ANTI-MONEY LAUNDERING & COUNTERING THE FINANCING OF TERRORISM (AML/CFT) REGULATIONS

FOR

FINANCIAL INSTITUTIONS IN SOMALIA

FINANCIAL REPORTING CENTER

MAY 2018

TABLE OF CONTENTS

ACRONYM AND ABBREVIATION

AML	-	Anti-Money Laundering
AMLRO	-	Anti-Money Laundering Reporting Officer
ATM	-	Automatic Teller Machine
CBS	-	Central Bank of Somalia
CDD	-	Customer Due Diligence
CFT	-	Combating of the Financing of Terrorism
CTR	-	Cash Transaction Report
FATF	-	Financial Action Task Force
FRC	-	Financial Reporting Center
KYC	-	Know Your Customer
LCT/LCTR	-	Large Cash Transaction Report
LEA	-	Law Enforcement Agency
ML	-	Money Laundering
MTBs	-	Monet Transfer Businesses
NGO	-	Non-Governmental Organisation
NIC	-	National Identity Card
NPOs	-	Non-profit Organizations
PEP	-	Politically Exposed Person
STR	-	Suspicious Transaction Report
TF	-	Terrorist Financing

CHAPTER ONE: GENERAL PRELIMINARIES

1.0. INTRODUCTIONS

1.1 Mandate of the regulation

Money laundering (ML) and terrorist financing (TF) has become global common issue and there has been growing recognition in recent times that both money laundering and terrorist financing pose major threats to international peace and security. This could more importantly undermine Somalia's post-war recovery and subsequent development progress. Coordinated global efforts have been made to combat these financial crimes, as result financial institutions have come under increased and constant regulatory regimes to improve their preventive measures, systems and controls to detect, prevent and respond effectively to the threat of money laundering and terrorist financing.

Following the enactment of the Anti-Money Laundering and Countering the Financing of Terrorism Act, 2016 and this AML/CFT regulation is now giving Somalia the necessary attention to the fight against money laundering and terrorist financing. The AML/CFT Act, 2016 and this AML/CFT regulation will only be effectively fruitful when there is full collaboration between Financial Reporting Center (FRC), Central Bank of Somalia (CBS) and other competent authorities as well as compliance by licensed financial institutions.

This regulation has incorporated necessary components of the AML/CFT Act 2016, FATF-Recommendations and other international best practices on Anti-Money Laundering and the Countering the Financing of Terrorism (AML/CFT). To avoid ambiguity and provide further clarification, this regulation has been included useful Appendixes on the areas like: Customer Due Diligence (CDD), Money Laundering and Terrorist Financing (red flags) and Politically Exposed Persons to assist financial institutions in their implementation of the anti-money laundering & countering the financing of terrorism (AML/CFT) requirements.

Financial institutions are constantly exposed to varying money laundering risks and serious financial and reputational damage if they do not manage adequately the AML/CFT risks. The implementation of customer due diligence would not only minimize the risk faced by licensed financial institutions of being used to launder the proceeds of crime but also provide protection against fraud, reputational and financial loss. Thus, the financial institutions are required to adopt a risk-based approach in the identification and management of their AML/CFT risks.

1.2 Scope of the regulation

This regulation applies to financial institutions such as banks, money transfer business (MTBs) and foreign exchange offices operating in the Federal Republic of Somalia as defined in the AML/CFT Act, 2016. This regulation establishes anti-money laundering and countering the financing of terrorism (AML/CFT) requirements and covers among others the following key areas of AML/CFT policy; Reporting or Chief Compliance Officer designation and duties; the requirement to cooperate with the supervisory authority such as Financial Reporting Center (FRC) and Central Bank of Somalia (CBS); Customer Due Diligence (CDD) procedures; monitoring of transactions and responding to suspicious transactions (STRs); reporting requirements; record keeping and retention; internal policies and procedures, and AML/CFT employee training, screening and programs.

1.3 Purpose of the regulation:

The financial reporting center (FRC) requires from all central bank licensed financial institutions and particularly banks and money transfer businesses to develop effective preventive measures, systems, controls, and practices to manage their potential money laundering/terrorist financing (ML/TF) risks. It is obligatory that the financial institutions licensed to operate in Somalia have satisfactory controls and procedures in place so that they know the customers with whom they are doing business relationships and dealings. Adequate due diligence on new and existing customers is a key part of these controls. Any person or institution that deliberately hinders or objects to cooperating with the FRC and other competent agencies in this regulation in the lawful exercise of their powers is guilty of an offence and shall be subject to appropriate administrative, civil or criminal fines or penalties pursuant to Part VI of Anti-Money Laundering and Countering the Financing of Terrorism Act, 2016.

1.4 Aims and Objectives of the regulation

The Aims and Objectives of this regulation are to detect, deter and disrupt the money laundering and terrorists financing to take place in anywhere in FRC jurisdiction. The goals of this regulation also include protecting financial institutions from being abused by financial crime practices, and thus, protecting their reputations and mitigating operational risk. The financial institutions are required to fully cooperate with the requirement of this regulation and perform their duties in the fight against financial crimes, particularly in the provisions of information that may lead to investigations and prosecutions of money launderers and terrorist financers. The cooperation between financial institutions, FRC, Central Bank of Somalia (CBS) and other competent organisations concerned will ultimately lead to the financial security of the country.

Financial institutions are therefore required to meet the terms and responsibilities set out by these regulations. The adherence of the standards set by this regulation will be monitored by the relevant competent authorities through on-site examinations and off-site analysis of data.

These regulations aim among others the financial institutions requirements:

a) To put in place policies, procedures, and controls to deter from financial crimes taking place.
b) To identify their customers effectively.
c) To have policies on customer acceptance that clearly identify when customers are to be denied business relationship.
d) To keep records of their transactions.
e) To designate of an anti-money laundering compliance officer responsible for enforcing the policies, procedures, and controls.
f) That the Chief compliance officer to be managerial level and to have been trained to the standards of FRC to carry out their duties under this regulation.
g) To submit reports on large cash transactions (LCT) and suspicious transactions reports (STR) to the FRC.

The definition of terms and key the legal words in this Regulation which have the same meaning as the AML/CFT Act, 2016 (unless the subject or context otherwise requires) are listed in Appendix v.

CHAPTER TWO: AML/ CFT GUIDELINES

Regulation 1: Policies and procedures and controls

Financial institutions shall address the following requirements:

1.1. They should develop risk-based internal policies, procedures, systems and controls to combat money laundering and terrorism financing. The internal policies and controls must indicate the Institution commitment to comply with this regulation and AML/CFT Act, 2016 to prevent any transaction that facilitates ML/TF activities.
1.2. The internal policies and controls should deter criminals from using institutions facilities for money laundering and terrorist financing and it should clearly indicate situations when a customer will be rejected and denied from business relationship.
1.3. Financial institutions shall ensure that internal policies, procedures, systems and controls are subject to independent testing and review. A copy of the written internal policies and procedures must be available upon request for evaluation to the satisfaction of FRC examiners that the policy has been implemented to the supervisory authority's standards.
1.4. The internal policies and procedures should be able to identify and handle in-coming wire transfers with no complete originator information. The incomplete originator information should trigger suspicious transaction assessment and whether it should be reported to FRC.

1.5. The internal policies, procedures, systems and controls should be adopted by the financial institution's board of directors and should be consistent with its size and complexity of their operations.
1.6. The internal policies, procedures, systems and controls should be applicable to all domestic and foreign branches and majority-owned subsidiaries of the financial institution.
1.7. Policies, procedures and controls should address risk evaluation of the customer, products, services, geographic locations, and delivery channels as well as transactions.
1.8. Institutions should ensure that the application of customer due diligence measures, identification and verification of the customer or beneficial owner, including one-off or occasional customers, and politically exposed persons (PEPs).
1.9. Maintain records and information obtained in the CDD process and information of transactions.
1.10. Institutions should monitor of transactions, including monitoring and identifying unusual or suspicious transactions.
1.11. The development of internal policies, procedures and controls shall be accompanied by appointment of a chief compliance officer at senior management level to ensure compliance with the provisions of the Anti-Money Laundering and Proceeds of Crime Law.
1.12. Institutions should ensure satisfactory screening procedures to make sure high standards when hiring these employees, ensuring training programs and providing on-going trainings to all new and existing employees, directors, board members, executive or supervisory management.
1.13. Financial institution shall ensure high standards while recruiting employees. This should include separate fit and proper requirements for employees in management positions or in positions perceived to have greater exposure to money laundering or terrorist financing.
1.14. Reporting to FRC of suspicious transactions and threshold transactions whether it's suspicious or not.

Regulation 2: Appointment of AML/CFT Reporting Officer and Internal Auditor

2.1 Financial institution shall develop appropriate AML/CFT compliance program, including at least, the appointment of a management level officer as the AML/CFT chief compliance officer (CCO) in line with this regulation.

2.2 The CCO and his/her team will have primary responsibility for development and implementation of the AML/CFT measures contained in this regulation. The internal controls must ensure that the necessary reports are filed with the FRC.

2.3 The AML/CFT compliance officer duty does not have to be a standalone position. He/she may perform other duties not related to AML/CFT compliance for his/her institution.

2.4 A separate internal auditor must be designated for auditing the implementation of the internal policies and procedures by the AML officer.

2.5 The appointed internal auditor shall also be responsible for assessing the overall adequacy of the anti-money laundering program in terms of risks identified in internal risk assessments and evaluating compliance of the financial institutions with its AML/CFT policy & procedures and FRC's AML/CFT regulation.

2.6 The internal auditor should report directly to the Board of directors of the financial institution and their reports should address the degree of AML officer's implementations of these measures.

2.7 Employee should get adequate training programs to ensure that they are kept informed of new developments and current ML and TF techniques, methods and trends.

Regulation 3: Performing Risk Assessments

3.1 Financial institutions should have processes to identify, assess, monitor, and mitigate money laundering and terrorism financing risks. Thus, shall effectively assess the risk that any business relationship or occasional transaction involves, or will involve, money laundering or terrorist financing, depending upon the type of customer, business relationship, product or transaction. The risk assessment and any underlying analysis and information shall be documented in writing, be kept up-to-date and readily available for FRC or any competent authority to review at their request.

3.2 Financial institutions shall be able to demonstrate to the FRC or any other competent authority that their CDD measures are appropriate taking into consideration the risks of money laundering and terrorist financing and that it has gathered suitable information to carry out the risk assessment requirement.

3.3 Financial institutions shall keep record of all the risk assessments and keep these documents up to date, and make the documents of the processes available to FRC or any competent authority upon request.

3.4 The following factors are to be considered by financial institutions when conducting their risk assessments.

a) The full customer's details including, nature of their business, occupation, or anticipated transaction activity.
b) Country in which customers operate or the place of origination or destination of transactions.
c) The source and origin of the customer's funds and delivery channels

d) The purpose of an account or relationship and products and services requested (i.e. risks that may be associated with the products and services offered)

e) Assessment of the risks associated with the size of transactions or deposits of the customer.

f) Assessment of the risks associated with the frequency of transactions or duration of the relationship.

3.5 Financial institutions should pay close attention to the risks set out in regulation 3 in particular, when designing and implementing customer identification policies and procedures. Therefore, financial institutions shall implement the following measures to manage and mitigate the money laundering and terrorism financing risks:

a. Acquire further information on the customer, beneficial owner, beneficiary and transaction that is being carried out.

b. Obtain any other documents as deemed necessary including its annual accounts, financial statements which may help the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer.

c. Establish a risk profile on customers and transactions. The customer profile should be based upon sufficient knowledge of the customer including the customer's anticipated business with the financial institution, and where necessary the source of funds or wealth of the customer.

d. Adopt enhanced customer due diligence to high-risk customers.

e. Update more regularly the information on all customers.

f. Apply other measures as may be prescribed by FRC or CBS.

3.5 Examples of high and low risk situations requiring Enhanced or Simplified Customer due Diligence (CDD) measures are set out in Appendix III.

CHAPTER THREE: CUSTOMER DUE DILIGENCE (CDD)

Regulation 4: Customer Identification and Due Diligence Requirements

The followings are some specimen when CDD measures are required to be applied for identification purposes:

4.1 Financial institutions shall not maintain or open an anonymous account or open an account in untrue names. They shall also, set up a registration system for the identification of their clients and establish the identity of clients when performing any transaction for them.

4.2 Financial institutions shall take additional steps to ensure proper customer identification when doubts have arisen, or where there is a suspicion that the customer is involved in money laundering or terrorist financing.

4.3 Financial institutions shall make sure that they know the true identity of the customer and have detailed knowledge of the customer's business before entering into the business relationship, including beneficial owners.

4.4 Financial institutions shall apply CDD measures to identity their customers effectively. Hence, Customer due diligence should be carried out in the following cases:

a) When opening an account or establishing a business relationship with a customer except for the situations provided in regulation 13 of this regulation (Simplified CDD)
b) when dealing with occasional customers or one-off transactions equal to or exceeding the designated threshold of USD $10,000 or the equivalent in any currency
c)Whenever there is a doubt about the reliability or adequacy of previously obtained customer identification data.
d) In other situations and scenarios when there is suspicion of money laundering and/or financing of terrorism, regardless of threshold.
e) Whenever sending or receiving cash of any amount, or any transaction of any amount where there is a suspicion of money laundering or terrorist financing

Regulation 5: CDD Measures for establishing Business Relationship

5.1 Financial institutions shall perform the following CDD measures when establishing Business Relationship:

a) Identify your customer & beneficial owners and verify their identity using reliable, independent source documents, data or information.
b) Identify and verify the identity of any person acting on behalf of the customer and whether he or she is authorized to do so.
c) Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.
d) Obtain the customers' tax identification number (TIN) and tax statements (if applicable) and in the case of legal persons, audited financial statements and personal details.
e) 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.
f) For legal persons, understanding and documenting the ownership and control structure of the customer.

5.2 Financial institutions shall make all reasonable efforts in identifying and verifying customer identities for establishing business relationship. For this purpose, ranges of documents which shall be obtained for different types of customers are provided in Appendix- II.

5.3 The Financial institutions shall obtain, verify and record the following information on KYC/CDD form or account opening form for identification and due diligence purposes.

a) Full name as per identity document;
b) Original Passport or National Identity Card or where the customer is not a natural person, the registration or incorporation number or business registration number (as applicable).
c) Residential address details registered or business address (as necessary), contact telephone number(s) and e-mail (as applicable).
d) Date of birth, incorporation or business registration (as applicable).
e) Nationality or place of birth, incorporation or registration (as applicable);
f) Nature of business, geographies involved (as applicable).
g) Purpose of account or Type of account.
h) Source of funds or Source of earnings.

5.4 Financial institutions shall obtain and keep record of information and documentation demonstrating that they are satisfied that the identity of the beneficial owner of the account or funds is known and verified.

5.5 Based on the level of risk and in the interest of improving access to financial services, a natural person's identity shall be verified by obtaining of an original national identity card, passport or birth certificate, or other reliable information and documentation as detailed in Appendix- II.

Regulation 6: Identification and Verification of Legal Person

6.1 The concerned financial institutions shall verify identities of their customers. In case of legal persons the identities of their natural persons should be verified from relevant authorities or using other reliable independent sources and keep records of all reference documents used for verification and identification.

6.2 The financial institution shall satisfy itself that the customer is the person he/she claims to be. In the cases, where a letter of statement is accepted from a professional person, it should include a telephone number where the person can be contacted for verification.

6.3 The financial institution should verify from an independent source the information provided by the professional person.

6.4 Legible file copies should be taken of the relevant identification and supporting documentation for all customers both natural and legal persons. The customer's signature or finger print should be obtained on each page of such copies.

6.5 Financial institutions may set out in guidelines additional identification and verification requirements for customers and legal persons.

6.6 Financial institutions shall verify if a natural person is claiming to act on behalf of a customer who is legal persons or legal arrangements. For legal persons, the following information should be obtained among others:

a) Name, legal form and proof of existence of the legal persons.
b) Location of the principal place of business of the legal person.
c) 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.
d) Mailing and registered address of legal person.
e) Nature and purpose of the business.
f) The identity of the beneficial owner.

Regulation 7: Identification and Verification of Natural Persons Acting on Behalf of Customer

7.1 For natural persons, financial institutions shall verify the required identity using reliable, independent source documents, data, or information as outlined in Appendix II of this Regulation.

7.2 The concerned financial institutions shall identify that any person acting on behalf of the customer is authorised to do so and shall be verified through documentary evidence including specimen signature ensure customer is legal person.

7.3 Monitor the business relationship 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.

7.4 For legal persons, understanding and documenting the ownership and control structure of the customer.

Regulation 8: Identification and Verification of Beneficial Owners

Financial institutions shall take reasonable measures to obtain information from beneficial owners to identify and verify the true identity of the real beneficial owners.

8.1 Financial institutions shall take necessary steps to determine if a customer is acting on his/her own or on behalf of beneficial owners.

8.2 In the cases where financial institution decides that the customer is acting on behalf of beneficial owner, then they should take rational measures to verify the identity of the beneficial owner by using relevant information or data obtained from a reliable source such that the financial institution is satisfied with the identity of the beneficial owner.

8.3 The measures to verify the identity and the information/documents to be obtained on beneficial owners should be consistent with the customer identification requirements outlined in **Appendix II of this Regulation.**

8.4 In the cases, Where the customers are other legal entities, the financial institutions should take enough 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:

1. With respect to such legal entities identification should be made of each natural person that:
    a) Owns or controls directly or indirectly of the legal entity;
    b) Is responsible for the management of the legal entity; or
    c) Exercises control of the legal person through other means.
2. With respect to legal arrangements, identification should be made of the settlor, trustee, protector, and beneficiary or of persons in similar positions.

8.5 For Non-Governmental Organizations (NGOs) and non-profit organizations (NPO) (such as societies, charities etc.) the financial institution shall also satisfy itself as to the legitimate purpose of the organization, including by reviewing its charter o governing document.

Regulation 9: CDD Measures for Occasional Customers and One-off Transactions

9.1 Financial institutions shall;

a) During occasional customers and one-off Transactions;
    I. Obtain copy of national identity card and or passport and fill LCT form from the customer while conducting cash transactions equal to or exceeding the designated threshold of USD $10,000 or the equivalent in any currency; and
    II. Obtain copy of national identity card and or passport while issuing remittance regardless of threshold.

b) Obtain copy of national identity card and or passport (regardless of threshold) while conducting online transactions by occasional customers or one-off customers.

9.2 Financial institutions shall not allow any transaction on behalf of a customer who declines to disclose their true identity or unwilling to disclose the source of their funds if the transaction is USD 10,000 or equivalent in any currency.

CHAPTER FOUR: ENHANCED CUSOMER DUE DILIGENCE (ECDD)

Regulation 10: Identifying and Dealing with Politically Exposed Persons (PEPs)

PEPs are defined as individuals who are or have been entrusted with prominent public functions both in Somalia or foreign countries and those associated with them. Some examples of PEPs are listed in **Appendix I.**

10.1 In relation to Politically Exposed Persons (PEPs) and their family members or close associates, the financial institutions 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 additional CDD measures;

a) Obtain approval from senior management before establishing or continuing a business relationship with such a person or beneficial owner, where the customer or a beneficial owner is PEP or subsequently becomes a PEP;
b) Taking all necessary steps, Identify the sources of wealth and funds of customers and beneficial owners identified as PEPs
c) During the course of business relations, apply enhanced on-going monitoring to the business relationship.

10.2 Procedures for determining whether a customer or beneficial owner is a PEP, should include but are not limited to the following:

a) Seeking relevant information from the customer or beneficial owner.
b) Accessing and reviewing available information from any reliable source about the customer or beneficial owner.
c) Searching and accessing commercial or non-confidential electronic databases of PEPs, if available.

Regulation 11: NGOs, NPOs and Charities' Accounts

When establishing relationship with Non-Governmental Organizations (NGOs), Not-for-Profit Organizations (NPOs) and Charities, the financial institutions 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.

11.1 Accounts should be opened for the concerned NPO ensuring that the name is matching with the documents of the entity. The individuals who are authorized to operate these accounts and members of their governing body should also be subject to enhanced CDD. Personal accounts shall not be allowed to be used for NPOs purposes or collection of donations.

11.2 All existing relationships of NPO and Charities should be reviewed and monitored to ensure that these organizations, their authorized signatories, members of their governing body and the beneficial owners are as the same as that of the entity soliciting donations. In case of any difference, immediate caution should be marked on such accounts and the matter should be considered for filing STR.

11.3 If the obligations above and other relevant regulations are not met, the financial institutions shall not open the account, commence or continue business relationships, or perform the transaction. In such case, the reporting entity shall submit a suspicious transaction report to the Financial Reporting Centre.

Regulation 12: Enhanced CDD on ML and TF Risks Measures

12.1 Where there is ML or TF risks, financial institutions shall carry out enhanced CDD measures, consistent with the risks identified. Financial institutions should also increase the scale and nature of monitoring of the business relationship, to establish whether those transactions or activities appear unusual or suspicious and whether they should be reported to FRC.

12.2 Financial institutions shall scrutinize by compiling additional information from the customer including; reason for the transaction, the purpose of all complex, unusual large cash transactions (LCTs), and all unusual patterns of transactions, which have no obvious economic or legitimate purpose

12.3 The financial institutions shall conduct the following enhanced CDD measures among others, for higher-risk business relationships;

a) Attaining additional information on the customer (e.g. occupation, volume of assets, available information on the customer), and updating more regularly the identification data of customer and beneficial owner.

b) Attaining additional information on the intended nature of the business relationship.

c) Attaining information on the source of funds/source of assets of the customer.

d) Attaining information on the reasons for intended or performed transactions.

e) Attaining the approval of senior management to commence or continue the business relationship.

f) Carrying out enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

g) Carrying out the first payment through an account in the customer's name with a bank subject to similar CDD measures.

12.4 Enhanced CDD should be applied to higher risk customers at each stage of the CDD process and on an on-going basis.

12.5 Enhanced CDD procedures for business relationships with natural persons not physically present for the purpose of identification should include:

a) Certification of documents in line with relevant Laws and Regulations;
b) Requisition of additional documents and development of independent verification measures and/or contact with the customer.

Regulation 13: Simplified CDD on ML and TF Risks

13.1 The customers must be subject to the full range of customer due diligence measures as provided in **Appendix III** of this Regulation. However, where the risks have been identified as low, financial institutions may apply simplified CDD measures by documenting the risk assessment of the customer relationship.

13.2 Financial institution may determine the risk of ML and TF of a customer is low, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems, simplified measures may be applied.

13.3 In the cases where, the customer has a business relationship with or in countries as mentioned in **Appendix III** or if there is a suspicion of money laundering or terrorism financing the financial institutions shall not employ simplified CDD measures and may consider filling STRs with FRC in this case.

13.4 Financial institutions shall submit the risk assessment measures and the grounds for their simplified CDD when requested by FRC. They shall make the documents of the assessment processes and procedures related to risk assessment available to FRC.

13.5 The simplified CDD procedures taken should be corresponding with the risk factors. Where the risks have been identified as low, possible simplified CDD measures could include, but are not limited to the following:

a) Reducing the frequency of customer identification updates
b) Reducing the degree of on-going monitoring and scrutinising transactions

Regulation 14: Timing of Customer Identification and Verification

14.1 Financial institutions shall obtain sufficient information from customers and beneficial owners for sole the purpose of establishing business relations.

14.2 Financial institutions shall employ risk management procedures with respect to the conditions under which a customer may use the business relationship prior to verification.

14.3 Financial institutions may employ in a limited business relationship with the customer prior to the completion of the customer verification process, if the following circumstances among others are met:

a) When the verification is being carried out as soon as reasonably possible.
b) When it is essential not to interrupt the normal conduct of business.
c) When the ML and TF risks are effectively managed.
d) When ATM card or cheque book is issued until the verification of identity of the customer is completed.

14.4 The risk management procedures should include a set of measures to manage and mitigate the ML and TF risks such as:

a) To set limit on the number, types and amount of transactions that can be carried out.
b) To monitor the nature and the complexity of transactions being carried out outside the expected norms for that type of relationship.

14.5 The financial institutions will maintain a list of all such customers/accounts where the business relationship needed to be closed on account of negative verification.

Regulation 15: Additional Customer Information Requirements

15.1 Financial institutions shall record and maintain customer information during the course of the business relationship. Customer information, data and Documents collected due to CDD process should be kept up to date by reviewing the existing records at regular intervals as decided by the institution, for instance;

a. Where there is a significant transaction is to take place;
b. Where transactions begin to deviate from its routine patterns or there is a significant change in the way the account is operated.
c. Where the information held on the customer record is inadequate to satisfy financial institutions to meet the requirement of these regulations.
d. Where the information held on the customer is not enough to enable the financial institution to understand the nature of the transactions being conducted or business relationship in general.

15.2 In the case of legal persons, financial institutions must make sure the following addition requirements are met including but not limited to:

a. The entity, company or business registration and licensing documents shall be valid and up-to-date throughout the duration of the business relationship.

b. Financial institutions shall obtain regular updated financial statements from customers.

c. Financial institutions shall ensure that the taxation information (copy of tax returns and certification) is obtained and updated on an annual basis if applicable.

15.3 Financial institutions shall perform the CDD requirements of this regulation to existing customers on the basis of materiality and risk.

15.4 The account opening forms (KYC forms) should be filled out by every customer in Somali language or English or Arabic if the customer is foreign.

15.5 Despite the provisions of other paragraphs of this regulation, financial institutions should renew and update the KYC forms of any customer at least on yearly basis.

CHAPTER FIVE: ONGOING TRANSACTION MONITORING

Regulation 16: On-going Monitoring of Customer Transactions

16.1 Financial institutions shall implement systems, and preferably automated systems, to examine on regularly the customer transactions and the relationship with the customer.

16.2 All business relations with customers shall be monitored on an on-going basis to ensure that the transactions are consistent with the financial institution's knowledge of the customer, its business and risk profile and where appropriate, the sources of funds.

16.3 Customers' account activity shall be monitored on a regular, reasonable schedule, to be able to establish patterns, the deviation from which may indicate suspicious activity. The background and purpose of these activities shall be documented and made this information available to the relevant competent authorities when required.

16.4 Financial institution shall regularly monitor linked transactions which is a series of transactions by a legitimate customer, or they may be transactions that appear to be independent, but are in fact split into two or more transactions to avoid detection. This typically happens when a customer tries to avoid anti-money laundering controls by splitting transactions into several smaller amounts, below the level at which you check ID or enquire about the source of funds.

16.5 Financial Institutions must be able to associate a series of money transfers made by different customers to the same recipient over a period of time. If you conduct business through branches or agents, your systems should be able to identify linked transactions that are conducted through all your locations. FRC recommends that financial institutions consider checking for linked transactions over a minimum rolling 90 day period.

16.6 Financial institutions shall regularly review whether the information obtained from the customers and beneficial owners are satisfactory and up to date, particularly for higher risk categories of customers as details in Appendix III. The review period and procedures thereof should be defined by financial institutions in their AML/CFT policies, as per risk based approach.

Regulation 17: Customer Relationship Prohibition and Termination

Existing Customers

17.1 When a Financial institution is unable to complete the required CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk, the existing customer relationships established prior to the enactment of this regulation should be terminated and filling a report with the FRC should be considered.

W**hen CDD Measures are not completed**

17.2 Financial institutions shall refrain from opening the account or commencing the business relationship or carrying out the transaction, where it is unable to verify the identity of the customer and beneficial owners. In these cases, the financial institution shall consider filing a suspicious transaction report to the FRC.

Anonymous or Fictitious Account

17.3 Financial institutions shall not open, maintain or operate anonymous accounts or accounts in fictitious names.

Prohibited relationships

17.4 Reporting entities are prohibited from establishing or maintaining business relationships with a shell bank (or any financial institution with no physical presence) in the jurisdiction in which it is incorporated or licensed.

17.5 Reporting entities are prohibited from doing business with sanctioned persons or entities imposed by the Ministry of Finance or other international authorised bodies. Financial instructions are also required to issue detailed regulations that identify sanctioned persons or entities.

Regulation 18: Reliance on Third Parties Intermediaries

18.1 Financial institutions should pay a close attention to the money laundering and terrorist financing risk associated with the country in which the third party they are trying to enter into a relationship with is based.

18.2 Financial institutions should know that ultimate responsibility for customer identification and verification shall remain with them and not with the third party they are relying on.

18.3 Financial institutions may only rely on third party intermediaries to perform the CDD requirements of this regulation if the following conditions are met:

a. They are satisfied that the third party is regulated, supervised or monitored for and has measures in place for compliance with the customer due diligence and record keeping requirements;

b. They are satisfied that copies of identification data and other documents relating to customer due diligence measures will be made available from the third party upon request and without delay.

c.The ultimate responsibility for customer identification and verification shall remain with the financial institution relying on the third party.

Regulation 19: Correspondent Banking and Shell Banks Relationships

Correspondent banking:

19.1 In addition to conducting standard CDD measures, financial institutions shall take the following measures, before entering into a cross-border correspondent banking relationship or other similar relationships:

a) Collect sufficient information about the respondent bank to understand the nature of its major business activities.
b) Know their geographical presence/jurisdiction (country) 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) Fully recognise and document the respective AML/CFT responsibilities of each bank.

f) Acquire approval of senior management, before establishing new correspondent banking relationship.

19.2 Financial institutions shall take extra precautions when establishing or continuing relationship with correspondent banks or financial institutions which are located in jurisdictions that have been identified by FATF for inadequate or poor AML/CFT standards in the fight against money laundering and financing of terrorism.

19.3 In the cases of the payable-through accounts, financial institutions shall satisfy themselves that the:

a) Respondent bank has carried out CDD measures requirements on its customers that have access to the correspondent bank's accounts.

b) Respondent bank can provide relevant CDD information when requested by the correspondent bank.

Shell banks:

19.4 Financial institutions 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.

19.5 The above obligations shall be applied by financial institutions to cross border correspondent banking and similar relationships established before the authorisation of this Regulation and or the AML/CFT Act 2016.

Regulation 20: Money Laundering and Terrorist Financing Red Flags

20.1 Constant monitoring and reporting of suspicious transactions is vital to AML/CFT effectiveness and compliance. Financial institutions are, therefore, required to put in place effective and efficient transaction monitoring programmes to facilitate the requirement of this regulation and AML/CTF Act 2016.

20.2 Although the types of transactions which could be used for money laundering are numerous, it is possible to identify certain basic features which tend to give reasonable cause for suspicion of money laundering as listed in **Appendix IV**. This red flag list may not be in-depth and comprehensive, but it does reflect some ways in which money launderers have been known to operate.

20.3 Transactions or activities highlighted in this list are not necessarily indicative of actual money laundering if they are consistent with a customer's legitimate business. Identification of any of the types of transactions listed here should put financial institutions on enquiry and provoke further investigation to determine the true legal status of the transaction activity.

CHAPTER SIX: WIRE TRANSACTION POLICIES AND REPORTING REQUIREMENTS

Regulation 21: Wire Transfers (Fund Transfers) Policies and Procedures

For the purposes of this Chapter;

21.1 The word Beneficiary means the natural or legal person who is identified by the originator as the receiver of the requested wire transfer and it is also refers to the term recipient in many times.

21.2 The word beneficiary financial institution means the financial institution which receives the wire transfer from the ordering bank directly or through an intermediary financial institution and makes the funds available to the beneficiary or recipient.

21.3 During the wire transfers, a beneficiary financial institution 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 this regulation.

21.4 The requirement of this regulation 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.

21.5 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:
    i. the date of the wire transfer,
    ii. the type and amount of currency,
    iii. the purpose and details of the wire transfer beneficiary and,
    iv. Relationship between originator and beneficiary, as applicable etc.
c. The account number of the originator or, in the absence of an account, a unique transaction reference number.
d. The originator's date and place of birth, address, or in the absence of an address, originator's national identity number;
e. The name and account number or a unique reference number and address of the beneficiary.

21.6 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 (21.15a) above.

21.7 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.

21.8 Ordering bank must make available the information on wire transfers within three business days of receiving the request from the beneficiary financial institution or from the FRC.

21.9 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.

21.10 The intermediary financial institutions should keep all wire transfer information including originator and beneficiary information when transaction is cross-border wire transfers.

21.11 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.

21.12 Financial institutions shall have efficient risk assessment procedures for deciding:

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.

Regulation 22: Suspicious Transactions Reporting (STRs) Requirements

22.1 Financial institutions shall comply with the provisions of AML/CFT Act, 2016 and this regulation by implementing appropriate internal policies, procedures and controls.

22.2 Financial institutions shall pay close attention to all unusual large transactions, and unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

22.3 The details of STRs should be reported to the FRC in the prescribed form as set out in Appendix VI within thirty days from day detected or formed a suspicion of

any transaction or attempted transaction. Some examples of suspicious transactions (Red Alerts) that may be a cause for increased examination for AML/CFT purposes are listed in **Appendix IV.**

22.4 The STRs submitted to FRC shall contain all essential supporting documents including: Identification documents (passport, national identification card, Business license and etc), updated customer's KYC, account opening forms and other relevant documents supporting the reasons for forming suspicion about the customer.

22.5 If FRC decides that the quality of reported STR is unsatisfactory, or some necessary supporting documents are missing, FRC may reject the acceptance of the STR stating the reasons of such rejection. In this case, the financial institution must rectify its mistake and resubmit the completed form the FRC.

22.6 The employees and directors of the financial institutions 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 to the FRC. This shall be made part of Code of Ethics of the financial institution which to be signed by employees and Directors of the institution.

Regulation 23: Large Cash Transactions (LCTs)Threshold Reporting Requirements

Financial institutions shall report to the FRC:

23.1 Financial institutions shall report to the FRC any transactions or series of transactions (linked transaction) that appear to be linked which exceed the designated threshold of USD $10,000 or the equivalent in any currency (withdrawals, deposits or transfer) under Reporting obligations Art. 14 of the AML/CFT Act, 2016.

23.2 Financial institutions shall report the full details of large Cash Transaction Report (LCTR) to the FRC, within fifteen days and on first and fifteenth day of each month, by 5:00pm, as batch for the transactions of the preceding the first and fifteenth.

23.3 Financial institutions shall include their report all required information as set out in the LCTR form. If incomplete report or carelessly filled out LCTR forms is submitted to FRC, proportionate administrative sanctions and penalties may be imposed to the institution by competent authority, as detailed in Part. IV of AML/CFT Act, 2016.

Regulation 24: 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/SAR forms about their transaction or attempted transaction are being filled with FRC.

24.1 When financial institution becomes aware of any red flag or suspicious money laundering activity, the financial institution is required to have a Review Panel without delay under the supervision of the AML/CFT Chief Compliance Officer and every action taken about the issue must be clearly documented. Red flag activity check list is explained in Appendix IV.

24.2 Employees and the directors of the financial institution are required by law to maintain confidentiality in respect of such investigation and any suspicious transaction report that may be filed with FRC or any other competent authority. 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 law and financing terrorists.

24.3 No criminal, civil, disciplinary or administrative proceedings for breach of banking or professional secrecy or contract shall lie against financial institutions 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 this regulation.

Regulation 25: New Products and Services

25.1 Prior to launching or using new technologies, products or services, financial institutions shall establish criteria of identifying and assessing the risks associated and take appropriate measures to manage and mitigate the ML/FT risks that may arise in relation to:

a) the development of new products and new business practices
b) the delivery mechanisms for new products and services

25.2 Financial institutions shall review of both new and pre-existing products and services on on-going basis.

Regulation: 26: Internal Control Systems, Compliance Officer and Audit

26.1 The chief compliance officer being appointed shall have appropriate experience and qualifications in the field of AML/CFT and have the authority to act independently and to report to financial institution's board of directors and FRC.

26.2 Every financial institution should provide FRC with details of their chief compliance officer, such as name, address, contact number, email address, qualifications and related training details.

26.3 The chief compliance officer and other compliance staff should have timely access to customer identification data and other CDD information, transaction records, and other relevant information.

26.4 The financial institution shall promptly inform FRC of any change in the compliance officer situation.

26.5 The internal audit and board of directors of the financial institution shall at regular intervals review the financial institution's compliance with the requirements of the Anti-Money Laundering and Proceeds of Crime Law and this Regulation.

26.6 The report from the review should be included a statement on all suspicious transactions detected, implications and measures taken by compliance staff to strengthen the financial institution's AML/CFT policies, procedures, systems and controls.

26.7 Financial institutions shall employ satisfactorily qualified and independent audit function to ensure that the chief compliance officer and staff of the financial institution are performing their duties in accordance with the financial institution's AML/CFT internal policies, procedures, systems and controls.

26.8 Financial institutions' external auditors shall report on the effectiveness of the internal control systems and include an explicit opinion on the financial institution's adherence to FRC regulations and Instructions, as well as the financial institution's adherence to its own policies, procedures, systems and controls. This report shall be made available to the FRC and CBS on request.

26.9 Financial institutions shall set up screening procedures when hiring employees. Such screening procedures should include fit and proper requirements to be applied when hiring employees.

26.10 Rigorous fit and proper requirements are required for employees in management positions or in positions perceived to have greater exposure to money laundering or terrorist financing. Employee screening procedures and fit and proper requirements must ensure that:

a) Employees have the high level of competence necessary for performing their duties as set out in their job descriptions;

b) employees have appropriate ability and integrity to conduct the business activities of the bank or financial institutions;

c) potential conflicts of interests are taken into account, including the financial background of the employee;

d) fit and proper and code of conduct requirements are defined;

e) Persons convicted of offences involving fraud, dishonesty, money laundering or other similar offences are not employed by the bank or financial institution, subject to laws of Somalia

CHAPTER SEVEN: RECORD KEEPING REQUIREMENTS, MEASURES TO COUNTER AND CONSEQUENCES

Regulation 27: Record Keeping Requirements

27.1 Financial institutions shall maintain all necessary records on transactions, including the findings of any analysis undertaken (e.g. inquiries to establish the background and purpose of unusual large transactions) for a minimum period of five years from the date of completion of the transaction.

27.2 All records of identification data obtained through CDD process (such as; copies of identification documents, KYC forms, account opening forms, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a minimum period of five years after the business relationship is ended.

27.3 All records shall be adequately documented to permit reconstruction of individual transactions including (the nature and date of the transaction, the amount and type of the currency and the type and identifying number of any account involved in the transactions so as to provide, when required, evidence for prosecution of the criminal activity.

27.4 Financial institutions shall maintain all copies of STRs sent and related documents for at least five years and for other reports and its related documents for at least five years after the date the report was sent to FRC.

27.5 Financial institutions shall satisfy any enquiry or order from the relevant competent authorities including law enforcement agencies, FRC or CBS for proving necessary information and records as per law.

27.6 Financial institutions shall, however, retain those records for longer period where transactions, customers or accounts involve litigation, or it is required by court or other competent authority.

Regulation 28: High Risk Countries

28.1 Financial institutions shall pay close attention to their subsidiaries and branches located in high risk countries as determined by FATF or CBS) and ensure that their AML/ CFT policy is observed by subsidiaries and branches in those countries.

28.2 Financial institutions are required to pay particular attention to transactions and business relationships with individuals from or in countries that have insufficient AML/CFT measures or under FATF Public Statement (high risk countries).

28.3 Financial institutions shall apply their AML/CFT policies to all of their branches and subsidiaries outside Somalia as laws and far as the law and regulations of the host country permit. In the cases where the AML/CFT measures of the host country differ from those in Somalia, the financial institutions require their overseas subsidiaries or branches to apply the higher of the two standards.

28.4 If the law and regulations of the host country, where the branch or subsidiary is situated prevent compliance with these obligations, for any reason, the financial institution shall so advise the FRC, which may take additional supervisory actions

28.5 Financial institutions are required to report any transactions with countries identified high risk countries FATF or CBS to the FRC.

Regulation 29: Compliance with AML/CFT Regulation on Asset Seizure and Confiscation

29.1 Proceeds of an offence, cash, instrumentalities of that offence, or any terrorist property can be subjected to seizure and confiscation through competent authorities as per the rules of AML/CFT Act, 2016.

29.2 Financial institutions should therefore develop and implement procedures to ensure compliance with these requirements at all times.

These requirements include but not limited to:

a) Procedures to freeze without delay funds, property, instrumentalities and assets held by the financial institution, in response to directions received from competent authorities.

b) Procedures to monitor attempted access by customers or other parties to the funds, property or assets.

c) Procedures to allow access to the funds, property or assets held in response to directions from competent authorities.

d) Funds, Proceeds of an offence, instrumentalities of that offence, or any terrorist assets in response to directions from competent authorities.

29.3 Financial institutions should submit a report to FRC without delay in relation to any attempt to access the funds, property, instrumentalities of the offence or assets which are subject to an order under this section.

Regulation 30: Maintaining Confidentiality

30.1 Financial institutions' staff and directors shall maintain confidentiality and not disclose information relating to their anti-money laundering activities to their clients or to others.

30.2 Financial institutions may share information about a customer or transactions that they have refused with other financial institutions or to their professional associations.

30.3 Financial institutions must not reveal or give hint to customer that they have filed suspicious transactions reports (STRs) about their activity.

30.4 Financial institutions are required to maintain clear signage and posters or written hand out notices to their customers that they are required to report all LCTs to the FRC. Staff may also orally advise their customer at the time the transaction is initiated.

Regulation 31: Staff Training and Awareness

31.1 Financial institutions shall implement suitable training program for their staff and management, which should be documented, in order to effectively implement the regulatory requirements and financial institutions own policies and procedures relating to AML/ CFT. Also, refresher training should be arranged at regular intervals i.e. at least annually to ensure that staff do not forget their responsibilities.

31.2 Employees training of financial institutions shall continuously and effectively update their skills and enable them to understand the new developments, money laundering and financing of terrorism techniques and methods.

31.3 Employees training shall be included real-world examples of transactions that constituted money laundering and terrorist financing, and an awareness of the role that staff play in the overall process of detecting and punishing money launderers and terrorist financers.

Regulation 32: On-site Supervision

32.1 The competent authorities' examiners shall conduct reviews of financial institutions' compliance to this regulation as part of scheduled and regular basis in accordance with the AML/CFT Act, 2016.

32.2 Any findings by the examiners that financial institution's policies, procedures and controls are inadequate or poorly implemented shall produce a rating of non-compliance, if it fails to comply with follow up recommendations of the examiners within specified time frame, shall result an enforcement action against involved financial institution.

32.3 Any financial institutions or person who deliberately hinders or objects to cooperating with the FRC or other competent authority in the lawful exercise of their powers is guilty of an offence and shall be subject to appropriate administrative, civil, or criminal fines or penalties in accordance with the AML/CFT Act ,2016.

32.4 The FRC may request necessary information such as documents and records of identification data obtained through CDD process like copies of identification documents, account opening and KYC forms.

32.5 Financial institutions shall make these documents and records available to the FRC or any enforcement agent upon request in a timely manner to ensure compliance with this regulation are met.

Regulation 33: Cooperation with Law Enforcement

33.1 Financial Institutions shall cooperate in any matters relating their AML/CFT activities, and coordinate issues regarding freezing or transferring the clients deposits according to the relevant provisions in the law and this regulation.

33.2 Financial institutions must be cooperative when they receive any request from appropriate competent authorities.

33.3 Any sort of non-cooperation in the investigation including obstructing or declining cooperation with the FRC, CBS or law enforcement authorities or declines to supply information being requested without any reasonable ground is guilty of an offence and shall be subject to appropriate administrative, civil, or criminal fines or penalties pursuant to Part VI of the Act.

Regulation 34: Penalties and Sanctions

Any natural or legal person who violates the directions mentioned in this regulation is liable to sanctions provided in Articles 27, 28 and 29 of the AML/CFT Act, 2016.

Sanctions and penalties imposed upon a legal entity or natural person can constitute any or all of the sanctions or penalties in any combination deemed appropriate based on the severity of the violations.

34.1 **(a) Penalties applicable to natural person**

Criminal penalties may be enforced against natural persons connected to the commission of the predicate offence, in addition to the following penalties for ML or TF:

a) Imprisonment for not less than a year;
b) Fines of not less than USD $1,000 or the equivalent in any currency and up to three times the amount of the money laundered;
c) Penalties may be either of the above or combination of both.

34.2 **(b)** Civil and or administrative penalties appropriate to the seriousness of the violation:

a) Fines of not less than USD $1,000 or the equivalent in any currency and up to three times the amount laundered.
b) Temporary or permanent suspension of license or authorization to operate based on registration requirements.
c) Temporary or permanent suspension from position if employed by or doing business as an independent financial institution.
d) All or any combination of the above.

34.2Penalties applicable to legal entities and the management thereof

Financial institution and their administrators or directors found to have failed to comply with this regulation, the FRC shall request it to correct the failure within an agreed period of time, in addition, law enforcement agencies may issue enforcement actions that may include but not limited to:

a) All penalties and sanctions stipulated above for natural persons.
b) Imprisonment upon officers, directors, managers or board members who neglected their responsibility for prohibiting, preventing and implementation of effective systems to detect and prevent violations.
c) Monetary penalties not less than USD $25,000 or the equivalent in any currency and not more than ten times the amount of the money laundered.

34.3 Violations to comply with ML/TF regulation which may lead to enforcement actions mentioned above include, but are not limited to:

a) Failing to set up an effective internal control system for AML/CFT activities
b) Failing to designate an effective compliance officer.
c) Failing to carry out KYC and CDD procedures appropriately.
d) Failing to maintain account information and transactions records on clients and updating the information.
e) Failing to report LCTs or STRs to the FRC, as required.
f) Intentionally or carelessly contributing in Money Laundering or Terrorist Financing.
g) Tipping off to customers that reports are being filed about them to the FRC or other competent authority.

Regulation 35: Foreign Financial Institutions Licensed in Somalia

35.1 Foreign financial institutions licensed to operate in Somalia shall cooperate and provide assistance to the anti-money laundering efforts of law enforcement agencies of the country, according to the laws of the land.

35.2 Foreign financial institutions shall abide by the provisions of laws governing anti-money laundering of the country or region where they are located.

Regulation: 36: Responsibilities of Professional Associations of Financial Institutions

36.1 Any umbrella association or organisation representing licensed banks or money transfer businesses may draft working guidelines for their members to ensure that their members are implementing AML/CFT regulations.

36.2 The professional association or organisation may discipline or suspend the membership of any financial institutions that do not comply with their working guidelines and AML/CFT regulation.

36.3 The professional association are also expected to encourage information sharing among their members concerning the details of customers or individual transactions that have been refused or denied business relationship.

APPENDIX I: POTENTIAL POLITICALLY EXPOSED PERSONS (PEPS)

PEPs are individuals who are or have been entrusted with prominent public functions both in Somalia or foreign countries and those associated with them. Examples of PEPs include, but are not limited to;	
Sr No	**Functions of potential Politically exposed person (PEPs)**
1.	Heads of State or government
2.	Ministers of State
3.	Politicians
4.	High ranking political party officials; and
5.	An artificial politically exposed person (an unnatural legal entity. belonging to a PEP)
6.	Senior public officials
7.	Senior Judicial officials
8.	Senior military officials
9.	Chief executives of state owned companies/corporations
10.	Family members or close associates of PEPs.

APPENDIX II: MINIMUM DOCUMENTS TO BE OBTAINED FROM VARIOUS TYPES OF CUSTOMERS UNDER AML/CFT REGULATIONS

Sr No	Type of Customers	Information/Documents to be obtained
1.	Individuals/ Natural person	1. Full name, Father Name including any aliases. 3. Gender. 4. National identification card or passport 5. Permanent address/ email 6. Business Name (in case of sole trader). 7. Date of birth. 8. Nationality. 9. Occupation. 10. Income and source of income. 11. Phone number 12. Photo.
2.	Sole trader/ Sole Proprietors	1. Information/Documents as per Serial No.1 above of the proprietor. 2. Business name 3. Registration certificate for registered businesses. 3. Business tax registration, where applicable. 4. Certificate or proof of membership of trade bodies etc, where applicable. 5. Declaration of sole proprietorship on business letter head. 6. Account opening application in business letter head.
3.	Partnership	1. Valid identity documentation as per Serial No. 1 above of all the partners and authorised signatories. 2. Proof of 'Partnership Deed' accordingly signed by all partners of the

		firm or business. 3. Copy of Registration Certificate with Registrar of Firms (Ministry of commerce). In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form. 4. Authority letter from all partners, in original.
4.	Limited Companies and Corporations	1. Proof of Resolution of Board of Directors for opening of account authorising the persons to open and operate the account. 2. Memorandum and Articles of Association. 3. Certificate of Incorporation if applicable. 4. Certificate of Commencement of Business, wherever applicable; 5. List of Directors the company or the corporate 6. Identity documentation as per Serial No. 1 above of all the directors and persons authorised to open and operate the account;
5.	Branch or Liaison office of Foreign Companies	7. Copy of permission letter from relevant authority like Board of Investment. 8. Copy of valid passports of all the signatories of account. 9. List of directors on company letter head 10. List of Directors the company or the corporate. 11. Documents as per Serial No. 1 above of all the directors and persons authorised to open and operate the account;
6.	Trusts, Societies and Associations etc	5. Copies of certificate of registration of Trust 6. Resolution of the Governing Body/Board of Trustees/Executive Committee authorising the person(s) to open and operate the account. 7. Copy of identity document as per Serial No. 1 above of the authorised person(s) and of the members of Governing Body/Board of Trustees /Executive Committee.
7.	Non-Governmental Organization / Non-Profit Organization / Charities (NGOs/ NPOs)	12. Name of NGO/NPO 13. Full Address, Telephone No. and email address 14. Certification of registration. 15. Constitution of the NPO. 16. Name and address of Executive committee. 17. Executive committee's decision regarding opening of account. 18. Identification documents of directors/senior officers of the NPO. 19. Authorization for the operation of accounts financial transactions. 20. Identification documents to identify the person authorized to represent the NPO in its dealings with the bank/financial institution. 21. Latest certified taxation return and related documentation. 22. The latest financial statement.

8.	Agents Accounts	1. Certification of registration. Certified copy of Agency agreement (power of attorney). 2. Photocopy of identity document as per Sr. No. 1 above of the agent. 3. The relevant documents/papers from Sr. No. 2 to 7, if agent or is not a natural person.

APPENDIX III-EXAMPLES HIGH AND LOW RISK SITUATIONS REQUIRING ENHANCED OR SIMPLIFIED CUSTOMER DUE DILIGENCE

When assessing the ML and TF risks relating to types of customers, countries or geographic areas and particular products, services, transactions or delivery channels, financial institutions can have regard to the following potentially higher risk situations that would require the application of enhanced CDD:

	Examples of High Risk Situations Requiring Enhanced CDD	
Sr No	**Types of Risk factors**	**Required Enhanced CDD**
1.	Customer	1. The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer). 2. Non-resident customers. 3. Legal persons or arrangements that manage the assets of third parties. 4. Companies that have nominee shareholders or shares in bearer form. 5. The ownership structure of the company appears unusual or with no visible economic purpose given the nature of the company's business. 7. Non face-to.-face business relationships and transactions. 8. PEPs or customers linked to PEPs. 10. High net worth customers, or whose source of income is unclear. 10. Entities and countries identified by the FRC, CBS or the FATF as of higher ML/FT risk. 11. Business relationships conducted with or in countries described in Section 10 above.
2.	Country risk factors	1. Countries classified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems. 2. Countries identified by CBS of FATF as high risk. 3. Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations. 4. Countries classified by credible sources as having significant levels of corruption or other criminal activity. 5. Countries or geographic areas classified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.
3.	Products, services, transaction or delivery channel risk factors	1. Private banking. 2. Anonymous transactions (which may include cash). 3. Accounts opened, business relationships or transactions conducted with customers that are not physically present for the purpose of identification. 4. Payment received from unknown or un-associated third parties 5. Complex trade financing products.

When assessing the ML and TF risks relating to types of customers, countries or geographic areas and particular products, services, transactions or delivery channels, financial institutions can have regard to the following potentially low risk situations that would require the application of simplified CDD:

Examples of Low Risk Situations Requiring Simplified CDD

Sr No	Types of Risk factors	Required Simplified CDD
1.	Customer	1. Financial institutions and Designated Non-Financial Businesses and Professions – where they are subject to requirements to combat money laundering and terrorism financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements. 2. Companies listed on a stock exchange and subject to disclosure requirements (either by law, or stock exchange rules or other binding Instructions or Regulations), which define requirements to ensure disclosure of beneficial ownership. 3. Public enterprises.
2.	Product, service, transaction or delivery channel	Financial products or services where there is a proven low risk of money laundering or terrorist financing which occurs in strictly limited and justified circumstances and it relates to a particular type of financial institution or activity or a financial activity is carried out by a natural or legal person on an occasional or very limited basis such that there is a low risk of money laundering and terrorist financing and that are provided to a low risk customer for financial inclusion purposes.
3.	Country	1. Countries classified by credible sources, such as mutual evaluation reports, as having effective AML/CFT systems. 2. Countries classified by credible sources as having a low level of corruption or other criminal activity.

APPENDIX IV: MONEY LAUNDERING AND TERRORIST FINANCING (RED FLAGS)

Sr. No	Scenarios	Money Laundering and Terrorist Financing (Red flags)
1.	Potential Transactions Identified as Suspicious	1. Transactions involving high-risk countries/jurisdictions vulnerable to ML. 2. Transactions involving shell banks/companies. 3. Transactions with correspondents that have been identified as higher risk. 4. LCT activity involving monetary instruments such as traveller's cheques, bank drafts, money order. 5. Transaction activity involving amounts that are just below the stipulated reporting threshold or enquiries that appear to test an institution's own internal monitoring threshold.
2.	Money Laundering Using Cash Transactions	1. Large increases in cash deposits of a customer without apparent cause, and more importantly if such deposits are subsequently transferred within a short period out of the account to a destination not normally associated with the customer. 2. Large cash transaction made by a customer whose normal business is transacted by cheques and other non-cash instruments. 3. Customers who deposit cash separately in short intervals of time such that the amount of each deposit is relatively small and the overall total is quite significant. 4. Customers whose deposits contain forged currency notes. 5. Branches of banks that tend to have far more cash transactions than usual. 6. Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.
3.	Money Laundering Using Financial Institutions	The following transactions may indicate possible money laundering, especially if they are inconsistent with a customer's legitimate business: 1. Minimal, vague or untrue information on the transaction provided by a customer that the financial institution is unable to verify. 2. unwilling to provide the required documentation for identification in support of an account opening application by a customer. 3. Customers maintaining multiple accounts at a financial institution or different financial institutions for no apparent legitimate reason. 4. Withdrawing large amounts of cash with no apparent reason or is inconsistent with the nature of the business. 5. Customers who make many deposits into accounts and soon afterwards request for electronic transfers or cash withdrawal from same accounts to other accounts. These transactions may be not consistent with the customers' legitimate business needs. 6. Unexpected increase in account activity. Typically, such an account is opened with a small amount which subsequently increases rapidly and significantly. 7. Businesses which deposit many cheques or cash into their accounts but with little or no withdrawals to meet their regular business needs. 8. Substantial cash deposits by professional customers into client or trust

		or accounts. 9. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit especially from abroad. 10. Substantial increase in deposits of cash by a professional firm or company, using client accounts or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts. 11. Large number of individuals making payments into the same account without an adequate explanation. 12. High velocity of funds that reflects the large volume of money flowing through an account. 13. An account of a licensed forex bureau (foreign exchange) that receives unusual deposits from third parties. 14. An account operated in the name of an off-shore company with structured movement of funds.
4.	Trade-Based Money Laundering	1. Over and under-invoicing of goods and services. 2. Multiple invoicing of goods and services. 3. Falsely described goods and services and where the exporter does not ship any goods at all after payments had been made. 4. Goods shipped are inconsistent with the nature of the customer's normal business and the transaction lacks an obvious economic rationale. 5. Transaction structure appears pointlessly complex and designed to obscure the true nature of the transaction. 6. Customer requests payment of proceeds to an unrelated third party. h. Considerably amended Letters of Credit (LC) without reason or changed the beneficiary or location of payment.
5.	Terrorist Financing (Red flags)	1. Persons involved in currency transactions share an address or phone number. 2. Financial transaction by a charitable non-profit organisation, for which there appears to be no link between the stated activity of the organisation and other parties in the transaction. 3. Large number of incoming or outgoing funds transfers takes place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves designated high-risk countries and territories. 4. The customer's work nature and occupation is inconsistent with the type and level of account activity. 5. The potential customer is unwilling to include the required information of the originator or the person on whose behalf the transaction is conducted. 5. Numerous personal and business accounts or the accounts of non-profit or charities organisations are used to collect and channel funds to a small number of foreign beneficiaries.
6.	Other Unusual or Suspicious Activities	1. Employee displays a lavish lifestyle that cannot be justified by his or her income or salary. 2. Employee fails to comply with standard operating guidelines of the financial institution. 3. Employee is unwilling to take his or her annual vacation. 4. Customer uses a personal account for regular business activities. 5. Official governmental business is conducted through personal account. 6. Official Embassy business is conducted through personal accounts.

		7. Embassy accounts are funded through substantial currency transactions. 8. Embassy accounts directly fund personal accounts of entities or individuals of foreign nationals with obvious reasons.

APPENDIX V: DEFINITION OF THE LEGAL WORDS

The words and terms in this Regulation have the same meaning as the AML/CFT Act, 2016 unless the subject or context otherwise requires.	
Legal terms	**Definitions of the legal words**
Beneficial owner	In relation to a customer of a bank/MTBs, means the natural persons who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes the persons who exercises ultimate effective control over a person or a body of persons whether incorporated or not.
Beneficiary	Means the person to whom or for whose benefit the funds are sent or deposited in bank or MTBs.
Beneficiary institution	Means the financial institution that receives the funds on behalf of the wire transfer or fund transfer beneficiary.
Control	In relation to a legal person, means the power to exercise a controlling influence over the management or the policies of the undertaking, and, in relation to shares, means the power to exercise a controlling influence over the voting power attached to such shares.
Correspondent bank	Means the bank in Somalia which provides correspondent banking services to bank or financial institution situated abroad and vice versa.
Correspondent banking	means provision of banking services by one bank (correspondent) to another bank (respondent) including but not limited to opening and maintaining accounts in different currencies, fund transfers, cheque clearing, payable through accounts, foreign exchanges services or similar other banking services.
Cross-border wire transfer	Means a wire transfer where the ordering institution and the beneficiary institution are located in different countries or jurisdictions.
Currency Transaction Report (CTR)	Means as defined under AML/CFT Act, 2016.
Customer	Means a person having relationship with the financial institution.
Customer due diligence (CDD)	Means Customer Due Diligence as defined in this Regulation and AML/CFT Act, 2016.
Domestic wire transfer	means any wire transfer where the originator and beneficiary institutions are located in Somalia regardless the system used to effect such wire transfer is located in another jurisdiction
Dormant or in-operative account	Means the account in which no transaction has been taken place from last one year.
FATF Recommendations	Means the Recommendations of Financial Action Task Force as amended from time to time.

Fund transfer/wire transfer	Means any transaction carried out by financial institution on behalf of originator electronically or otherwise to make an amount of money available to beneficiary at another beneficiary institution, irrespective of whether the originator and the beneficiary are the same person.
Government entity	means federal or provincial government, a ministry within such a government, a local government or an agency specially established by any such government, or a department, organization or corporation owned or controlled by such government under federal, provincial or local law.
Intermediary institution	Means an intermediary in the wire transfer payment chain; that receives and transmits a wire transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution.
Monetary threshold	Expressed in US dollars, includes a reference to the equivalent amount expressed in any other currencies.
Money laundering	Has the same meaning as ascribed to them in AML/CFT Act, 2016.
Occasional or walk-in customer	means the person conducting occasional transactions and is not a customer; having relationship with the financial institution
Occasional or One-off transaction	”means a transaction initiated by or on behalf of a person who is not a customer; having relationship with the financial institution.
Online transaction	means deposit or withdrawal of cash using different branches of a
Ordering institution	means the financial institution that initiates a wire transfer on the instructions of the wire transfer originator in transferring the funds
Originator	ans the person who allows or places the order to initiate a fund transfer/wire transfer or an online transaction;
Payable-through account	Refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.
Person	Includes natural and legal persons as described AML/CFT ACT
Politically exposed persons or PEPs	Are individuals who are entrusted with prominent public functions either domestically or by a foreign country, or in an international organization.
Respondent bank	Means the bank or financial institution outside Somalia to whom correspondent banking services in Somalia are provided and vice versa
Risk	Refers to risk associated with money laundering and financing of terrorism
Senior management	Senior management comprise persons employed by a financial institution who exercise senior management responsibilities. Senior management responsibilities mean having primary responsibility
Settlor	means a natural or legal person who transfers ownership of their assets to trustees by means of a trust deed or similar arrangement

Shell bank	means a bank that has no physical presence, in the country in which it is incorporated and licensed and/or which is not affiliated with a regulated financial service
Suspicious transaction report or STR	Means as defined under AML/CFT Act, 2016. "Threshold Reporting (Large Cash Transaction Report)" means report of the particulars of transactions (deposits, withdrawals or transfers) in excess of an amount specified in this regulation or any other applicable regulation.
Terrorist Financing	The offense as defined in AML/CFT Act, 2016.
Trustee	Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or non-professional (e.g. a person acting without reward on behalf of family)
The Law	Means AML/CFT Act, 2016

APPENDIX VI: SUSPICIOUS TRANSACTION REPORTING (STRs) FORM

	PART 1: DISCLOSING PART	
1.	**INSTITUTION NAME**	
2.	**CONTACT DETAILS OF THE HEAD OFFICE**	
	Address	
	District / Area	
	Postal	
	Telephone Number	
	Email	
3.	**ADDRESS AND CONTACT OF BRANCH** - *"where activity / transaction occurred"*	
	Address	
	District / Area	
	Postal	
	Telephone Number	
	Email	
	PART II: PERSON SUBJECT OF THE SUSPECIOUS TRANSACTION REPORT	
4.	**PERSON DETAILS**	
	Surname	
	First Name	
	Middle Name	
	Other name (s) / Aliases	
	Date of Birth	
	Place of Birth	
	Registered Address	
	Passport number	
	Nationality	
	ID number	
	Occupation	
	Name of Employer	
If the subject of the disclosure is a company, fill in the below tables		
5.	**COMPANY DETAILS**	
	Name	
	Registered Address	
	Incorporation number	
	Type of business	
If the subject of the disclosure is a trust, fill in the below tables		
6.	**TRUST DETAILS**	
	Trust name	
	Nature and purpose of the trust	
	Date of establishment	
	Identity of settler (s)	
	Identity of protector (s)	
	Beneficiary / Beneficiaries	
	PART III: ACCOUNT (S) SUBJECT OF THE SUSPECIOUS TRANSACTION REPORT	
7.	**ACCOUNT DETAILS**	
	Account number	
	Account-holder name	
	Sort / bank code	
	Account type	

	Account Balance	
	Date of account balance	
	Date Opened	
	Date Closed	
PART IV: ASSOCIATES OF THE SUBJECT OF THE DISCLOSURE		
If the subject of the disclosure has an associate, fill in the below tables		
8.	**ASSOCIATE DETAILS** *(if the associate is a Person)*	
	Surname	
	First Name	
	Middle Name	
	Other name (s) / Aliases	
	Date of Birth	
	Gender	
	Place of Birth	
	Registered Address	
	Passport number	
	Nationality	
	ID number	
	Occupation	
	Relationship to main subject	
9.	**ASSOCIATE DETAILS** *(if the associate is a Company)*	
	Name	
	Registered Address	
	Incorporation number	
	Type of business	
	Relationship to main subject	
10.	**ASSOCIATE DETAILS** *(if the associate is a Trust)*	
	Trust name	
	Nature and purpose of the trust	
	Date of establishment	
	Identity of settler (s)	
	Identity of protector (s)	
	Beneficiary / Beneficiaries	
	Relationship to main subject	
PART V: INFORMATION ABOUT SUSPICIOUS ACTIVITY OR TRANSACTION		
11.	**SUSPICIOUS ACTIVITY (SARs) OR SUSPICIOUS TRANSACTION (STRs)**	
	Date of STR / SARs	
	Type of transaction	
	Amount involved	
	Description of suspicious activity	
	Source of fund	
	Account number,	
	Account name,	
	Sort/bank code,	
	Institution name	
	Destination of the funds	
	Account number	
	Account name	
	Sort/bank code	
	Institution name	
	Basis of suspicion	
	Any actions taken	
	List of available documents	

PART VI: DETAILS OF REPORTING OFFICER

12.	**Reporting officer**	
	Full name **Position** **Signature** **Date**	