financial Institutions should ensure that non-routine wire transfers are not batched.
- 7.3.5. The intermediary Financial Institutions should keep all wire transfer information including originator and beneficiary information when transaction is cross-border wire transfers.
- 7.3.6. In the cases where, technical limitations prevent the required information accompanying a cross-border wire transfer from remaining with related domestic wire transfer information, the intermediary financial institution should keep a record, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.

### 7.4. INCOMING AND OUTGOING WIRE TRANSFERS REQUIREMENTS

- 7.4.1. The requirement of this regulations shall apply to a financial institution when sending or receiving funds equal to or above USD \$1,000 or in any currency by wire transfer. They should record originator and beneficiary information on wire transfers and ensure that the information remains with the wire transfer during whole the payment process. Information required with the wire transfers should always include:
  - a) The full name and date and place of birth the originator;
  - b) Adequate details of the wire transfer including;
  - c) the date of the wire transfer;
  - d) the type and amount of currency;
  - e) the purpose and details of the wire transfer beneficiary and;
  - f) Relationship between originator and beneficiary, as applicable etc.;
  - g) The account number of the originator or, in the absence of an account, a unique transaction reference number;
  - h) The originator's date and place of birth, address, or in the absence of an address, originator's national identity number;
  - i) The name and account number or a unique reference number and address of the beneficiary.



## 7.5. RECORD KEEPING REQUIREMENTS

- 7.5.1. Reporting entities shall maintain records in accordance with Article 13 of AML/CFT, Act on customer transactions, relevant information obtained when conducting the transaction. (e.g. inquiries to establish the background and purpose of unusual large transactions)
- 7.5.2. All records of identification data obtained through CDD process (such as; copies of identification documents, account opening forms, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a period of five years after the business relationship is ended.
- 7.5.3. Reporting entities shall establish and maintain a customer record for all customers when establishing a business relationship or before carrying out a transaction.
- 7.5.4. Reporting entities shall periodically update customer records.
- 7.5.5. Reporting entities shall not keep anonymous customer records or customer records in fictitious names. Any such customer records in existence prior to the issuance of these regulations shall be closed within three months of this regulations's adoption unless all identification requirements in the AML/CFT law, and other relevant regulations are fulfilled.
- 7.5.6. The reporting entities are required to provide; identification data, transaction records, customer due diligence information, files and related correspondence to the relevant regulator upon request and in a timely manner.
- 7.5.7. Reporting entities shall maintain copies of STRs sent and related documents for at least five years.

## 7.6. TIPPING-OFF OFFENCES

Under Part II of AML/CFT Act, 2016 it is a criminal offence to inform or warn someone that he or she is under suspicion of money laundering or STR/LCT forms about their transaction or attempted transaction are being filled with FRC.

- 7.6.1. Employees and the directors of the reporting entities are required by law to maintain confidentiality in respect of such investigation and any suspicious transaction report that may be filed with FRC or informed to the law enforcement agencies. Tipping off (doing or saying anything that might inform someone else that he is under suspicion of money laundering), is a criminal offence under the provisions of the money laundering and terrorism financing law.
- 7.6.2. No criminal, civil, disciplinary or administrative proceedings for breach of banking or professional secrecy or contract shall lie against reporting entities or their respective directors, principals, officers, partners, professionals or employees who in good faith submit reports or provide information in accordance with the provisions of these guidelines.

## Regulation 8: ENFORCEMENT

- 8.1. Any natural or legal person who violates the directions mentioned in the AML/CFT Act and this regulation shall be liable to sanctions and penalties provided in Articles 27, 28 and 29 of the AML/CFT Act, 2016.
- 8.1.1. CBS and other Regulatory Bodies shall make it clear in their sectoral regulations that any reporting entity fail to implement appropriate AML/CFT internal controls, policies and procedures or fail to submit the required reports to the FRC shall be subject to the following:
- a) Informal warning – issued informal warnings by given them a month to resolve the identified issues.
  - b) Formal warning – if they fail to resolve it then issue formal warning by given them two months to resolve the identified issues
  - c) Monetary penalty – if the issue(s) remain unresolved then issuance of dissuasive and proportionate financial penalty(s) will be levied within three months from the date of issue
  - d) Suspension - in event they fail to pay the issued penalty within the specified period then suspend their license or registration until the fine has been paid
  - e) Revocations – if there is no payment after six months and identified issues remain unresolved then revoke their license or registration.
- 8.1.2. In accordance with Article 23 of the AML/CFT Act, FRC shall make it clear in its guidelines that any reporting entity that fails to provide the required AML/CFT reports in such format as prescribed by FRC shall be subject to the following actions:
- a) Informal warning – FRC shall write to the non-complying reporting entity requesting the submission of the required reports within a month, while simultaneously informing the relevant regulatory body.
  - b) Formal warning – if failure to submit required AML/CFT reports persists, FRC shall then issue a formal warning to the non-complying reporting entity by giving a notice of two months to resolve the identified issues, while simultaneously informing the relevant regulatory body.
  - c) Monetary penalty – if the issue (s) remain unresolved then FRC shall through the relevant regulatory body impose levied penalty for failing to provide the requested information and / or for failing to submit the AML/CFT required reports;
    - a. Together with each relevant regulatory body, FRC shall develop proportionate monetary penalties for the above violations.
    - b. All penalties shall be paid within three months from the date of issue and shall be credited to the Treasury Account.
  - d) Suspension – in the event that the non-compliant reporting entity continues failing to comply and pay the issued penalty within the specified period, then, FRC shall through the relevant regulatory body issue determination for suspension of license or registration for a period of two months.
  - e) Revocation – if the non-compliant reporting entity fails to comply with identified issues and / or pay the issued penalty, FRC shall, then, through the relevant regulatory body issue determination for revocation of license or registration for period of three months or until such time that the non-compliant entity clears its penalty arrears and provides the required reports to the FRC.

### Regulation 9: COOPERATION WITH LAW ENFORCEMENT

- 9.1. Central Bank of Somalia and Other Regulatory Bodies, where appropriate, shall assist law enforcement agencies in the criminal investigations as well as instruct those they regulate by making provision in the sectoral regulations.
- 9.2. FRC, where appropriate, shall assist law enforcement agencies with additional information relevant to ongoing investigation in connection with the money or the assets to the criminal activity.

### Regulation 10: REVISION AND AMENDMENTS

In consultation with the FRC and other members of NAMLC, the Minister may subject this regulations document to revisions and amendments as may be required by the AML/CFT law.

These regulations will come into effect with the signature of the Minister of Finance of the Federal Republic of Somalia:

Dr. Abdirahman Dualeh Beileh

Minister of Finance

Signature: \_\_\_\_\_



Date: \_\_\_\_\_

28 / 10 / 2019