FINANCIAL INTELLIGENCE CENTER OF THE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA

FINANCIAL ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM COMPLIANCE DIRECTIVES NUMBER 01/2014

January 2014
Addis Ababa

FINANCIAL ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM COMPLIANCE DIRECTIVES NUMBER 01/2014

WHEREAS, sound know your customer policies and procedures constitute an essential part of internal control and risk management aspects of Financial Institutions;

WHEREAS, there is a need to strengthen internal control and risk management systems of Financial Institutions to prevent them from exposure to undue reputational, operational, legal and concentration risks that may result from abuse of money launderers and terrorist financiers;

WHEREAS, conducting customer due diligence is a key part of customer identification, internal control and risk management of Financial Institutions;

WHEREAS, there is a need to ensure that Financial Institutions have sound policies, procedures and controls in place that enable them to identify their new and existing customers;

Now, therefore, in accordance with Articles 6(3)(b)(1), 6(5)(e), 7, and 54(2) of Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation Number 780/2013, the Financial Intelligence Center of Ethiopia hereby issues these directives.

PART-I
GENERAL PROVISIONS

1. Short Title

These directives may be cited as "Financial Anti-Money Laundering and Countering the Financing of Terrorism Compliance Directives Number 01/2014".

2. Definitions

For the purpose of these directives, unless the context provides otherwise:

1) "Account" means a facility or an arrangement by which a financial institution :
   (a) accepts deposits of currency ;
   (b) allows withdrawals of currency or transfers into or out of the account; or
   (c) pays cheques or payment orders drawn on a financial institution or cash dealer by a person or collect cheques or payment orders on behalf of a person ; supplies a facility or an arrangement for a safe deposits box ;
2) "Applicant for Business" means the person or company seeking to establish a 'business relationship' or an occasional customer undertaking a 'one-off' transaction whose identity must be verified;
3) "Beneficiary" means a natural or legal person or any other form of legal arrangement identified by the originator as a receiver of the requested transfer, and:
   (a) In trust, a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement; and

(b) In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds where an insured event occurs, which is covered by the policy.

4) "Business relationship" means any arrangement between a financial institution and the applicant for business which purpose is to facilitate the carrying out of transactions between the parties on a frequent, habitual or regular basis ;
5) "Center" means the Financial Intelligence Center of Ethiopia.
6) "Cross-border transaction" means any transaction including wire transfer where the originator and beneficiary Operators are located in different jurisdictions at the time of initiating the transfer. This term also refers to any chain of transaction that has at least one cross-border element;
7) "Domestic transfer" means any wire transfer where the originator and beneficiary persons are located in the same jurisdiction at the time of initiating the transfer and includes any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another;
8) "Enhanced Due Diligence" means additional consideration of situations that present a higher risk of Money Laundering or Terrorist Financing including steps additional to those in customer due diligence measures which should be taken depending on the situation that is present, and includes:
   (a) Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.);
   (b) updating more regularly the identification data of customer and beneficial owner;
   (c) Obtaining additional information on the intended nature of the business relationship;
   (d) Obtaining information on the source of funds or source of wealth of the customer;
   (e) Obtaining information on the reasons for intended or performed transactions;
   (f) Obtaining the approval of senior management to commence or continue the business relationship;
   (g) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and
   (h) Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.
9) "False disclosure" means a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the disclosure or otherwise requested by competent or regulatory authorities in Ethiopia.
10) "financial institution" means a bank, an insurance company, a micro finance institution, postal savings, money transfer institution or any other institution designated as such by the National Bank pursuant to the relevant law.
11) "financing of terrorism" means the offence as defined under Article 31 of the Proclamation;
12) "High risk categories" means customers, businesses or transactions that need to be subjected to more regular reviews, particularly against the know-your-customer

information held by Financial Institutions the activity in the account. Such categories shall include, but not be limited to:

(a) Customer risk factors:
    (i) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
    (ii) non-resident customers such as those staying in the country for less than one year or those in short visit or travel;
    (iii) legal persons or arrangements such as trusts that are personal asset holding vehicles;
    (iv) Companies that have nominee shareholders or shares in bearer form;
    (v) Business that are cash-intensive;
    (vi) complex, unusual or large transactions including the ownership structure of the company appears unusual or excessively complex given the nature of the company's business; and
    (vii) Politically Exposed Persons (PEPs) and persons or companies related or close associated to them.

(b) Country or geographic risk factors:
    (i) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.
    (ii) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
    (iii) Countries identified by credible sources as having significant levels of drug production, trafficking or smuggling, corruption or other criminal activity.
    (iv) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have terrorist organizations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:
    (i) Private banking;
    (ii) Anonymous transactions (which may include cash);
    (iii) cross-border business relationships;
    (iv) wire transfers or non face-to-face business relationships or transactions; and
    (v) Payment received from unknown or un-associated third parties.

13) "Identity" generally means features which can uniquely identify a natural or legal person and includes a set of attributes such as name(s) used, date of birth and the residential address at which the customer can be located.
14) "Legal person" refers to a body corporate, foundation, partnership, non-profit organization or association, or any similar body that can establish customer relationship with a bank or other financial institution, or otherwise own property;
15) "money laundering" means the offence as defined under Article 29 of the Proclamation;
16) "One-off Transaction" means any transaction carried out other than in the course of an established business relationship.
17) "Originator" means the account holder, or where there is no account, the person (natural or legal) that places the order with the Financial Institution to perform the Financial Transaction ;

18) "Payable through account" means correspondent account that are used directly by third parties to transact business on their own behalf ;
19) "Physical presence" means meaningful mind and management located within a country. The existence simply of a local agent or low level employee does not constitute physical presence ;
20) "Politically exposed persons" (PEPs) includes:
    (a) individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of State owned corporations and political party officials and persons or companies related or close associated to them.
    (b) individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of Government, senior politicians, senior government, judicial or military officials, senior executives of State owned corporations and political party officials and persons or companies related or close associated to them; and
    (c) persons who are or have been entrusted with a prominent function by an international organization and includes members of senior management such as directors, deputy directors and members of the board or equivalent functions other than middle ranking or more junior individuals ;
21) "Private" means customer service rendered on a more personal basis than in mass-market retail banking, usually via dedicated bank advisers.
22) "Private banking" means banking, investment and other financial services provided by banks to private individuals who invest sizable assets, and does not refer to a private bank.
23) "Proclamation" means the Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No.780/2013;
24) "Risk" means the risk of money laundering, predicate offences or terrorist financing ;
25) "Senior management" means a team of executives at the highest level who have the day-to-day responsibilities of managing a financial institution as defined by each financial institution;
26) "Settlors" are persons or companies who transfer ownership of their assets to trustees by means of a trust deed.
27) "Shell bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.
28) "simplified CDD" means measures taken where the risks of money laundering or terrorist financing are lower taking into account the nature of the risk and includes:
    (a) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
    (b) Reducing the frequency of customer identification updates;
    (c) Reducing the degree of on-going monitoring and scrutinizing transactions based on monetary thresholds stipulated under the provisions of these directives; or
    (d) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but

inferring the purpose and nature from the type of transactions or business relationship established.

29) "Suspicious Transaction" means one which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering, predicate offense or terrorist financing methods and includes:
   (a) Transactions or patterns of transactions that is inconsistent with a customer's known, legitimate business or personal activities or normal business for that type of account or that lacks an obvious economic rationale;
   (b) transactions involving high-risk categories vulnerable to money laundering, predicate offenses or terrorist financing;
   (c) transactions involving shell companies ;
   (d) transactions with correspondents that have been identified as higher risk ;
   (e) transaction activity that exceed certain limits or involving amounts that are just below the stipulated reporting sum under the provisions of these Directives or enquiries that appear to test an institution's own internal monitoring or controls;
   (f) large volume of cash transactions through a business account, where there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves high- risk locations or very high account turnover inconsistent with the size of the account balance ;
   (g) large transaction activity involving monetary instruments such as traveler's cheques, bank drafts, money order, particularly those that are serially numbered ;
   (h) where persons involved in a transaction share an address or phone number; particularly when the address is also a business location or does not seem to correspond to the stated occupation, such as student, unemployed, or self-employed;
   (i) cash transaction by a nonprofit or religious organization, for which there appears to be no logical economic purpose or for which there appears to be no link between the stated activity of the organization and other parties in the transaction ;
   (j) where the stated occupation of the customer is inconsistent with the type and level of account activity ;
   (k) multiple personal and business account or the account of non-profit organizations or charities that are used to collect and channel securities to a small number of foreign beneficiaries ;
   (l) reference to the persons or entities listed in the UN lists or Ethiopian or foreign jurisdiction lists of terrorists or terrorist organizations;
   (m) failure to comply with approved operating guidelines by any person including employees of the Financial Institutions ; or
   (n) other money laundering, predicate offenses and terrorist financing indicators indicated under the provisions of these directive or identified by the Financial Institutions or approved by the Center.

30) "Trustees" include paid professionals or companies or unpaid persons who hold the assets in a trust fund separate from their own assets.

31) "Unique identifier" means any unique combination of letters, numbers or symbols that refer to a specific originator;

32) "wire transfer" refers to any transaction carried out on behalf of an originator person through a bank or other financial institution by electronic means with a view to making

an amount of money available to a beneficiary person at another bank or financial institution. The originator and the beneficiary may be the same person;

33) Each of the neuter, feminine or masculine gender(s) includes the other(s).

34) Terms which are not defined under these Directives shall have the definitions assigned to them under Article 2 of the Proclamation.

3. Scope of Application

These Directives shall apply to the activities of money laundering, predicate offenses, and financing of terrorism in Financial Institutions including money or value transfer providers and operating in Ethiopia.

PART-II
INSTITUTIONAL POLICY FRAMEWORK AND INTERNAL COMPLIANCE PROGRAMS

4. Internal Policies, Controls and Procedures

1) Financial Institutions shall:

(a) establish, implement, monitor, and maintain, an effective program of compliance with the requirements of the Proclamation and other related laws;

(b) adopt written policy framework stating their commitment to comply with Anti–Money Laundering and Countering the Financing of Terrorism (AML/CFT) obligations under any law to actively prevent any transaction that facilitates criminal activities by enabling their employees to monitor, recognize, detect and respond appropriately to suspicious transactions, the CDD, record retention, and the reporting obligation;

(c) formulate and implement internal controls and other procedures that will deter criminals from using its facilities for money laundering and terrorist financing and to ensure that its obligations under subsisting laws are met in accordance with Article 11 of the Proclamation and the provisions of these Directives;

(d) screening procedures to ensure high standards when hiring employees;

(e) designate Compliance Officer at a senior management level and employ other appropriate employees with the relevant competence, authority and independence to implement the institution's AML/CFT compliance program in accordance with Article 11(3) of the Proclamation;

(f) designate adequately resourced and independent audit function to test compliance with the procedures, policies and controls in accordance with Article 11(2)(f) of the Proclamation;

(g) allocate sufficient resources for the proper functioning of AML/CFT compliance;

(h) establish an ongoing employee awareness and training program to ensure that employees are kept informed of new developments, including information on current AML/CFT techniques, methods and trends; and that there is a clear explanation of all aspects of AML/ CFT laws and obligations in Accordance with Article 42 of these Directives; and

(i) ensure that relevant policies, procedures, processes and controls are communicated to all relevant employees.

2) Financial Institutions shall render quarterly returns on their level of compliance to the Center in accordance with Article 11 of these Directives.

3) Financial Institutions shall ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the requirements of the Proclamation, these Directives and other relevant laws, where the minimum AML/CFT requirements of the host country are less strict than provisions of the Proclamation, these Directives and other relevant laws, to the extent that host country laws and regulations permit.
4) If the host country does not permit the proper implementation of AML/CFT measures consistent with the provisions of the Proclamation, these Directives and other relevant laws, Financial Institutions shall apply appropriate additional measures in accordance with the provisions of the Proclamation, these Directives and other relevant laws to manage the money laundering, predicate offenses and financing of terrorism risks, and inform the same to the Center.

5. Compliance Management Arrangements

1) The Board of Financial Institutions shall ensure that a program of compliance with the Proclamation, these directives and other subsisting laws.
2) The duties of a Compliance Officer under Article 4(1)(e) of these Directives shall include but not limited to:
   (a) developing an AML/CFT Compliance Program ;
   (b) rendering returns on mandatory disclosure and the monitoring of suspicious transactions including receiving, vetting from employee, and reporting suspicious transaction reports to the Center ;
   (c) rendering returns on Foreign Exchange Transactions to the Center ;
   (d) conducting regular and internal supervision to ensure compliance and rendering reports on similar matters to the Center;
   (e) coordinating the training of employee in AML/CFT awareness, detection methods and reporting requirements ;
   (f) serving as liaison officer to the Center and competent and regulatory authorities; and
   (g) serving as a point of contact for all employees of the Financial Institutions on issues relating to money laundering and terrorist financing.
3) Financial Institutions shall make appropriate provisions for any absence of the compliance officer and shall appoint a suitable deputy to assume the responsibilities set out under Sub-article (2) of this Article.
4) The compliance officer shall be sufficiently senior and independent to act on his own authority, have direct access to senior management, and has sufficient resources including offices, and appropriately trained and effective employees.
5) The compliance officer shall have access to relevant information concerning customers, representatives of the customers, business relationships and transactions and the details of such transactions which the financial institution enters into, or considers entering into, with or for a customer or other party.
6) Financial Institutions shall commission an annual report from its compliance officer which shall report the level of compliance adherence to relevant policies, procedures, processes and controls with respect to regulatory obligations.

6. Risk Assessment

Financial Institutions shall take appropriate steps to identify, assess, and understand their money laundering and terrorist financing risks. This includes but not limited to:

(i) document their risk assessments;

(ii) consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

(iii)keep these assessments up to date; and

(iv)have appropriate mechanisms to provide risk assessment information to the Center.

7. New Technologies

1) Financial Institutions shall identify and assess the money laundering or terrorist financing risks that may arise in relation to:
   (a) the development of new products and new business practices, including new delivery mechanisms; and
   (b) the use of new or developing technologies for both new and pre-existing products.
2) Financial Institutions shall put in place:
   (a) policies or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes such as internationally accepted Credit or Debit Cards ; and
   (b) policies and procedures to address any specific risks associated with non-face to face business relationships or transactions in accordance with Article 21 of these Directives.
3) These policies and procedures shall be applied automatically when establishing customers' relationships and conducting ongoing due diligence,
4) Risk assessment shall take place prior to the launch of such new products, business practices or the use of new or developing technologies, and Financial Institutions shall take appropriate measures to manage and mitigate those risks in accordance with Article 6 of these Directives.

8. Additional Areas of Risks

1) Financial Institutions shall review, identify and record other areas of potential money laundering, predicate offences and terrorist financing risks not covered by these directives and report same quarterly to the Center.
2) Financial Institutions shall review their AML/CFT frameworks from time to time with a view to determining their adequacy and identifying other areas of potential risks not covered by these Directives.

9. Risk Mitigations

Financial Institutions shall:

(a) have policies, controls, manuals and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified either by the center or by the financial institution business or profession;

(b) monitor the implementation of those controls policies, controls, manuals and procedures and to enhance them if necessary; and

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

10. Board Approval of the AML/CFT Compliance Program

1) Financial Institutions shall have a comprehensive AML/CFT compliance program including Manuals, Policies, Controls and Procedures to guide their compliance efforts and to ensure the diligent implementation of their program.
2) The Board of Directors of a Financial Institution shall ensure that programs under Sub-article 1 of this Article are formulated and presented to the Board for consideration and formal approval.
3) The Compliance Manuals, policies, controls, and procedures formulated and approved by the Board shall be forwarded to the Center for consideration and necessary action within one month of their release.

11. Testing for the Adequacy of Compliance

1) Financial Institutions shall make a policy commitment and subject their AML/CFT Compliance Program to independent-testing to determine their adequacy, completeness and effectiveness, and quarterly reports on their AML/CFT compliance status shall be presented to their Board and the Center for their information and necessary action.
2) Any identified weaknesses or inadequacies shall be promptly addressed by financial institution.

12. Cooperation with Competent Authorities

1) Financial Institutions shall comply promptly with all the requests made pursuant to the Proclamation and subsisting laws and directives and shall provide relevant information to the Center and other authorities on AML/CFT matters.
2) Where there is a request for information on money laundering, predicate offences and terrorist financing, Financial Institutions shall:
   (a) search immediately and without delay but not later than 24 hours the institution's records and electronic data-base to determine whether it maintains or has maintained any account for or has engaged in any transaction with any individual, entity or organization named in the request ;
   (b) report promptly to the Center the outcome of the search ; and
   (c) protect the security and confidentiality of such requests.
3) The Director General of the Center may modify the time specified under Sub-Article (2) (a) of this Article by issuing circulars based on the circumstances of the case.

13. Secrecy and Confidentiality Law

Secrecy and confidentiality laws of Financial Institutions shall not inhibit the implementation of the requirements of these Directives in view of the provisions in the Proclamation and other relevant subsisting laws and in giving the Competent Authorities, either domestically or internationally, power to access information to properly perform their functions in combating money laundering and financing of terrorism.

14. Anonymous and Numbered Account

A Financial Institution shall not keep anonymous account in fictitious names including numbered account**;** and where nominee account are maintained, details of the beneficial owners shall be provided on request.

PART-III
KNOW YOUR CUSTOMER (KYC) AND IDENTIFICATION PROCEDURES

15. General Principles

1) Subject to Article 24 of these Directives, Financial Institutions shall take a risk-based approach to the 'Know Your Customer' requirement and identify all their customers whether permanent or occasional, and whether natural or legal person or legal arrangement and verify their identities using reliable, independently sourced documents up-to-date data or information including government and third parties in accordance with Article 35 of these Directives.
2) Financial Institutions shall not establish a business relationship until all relevant parties to the relationship have been identified and the nature of the business they intend to conduct ascertained; and once an on-going business relationship is established, any inconsistent activity shall then be examined to determine whether or not there is an element of money laundering or terrorism financing.
3) In carrying out transactions with any customer, Financial Institutions shall identify the ultimate beneficial owner and take reasonable measures to verify the identity of the beneficial owner using relevant information or data obtained from a reliable source such that the financial institution is satisfied that it knows who the beneficial owner is.
4) Financial Institutions shall in respect of all customers, determine whether a customer is acting on behalf of another person; and where the customer is acting on behalf of another person, they shall take reasonable steps to obtain sufficient identification data and to verify the identity of that other person.
5) The establishment of identity under these Directives shall be in the following broad categories of customer:
   (a) Natural Person Customers ; or
   (b) Customers that are Legal Persons or Legal Arrangements.

16. Natural Person Customers

1) The following information shall be established and independently validated for all natural persons whose identities need to be verified as they are required by competent authorities which are the:
   (a) given or legal name and all other names used;
   (b) permanent address;
   (c) telephone number, fax number and e-mail address, if available;
   (d) date and place of birth, if possible;
   (e) nationality;
   (f) occupation, public position held and/or name of employer;
   (g) type of account; and
   (h) signed statement certifying accuracy of the information provided.
2) The extent and number of checks can vary depending on the perceived risk of the service or business sought and whether the application is made in person or through a remote medium such as telephone, post or the internet.
3) For personal account relationships, all joint-account holders need to be verified.

17. Customers that are Legal Persons or Arrangements

1) For customers that are legal persons and arrangements, Financial Institutions shall verify the status of the legal person by obtaining proof of incorporation from the relevant authority or similar evidence of establishment or existence and any other relevant information.
2) For these customers, Financial Institutions shall:
   (a) take reasonable measures to understand the ownership and control structure of the customer and determine who the natural persons that ultimately own or control the legal person or arrangement are; this shall include those natural persons who exercise ultimate effective control over the legal person or arrangement;
   (b) verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person;
   (c) verify the legal status of the customer at a minimum by obtaining proof of incorporation or similar evidence of establishment or existence and information concerning the legal person's or arrangement's:
      (i) name,
      (ii) legal form and proof of existence,
      (iii) some form of official identification number such as tax identification number (if available),
      (iv) address which includes country, city/town/wereda/kebele in which the head office is located and if available, house number, mailing address, telephone number and fax number,
      (v) the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position including directors, if applicable, and the chief executive officer in the legal person or arrangement;
      (vi) the resolution of the board of directors (if applicable) or any other authorized body or person to open an account;
      (vii) to the extent that there is doubt under (i) and (ii) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and
      (viii) identification of those who have authority to operate the account.
3) For the proper implementation of Article 5 of the Proclamation and the provisions of these Directives, legal persons shall:
   (a) take reasonable measures to obtain and maintain their name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers, a list of directors, a register of their shareholders or members, containing the number of shares held by each shareholder and categories of shares (including the nature of the associated voting rights), their beneficial owners;
   (b) use existing information, including:
      (i) information obtained by Financial Institutions in accordance with Articles 25, 26 and 27 of these Directives;
      (ii) information held by other competent authorities on the legal and beneficial ownership of companies;

(iii) information held by the legal person as required in Sub-Article 3(a) of this Article; and

(iv) available information on companies listed on a stock exchange,

where disclosure requirements ensure adequate transparency of beneficial ownership;

(c) require shareholders with a controlling interest of bearer share or share warrants to notify such entity, and the legal person to record their identity;

(d) require nominee shareholders and directors to disclose the identity of their nominator to such entity and to any relevant registry, and for this information to be included in the relevant register;

(e) authorize one or more natural persons or a designated non financial business or profession resident in Ethiopia to be accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities;

(f) ensure that information obtained and maintained under Sub-Articles 7(a) - (c) of this Article is kept accurate and updated on a timely basis;

(g) maintain the information and records referred to by the entity itself (or its administrators, liquidators or other persons involved in the dissolution of the company), for at least ten years after the date on which the entity is dissolved or otherwise ceases to exist, or after the date on which the company ceases to be a customer of the financial institution business or profession; and

(h) take other comparable measures, specifically identified by the Center.

4) In the case of Trusts or other types of legal arrangements, Financial Institutions shall obtain and verify the identity of those providing funds for the Trust including the settler and those who are authorized to invest, transfer funds or make decisions on behalf of the Trust such as the principal trustees and controllers who have power to remove the Trustees, the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership) or persons in equivalent or similar positions.

5) For the proper implementation of Article 6(5)(c) of the Proclamation and the provisions of these Directives, legal arrangements shall:

(a) obtain and hold adequate, accurate, and current information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust;

(b) hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors; and

(c) professional trustees to maintain this information for at least ten years after their involvement with the trust ceases;

(d) ensure that information obtained and maintained under Sub-Articles 5(a) - (c) of this Article is kept accurate and updated on a timely basis;

(e) disclose their status to the Center or other competent authorities or Financial Institutions on a timely basis when forming a business relationship or carrying out an occasional transaction above the threshold indicated under the provisions of these Directives;

(f) provide competent authorities with any information relating to the trust; or provide Financial Institutions, upon request, with information on the beneficial ownership, control of the trust, the residence of the trustee and the assets of the trust to be held or

managed under the terms of the business relationship or for which they undertake an occasional transaction.

18. Duty to Obtain Identification Evidence

1) Financial Institutions shall ensure that they are dealing with a real person or organization, natural, corporate or legal, by obtaining sufficient identification evidence, and the requirement in all cases is to obtain satisfactory evidence that a person of that name lives at the address given and that the applicant is that person or that the company has identifiable owners and that its representatives can be located at the address provided.
2) While considering proposals for extending facilities, financial institutions shall make all reasonable efforts to determine the true identity of their customers and shall develop and implement effective procedures and methods for the purpose.
3) Subject to the provisions of these Directives, Financial Institutions shall:
   (a) obtain identification evidence after they have contact with a customer with a view to agreeing with the customer to carry out an initial transaction; or reaching an understanding, whether binding or not, with the customer that it may carry out future transactions ; and
   (b) where the customer does not supply the required information as stipulated in Sub-Article (a) of this Sub-Article, Financial Institutions shall discontinue any activity it is conducting for the customer ; and bring to an end any understanding reached with the customer.
4) Notwithstanding the Sub-article 3 of this Article, a financial institution may however start processing the business or application immediately, provided that it:
   (a) promptly takes appropriate steps to obtain identification evidence; and
   (b) does not transfer or pay any money out to a third party until the identification requirements have been satisfied.
5) Savings Schemes and Investments in Third Parties' names such as when an investor sets up a savings account or a regular savings scheme whereby the funds are supplied by one person for investment in the name of another (such as a spouse or a child), the person who funds the subscription or makes deposits into the savings scheme shall be regarded as the applicant for business for whom identification evidence must be obtained in addition to the legal owner.
6) In the case of Personal Pension Schemes identification evidence shall be obtained at the outset for all investors, except personal pensions connected to a policy of insurance taken out by virtue of a contract of employment or pension scheme; and personal pension advisers are charged with the responsibility of obtaining the identification evidence on behalf of the pension fund provider.
7) Financial Institution shall put in place written and consistent policies of closing an account or unwinding a transaction where satisfactory evidence of identity cannot be obtained and ensure that the identification processes is cumulative considering that no single form of identification can be fully guaranteed as genuine or representing correct identity, and the procedures adopted to verify the identity of private individuals, whether identification was done face-to-face or remotely, shall be fully stated in the customer's file.

8) The identification evidence collected at the outset shall be viewed against the inherent risks in the business or service and shall include a set of attributes such as names used, date of birth and the residential address at which the customer can be located.
9) The failure or refusal by an applicant to provide satisfactory identification evidence within a reasonable time-frame without adequate explanation and single or multiple fictitious applications, substitution, or fraudulent impersonation shall lead to suspicion in accordance with the provisions of these Directives that the customer is engaged in money laundering, predicate offenses or terrorist financing and Financial Institutions shall make Suspicious Transactions Reports to the Center based on the information in their possession before the funds involved are returned to the potential customer or where they came from.
10) The reasonable steps taken to avoid the situations under Sub-article 8 of this Article shall be stated by the Financial institution in the customer's file and an introduction from a respected customer or a person personally known to a Director, Manager or a member of staff which often provides comfort, must not replace compliance with identification evidence requirements set out under these Directives.

19. Identification Procedure

1) While gathering identification evidences, no single form of identification can be fully guaranteed as genuine or representing correct identity and the identification process shall therefore be cumulative.
2) Finance Institutions shall *inter alia* obtain copies of National Identity Card or Passport or Driving license etc. of the customer which shall be stamped as "original seen" by employee of the financial institution.
3) Before extending deposit services customers who are legal persons or arrangements, financial institutions shall obtain Memorandum and Articles of Association and Board Resolution etc. which shall be stamped as "original seen" by employee of the financial institution.
4) Notwithstanding Sub-article (1) of this Article, in far-flung and remote areas where people do not have identity cards, micro finance institutions may extend micro-credit by establishing identity through other appropriate means.
5) Where an international passport, driving license or identity card is taken as evidence of identity, the number, date and place or country of issue as well as expiry date are required to be recorded.
6) Financial Institutions may however start processing the transaction or application immediately, provided that they promptly take appropriate steps to obtain identification evidence and do not transfer or pay any money out to a third party until the identification requirements have been satisfied.
7) Details of the person who initiated and authorized the introduction shall be kept in the customer's mandate file along with other records.
8) Once identification procedures have been satisfactorily completed and the business relationship established, as long as contact or activity is maintained and records concerning that customer are complete and kept, no further evidence of identity is needed when another transaction or activity is subsequently undertaken.
9) Under this Article, "*transaction*" includes the giving of advice and the **"**advice" here does not apply to when information is provided about the availability of products or services

nor applies to when a first interview/discussion prior to establishing a relationship takes place.

10) The procedures adopted to verify the identity of private individuals and whether or not identification was done face to face or remotely shall be stated in the customer's file.
11) An introduction from a respected customer, a person personally known to a Director or Manager or a member of staff shall not replace the need for identification evidence requirements to be complied with as set out in the Directives and details of the person who initiated and authorized the introduction shall be kept in the customer's mandate file along with other records.

20. Timing of Verification

1) An acceptable time-span for obtaining satisfactory evidence of identity shall be determined by the nature of the business, the geographical location of the parties and whether it is possible to obtain the evidence before commitments are entered into or money changes hands but any occasion when business is conducted before satisfactory evidence of identity has been obtained shall be exceptional and shall only be those circumstances justified with regard to the risk.
2) Financial Institutions shall verify the identity of the customer, beneficial-owner and occasional customers before or during the course of establishing a business relationship or conducting transactions for occasional customers or when series of linked transactions take place.
3) Notwithstanding Sub-article (2) of this Article, Financial Institutions may complete the verification of the identity of the customer and beneficial owner following the establishment of the business relationship where:
   (a) it shall take place as soon as reasonably practicable ;
   (b) it is essential not to interrupt the normal business conduct of the customer ; and
   (c) the money laundering and terrorism financing risks can be effectively managed.
4) The persons whose identity are required to be verified include customers and persons acting on behalf of another provided that there is no obligation to look beyond the customer where:
   (a) he is acting on his own account rather than for a specific customer or group of customers ;
   (b) a customer is a regulated financial institution profession or business; and
   (c) the business is to be undertaken in the name of a regulated Financial Institution.
5) In other circumstances, except the customer is a regulated Financial institution or financial institution acting as agent on behalf of one or more underlying customers within Ethiopia and has given written assurance that it has obtained the recorded-evidence of identity to the required standards, identification evidence shall be verified on:
   (a) the named account holder and person in whose name an investment is registered ;
   (b) any principal beneficial owner of funds being invested who is not the account holder or named investor ;
   (c) the principal controller(s) of an account or business relationship (such as those who regularly provide instructions) ; and
   (d) any intermediate parties (such as where an account is managed or owned by an intermediary).

6) Normal conduct of business may not be interrupted in cases such as:
   (a) securities transactions where the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them and the performance of the transaction may be required before verification of identity is completed;
   (b) non face-to-face business, and
   (c) life insurance business in relation to identification and verification of the beneficiary under the policy which may take place after the business relationship with the policy holder is established.
7) In all such cases listed under Sub-article (3) of this Article, identification and verification shall occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.
8) Where a customer is permitted to utilize the business relationship before verification, Financial Institutions shall adopt risk management procedures concerning the conditions under which this may occur and these procedures shall include but not limited to a set of measures such as:
   (a) types and amount of transactions that can be performed, and
   (b) the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

21. New Business Relation by an Existing Customer

1) Where an existing customer closes one account and opens another or enters into a new agreement to purchase products or services, there is no need to verify the identity or address of such a customer except where the name or the address provided does not tally with the information in the Financial Institution's file.
2) Procedures shall be put in place by Financial Institutions to guard against impersonation and fraud and the opportunity of opening the new account shall also be taken to ask the customer to confirm the relevant details and to provide any missing KYC information especially where:
   (a) there was an existing business relationship with the customer and identification evidence had not previously been obtained ; or
   (b) there had been no recent contact or correspondence with the customer within the past six months; or
   (c) a previously dormant account is re-activated.
3) Notwithstanding the provisions of Sub-article (1) of this Article, the previous account and any identification evidence previously obtained or any introduction records shall be linked to the new account records and retained for the prescribed period in accordance with the provisions of these Directives.

22. Non Face-to-Face Transaction

1) When conducting "non-face-to-face" business with clients that have not been physically present for the purposes of identification and verification, Financial Institutions shall have policies, procedures, systems and controls in place to manage specific risks associated with such "non-face to face" business, relationships or transactions.
2) Financial Institutions shall at a minimum require two pieces of formal identification which have been certified appropriately by a notary public or court of competent jurisdiction, senior public servant or their equivalent in the private sector shall be

obtained and a person undertaking the certification must be known and capable of being contacted, and one formal document that will verify the physical address of the client.

3) Where the client is a legal person or arrangement, Financial Institutions shall require documentary evidence of the existence of the legal person and a certified copy of acceptable identification and address documentation to verify the address of any person defined in Article 17 of these Directives.
4) In order to guard against the dangers of postal-interception and fraud, prospective customers shall not be asked to send by post originals of their valuable personal identity documents such as international passport, identity card or driver's license.
5) In the case of foreign nationals, the copy of international passport, national identity card or documentary evidence of his address shall be certified by:
   (a) the embassy, consulate or high commission of the country of issue;
   (b) a senior official within the account opening institution;
   (c) notary Public or Court of competent jurisdiction, or
   (d) copies of identification evidence stamped, dated and signed "original sighted by me" by a senior officer of the Financial Institution.
6) Financial Institutions shall always ensure that a good production of the photographic evidence of identity is obtained and where this is not possible, a copy of evidence certified as providing a good likeness of the applicant could only be acceptable in the interim.
7) When conducting "non-face-to-face" business, Financial Institutions shall require at a minimum that the first payment received from the non face-to-face customer is carried out through an account in the customer's name with a financial institution which is subject to internationally recognized AML/CFT standards.
8) Financial Institutions shall ensure that adequate procedures for monitoring activity of "non-face to face" business are implemented and managed effectively.

23. Recording Identification Evidence

1) Unless otherwise a higher time span is provided by other subsisting laws in Ethiopia, records of the supporting evidence and methods used to verify identity are required to be retained for a minimum period of ten years after the account is closed or the business relationship ended in Accordance with Article 42 of these Directives.
2) Where the supporting evidence could not be copied at the time it was presented, the reference numbers and other relevant details of the identification evidence are required to be recorded to enable the documents to be obtained later.
3) Confirmation shall be provided and the original documents shall be seen by certifying either on the photocopies or on the record that the details were taken down as evidence.
4) Where checks are made electronically, a record of the actual information obtained or of where it can be re-obtained shall be retained as part of the identification evidence and such records will make the reproduction of the actual information that would have been obtained before, less cumbersome.

24. Concession in Respect of Payment Made by Post

1) Where the money laundering, predicate offense or terrorist financing risk is considered to be low, concession may be granted for product or services in respect of long-term life insurance business or purchase of personal investment products and where payment is to

be made from an account held in the customers' name, or jointly with one or more other persons, at a regulated Financial Institution, no further evidence of identity is necessary.

2) Waiver of additional verification requirements for postal or electronic transactions shall not apply to:
   (a) products or account where funds can be transferred to other types of products or account which provide cheque or money transfer facilities;
   (b) situations where funds can be repaid or transferred to a person other than the original customers ; and
   (c) investments where the characteristics of the product or account may change subsequently to enable payments to be made to third parties.
3) Postal concession is not an exemption from the requirement to obtain satisfactory evidence of a customer identity.
4) Payment debited from an account in the customer's name shall be capable of constituting the required identification evidence in its own right.
5) Financial Institutions shall maintain records for a minimum period of ten years after the account is closed or the business relationship ended indicating how a transaction arose, including the details of its branch and account number from which the cheque or payment is drawn.
6) The concession shall apply to where an application is made directly to the Financial Institution and where a payment is passed through a regulated intermediary.

25. Exemptions

1) Identification of a customer does not need to be verified where the customer is itself a regulated bank or other financial institution that is subject to anti-money laundering and combating terrorist financing obligations.
2) Where the customer or owner of the controlling interest is a public enterprise established in Ethiopia, it is not necessary to identify and verify the identity of the shareholders of such an enterprise.

PART-IV
CUSTOMER DUE DILIGENCE (CDD) MEASURES

26. CDD Measures by Financial Institutions

1) Financial Institutions shall:
   (a) carry out the full range of the CDD measures on a risk sensitive-basis in accordance with Article 6(5) of the Proclamation and as provided for in these Directives;
   (b) determine in each case if the risks are lower or not, depending on the type of customer product, transaction or location of the customer; and
   (c) understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship including the expected or predictable pattern of transactions.
2) Financial Institutions shall undertake Customer Due Diligence (CDD) measures when:
   (a) business relationship is established ;
   (b) carrying out occasional cash transaction with a customer, which at a minimum exceeds Birr 300,000, USD 15,000 or equivalent in other foreign currencies or such other thresholds as may be determined by the Center from time to time, subject to the

Proclamation; this shall include situations where the transaction is carried out in a single operation or in several operations that appear to be linked or structured;

(c) carrying out occasional transactions that are wire transfers, including those applicable to cross-border and domestic transfers between Financial Institutions when credit or debit cards are used as a payment system to effect money transfer which at a minimum exceeds Birr 20,000, USD 1,000 or equivalent in other foreign currencies or such other thresholds as may be determined by the Center from time to time, subject to Article 8 of the Proclamation and Articles 34 and 40 of these Directives;

(d) there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or any other sum referred to in these directives; or

(e) there are doubts about the veracity or adequacy of previously obtained customers identification data;

provided that, a financial institution shall not be required to repeatedly perform identification and verification exercise every time a customer conducts a transaction, unless the institution suspects that there is a change in the documents earlier provided.

3) If the amount of the transaction referred to in Sub-article (2)(b)and (c) of this Article is unknown at the time of the operation, the identification of customer shall be done as soon as the amount becomes known or tilt threshold is reached.

27. CDD for Beneficiaries of Life Insurance Policies

1) For life or other investment-related insurance business, Financial Institutions shall, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/:
   (a) For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements, taking the name of the person;
   (b) For beneficiary(ies) that are by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will), obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.
2) The information collected under (a) and/or (b) of Sub-article 1 of this Article shall be recorded and maintained in accordance with the provisions of the Proclamation and these Directives.
3) For both the cases referred to in under (a) and (b) of Sub-article 1 of this Article, the verification of the identity of the beneficiary(ies) shall occur at the time of the payout.
4) The beneficiary of a life insurance policy shall be included as a relevant risk factor by the Financial Institution in determining whether enhanced CDD measures are applicable.
5) If the Financial Institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it shall take enhanced measures which include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.
6) Where a financial institution is unable to comply with Sub-articles 1 to 3 of this Article, it shall make a suspicious transaction report to the Center.

28. On-going Due Diligence

1) Financial Institutions shall conduct ongoing due diligence on a business relationship.

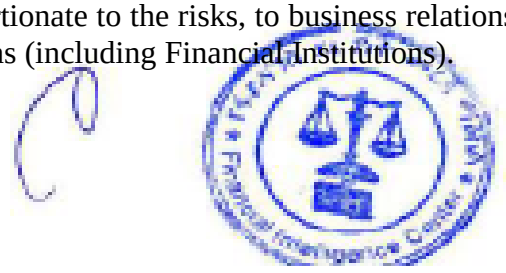
2) The ongoing due diligence measures under Sub-Article (1) of this Article includes:
   (a) scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the financial institution's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and
   (b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.
3) For customers that may require additional caution to be exercised when transacting with them, activities in such customer's account shall be monitored on a regular basis for suspicious transactions.
4) Financial Institutions shall refuse to do business with the customer referred to in Sub-Article (2) of this Article or automatically classify them as high risk and subject them to an enhanced customer due diligence.
5) Financial Institutions shall consider reclassifying a customer as higher risk and file a suspicious transaction report to the Center if following its initial acceptance of the customers the pattern of account activity of the customer does not fit in with their knowledge of the customer in accordance with Article 17 of the Proclamation and provisions stipulated under Part V of these Directives.

29. Application of CDD to Existing Customers

1) Financial Institutions shall apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.
2) The appropriate time to conduct CDD by a Financial Institution includes where:
   (a) a transaction of significant value takes place ;
   (b) customers documentation standards change substantially ;
   (c) there is a material change in the way that the account is operated ; and
   (d) the institution becomes aware that it lacks sufficient information about an existing customer.
3) A Financial Institution shall properly identify the customers in accordance with the provision of the Proclamation and these Directives; and the customers' identification records shall be made available to the compliance officer, other appropriate employee and relevant authorities.

30. Application of Enhanced Customer Due Diligence

1) Financial Institutions shall adopt enhanced CDD measures whenever there is suspicion of money laundering and terrorism financing or for higher risk categories of customers, countries or geographic areas, and particular products, services, transactions or delivery channels in accordance with the provisions of these Directives.
2) Financial Institutions shall exercise greater caution when approving the opening of account or conducting transactions for high risk customers.
3) The type of enhanced due diligence measures applied by Financial Institutions under these Directives shall be effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including Financial Institutions).

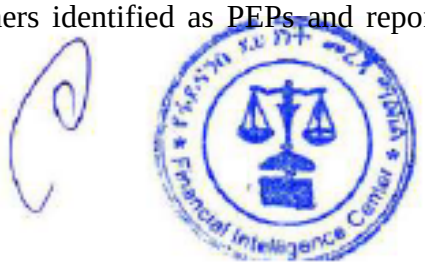


31. Lower Risk Categories of Customers

1) Without prejudice to Article 19 of these directives, simplified CDD process may be adopted for lower risk categories of customers, business relationships or transactions commensurate with the lower risk factors and identified through an adequate analysis of risks by the financial institution.
2) For the purpose of Sub-article 1 of this Article, Financial Institutions may consider the following as categories of low risk customers:
   (a) Financial Institutions, provided they are subject to requirements for the combat of money laundering and terrorist financing which are consistent with the provisions of these Directives and are supervised for compliance ;
   (b) public enterprises established in Ethiopia or similar situations that are subject to regulatory disclosure requirements ;
   (c) Government ministries, departments, parastatals and agencies ;
   (d) insurance policies for pension schemes where there is no surrender value clause and the policy cannot be used as collateral ;
   (e) a pension, super annuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme ; and
   (f) beneficial-owners of pooled-account held by designated non financial businesses and professions (DNFBPs) provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the provisions of the Proclamation and other laws including these Directives and have been so certified by their regulators or self-regulatory organizations.
   (g) Such other categories as approved by the Center identified through an adequate analysis of risks and concerns about strengths or weaknesses in the AML/CFT systems of other countries.

32. Determination of a Politically Exposed Person

1) Financial Institutions shall, in addition to performing CDD measures in accordance with the provisions of the Proclamation and these directives, put in place appropriate risk management systems to determine whether a potential customer or existing customers or the beneficial-owner is a Politically Exposed Person (PEP).
2) Financial Institutions established in a form of artificial persons shall obtain senior management approval before they establish business relationships with PEPs and render monthly returns on their transactions with PEPs to the Center in addition to its regular activities on rendering suspicious and cash transaction reports.
3) Where a customer has been accepted or has an ongoing relationship with the Financial institution and the customer or beneficial-owner is subsequently found to be or becomes PEP, in order to continue the business relationship, they shall obtain approval pursuant to Sub-articles (2) and (3) of this Article.
4) Financial Institutions shall take enhanced CDD measures pursuant to Article 6(8) of the Proclamation and Article 19 of these Directives, to establish the source of wealth and the sources of funds of customers and beneficial owners identified as PEPs and report all suspicious transactions immediately to the Center.



5) Financial Institutions in a business relationship with PEPs shall conduct enhanced ongoing monitoring of that relationship and in the event of any transaction that is unusual; they shall flag the account and report the suspicion immediately to the Center.
6) In relation to life insurance policies, Financial Institutions shall take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs, at the latest, at the time of the payout.
7) Where higher risks are identified, Financial Institutions shall inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a suspicious transaction report.

33. Correspondent Banking

1) With respect to correspondent banking and other similar relationships, Financial Institutions, in addition to performing CDD measures, shall:
   (a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
   (b) assess the respondent institution's anti-money laundering and combating terrorist financing controls, and ascertain that they are adequate and effective;
   (c) obtain approval from a senior management member of the bank before establishing new correspondent relationships; and
   (d) clearly understand and document the anti-money laundering and combating terrorist financing responsibilities of each institution;
2) Where a correspondent relationship involves the maintenance of "payable through account", Financial Institutions shall satisfy themselves that:
   (a) their respondent financial institution has performed all the CDD obligations set out in these directives on those of its customers that have direct access to the account of the correspondent financial institution; and
   (b) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.
3) Where a correspondent financial institution fails to comply with national anti-money laundering and combating terrorist financing laws, Financial Institutions shall:
   (i) not open an account, commence business relations or perform transaction;
   (ii) terminate the business relationship with such correspondent Financial Institutions; and
   (iii) consider making a suspicious transaction report to the Center in relation to correspondent Financial Institutions.

34. Correspondent Relationships with Shell Banks

1) Financial Institutions shall not create, operate, manage, or facilitate activity for or on behalf of a shell bank or entering into, or continuing, correspondent banking relationships with such banks in Ethiopia.

2) Financial Institutions shall take all necessary measures to satisfy themselves that a correspondent Financial Institution in a foreign country does not permit its account to be used by shell banks.

35. Wire Transfers

1) Financial Institutions including intermediary Financial Institutions, money or value transfer service operators shall include the required and accurate originator and beneficiary information, on wire transfers and related messages, and ensure that the information remains with the wire transfer or related message throughout the payment chain.
2) For domestic transfer of Birr 20,000 or cross-border wire transfers of USD 1000 or any equivalent foreign currency or more, Financial Institutions, including intermediary Financial Institutions, money or value transfer service operators, shall obtain and keep a record, for at least ten years, the full originator's and the beneficiary's information in the message or payment form accompanying the wire transfer including but not limited to:
   (a) full name,
   (b) account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and
   (c) the originator's address, national identity number, or customer identification number, and date and place of birth.
3) For all other domestic or cross-border wire transfers below Birr 20,000 or USD 1000 or any equivalent foreign currency, Financial Institutions including intermediary Financial Institutions, money or value transfer service operators shall ensure that they are always accompanied by the following originator and beneficiary information:
   (a) full name; and
   (b) account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.
4) The information mentioned in Sub-article 3 of this Article need not be verified for accuracy unless there is a suspicion of money laundering and terrorism financing.
5) Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries in Ethiopia, the batch file shall contain required and accurate originator information, and full beneficiary information pursuant to Sub-article 2 of this Article and that is fully traceable within the beneficiary country; and the financial institution including intermediary Financial Institutions, money or value transfer service operators shall include the originator's account number or unique transaction reference number.
6) In processing wire transfers, Financial Institutions including intermediary Financial Institutions, money or value transfer service operators shall take freezing action in accordance with the provisions of the Proclamation and other relevant laws and shall prohibit conducting transactions with persons and entities, as per the obligations set out in the relevant United Nations Security Council Resolutions (UNSCRs), relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCRs 1267 and 1373, and their successor resolutions.

7) Beneficiary Financial Institutions including money or value transfer service operators shall take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.
8) For cross-border wire transfers of USD 1,000 or equivalent currency or more, a beneficiary financial institution shall verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with the provisions of these Directives.
9) If a money or value transfer service provider controls both the ordering and the beneficiary side of a wire transfer, it shall:
   (a) take into account all the information from both the ordering and beneficiary sides in order to determine whether a suspicious transaction report has to be filed; and
   (b) file a suspicious transaction report in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Center
10) Financial Institutions including intermediary Financial Institutions, money or value transfer service operators shall adopt effective risk-based policies and procedures to take reasonable measures, which are consistent with straight-through processing, for identifying and handling wire transfers that are not accompanied by complete information, and for determining:
   (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
   (b) the appropriate follow-up action.
11) Financial Institutions including intermediary Financial Institutions, money or value transfer service operators shall not execute the wire transfer if they do not comply with the requirements specified under this Article of the Directives and provisions of the Proclamation.

36. Reliance on Third Parties and Outsourcing

1) A financial institution may outsource the technical aspects of CDD process only to qualified service providers duly regulated and supervised in the country where they are based and incorporated, as long as such outsourcing allows for:
   (a) Such institution, to promptly obtain from the CDD service provider the information under this Part of the Directives;
   (b) The institution, take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request promptly;
   (c) Such institution, satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, CDD, know your customer policies and record-keeping requirements in line with the Proclamation and these Directives; and
   (d) The institution, take steps to obtain immediately the necessary information concerning property which has been laundered or which constitutes proceeds from, instrumentalities used in and intended for use in the commission of money laundering and financing of terrorism or other predicate offences.
2) If a Financial institution businesses or professions rely upon third party Financial Institutions to perform elements of CDD measures such as identification of the customer;

identification of the beneficial owner; and understanding the nature of the business or to introduce business, the ultimate responsibility for CDD measures shall remain with the financial institution relying on the third party.

37. Failure to Complete CDD Measures

Where Financial Institutions are unable to comply with relevant CDD measures under the provisions of the Proclamation and these Directives, they shall:

(a) not open an account, commence business relations or perform the transaction; or terminate the existing business relationship; and

(b) consider making a suspicious transaction report in relation to the customer.

pursuant to the provisions of the Proclamation, other laws and these Directives

PART-V
MONITORING AND REPORTING OF CASH AND SUSPICIOUS TRANSACTIONS

38. Identification of Proceeds of Crime

Financial Institutions shall, in the course of their business, identify and report to the Center, any suspicious transactions with respect to proceeds derived from the following predicate offenses:

(a) participation in an organized criminal group and racketeering;
(b) terrorism, including terrorist financing;
(c) trafficking in human beings and migrant smuggling;
(d) sexual exploitation, including sexual exploitation of children;
(e) illicit trafficking in narcotic drugs and psychotropic substances;
(f) illicit arms trafficking;
(g) illicit trafficking in stolen and other goods;
(h) corruption and bribery;
(i) fraud;
(j) counterfeiting currency;
(k) counterfeiting and piracy of products;
(l) environmental crime;
(m) homicide and grievous bodily injury;
(n) kidnapping, illegal restraint and hostage-taking;
(o) robbery or theft;
(p) smuggling; (including in relation to customs and excise duties and taxes);
(q) tax crimes (related to direct taxes and indirect taxes);
(r) extortion;
(s) forgery;
(t) piracy;
(u) insider trading and market manipulation; and
(v) any other offense specified in any law of Ethiopia, capable of generating proceeds of crime and punishable at least with simple imprisonment for one year.

39. Suspicious Transactions "Red Flags"

1) Financial Institutions shall pay special attention to all suspicious transactions and maintain a checklist of such transactions as 'red flag' which shall be disseminated to their relevant employees and made available to the Center.
2) In cases where Financial Institutions form a suspicion of money laundering or predicate offenses or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, they shall not pursue the CDD process, and instead file a suspicious transaction report.
3) Without prejudice to Article 17(2) of the Proclamation and Sub-article 5 of this Article, when any concerned person in the Financial Institution or designate detects any "red flag" for suspicious money laundering activity or predicate offenses or financing terrorism, such person is required to promptly institute a "Review Panel" under the supervision of the Compliance Officer, who shall immediately file a suspicious transaction report to the Center immediately and without delay but not later than 24 hours provided that all suspicious transactions, including attempted transactions are to be reported regardless of the amount involved.
4) Without prejudice to Article 20(2) of the Proclamation, Financial Institutions, their directors, officers and employees (permanent and temporary) shall maintain confidentiality in respect of any detection, investigation and report of suspicious transaction that will be filed or has been filed with or in possession of the Center and other competent and regulatory authorities in accordance with the provisions of the Proclamation and these Directives.
5) Where the violations involve the Compliance Officer, employees shall report such to the Center.

40. Protection of Employee who Report Violations

1) Financial Institutions shall create an enabling working environment that can make it possible for employees to report any violations of the institution's AML/CFT compliance program to the Compliance Officer and the Center.
2) Financial Institutions shall inform their concerned employees in writing to make such reports confidential and that they will be protected from victimization for making them.

41. Threshold for Cash Transaction and Wire Transfer Reports

1) Financial Institutions shall report all cash transactions in any currency above the sum of ETB 300,000.00 or USD 15,000 or equivalent foreign currency for both individuals and legal persons to the Center whether conducted as a single transaction or several transactions that appear to be linked.
2) The threshold for wire transfers shall be determined under a Circular issued by the Center.

PART-VI
EMPLOYEE CONDUCT AND TRAINING PROGRAMME

42. Comprehensive Employee Awareness and Training Programs

1) Financial Institutions shall design comprehensive employee awareness and training programs not only to make employees fully aware of their obligations but also to equip them with relevant skills required for the effective discharge of their AML/CFT tasks; provided that the timing, coverage and content of the employee awareness and training program shall be tailored to meet the perceived needs of Financial Institutions.
2) The employee awareness and training program under Sub-Article 1 of this Article shall be developed under the guidance of the Compliance Officer in collaboration with the top Management; and the basic elements of the employee training programs shall include but not limited to:
   (i) AML/CFT laws and predicate offences ;
   (ii) the nature of money laundering and terrorism financing ;
   (iii) Money laundering and terrorist financing 'red flags' and suspicious transactions, including trade based money laundering typologies ;
   (iv) reporting requirements ;
   (v) Customers Due Diligence ;
   (vi) risk-based approach to AML/CFT ; and
   (vii) record keeping and retention policy.
3) Financial Institutions shall submit their Annual AML/CFT employee training program together with report of the implementation of the previous program to the Center not later than the end of the first month of the fiscal year of Ethiopian government on which that new program has been made.
4) Except in respect of senior managers and compliance officers whose training must be provided immediately on assumption of their duties, Financial Institutions shall ensure that all relevant employees receive appropriate training within 30 days of commencement of employment.

43. Monitoring of Employee Conduct

1) Financial institutions shall monitor their employees' accounts for potential signs of money laundering and subject employees' accounts to the same AML/CFT procedures as applicable to other customers' accounts under the supervision of the Compliance Officer.
2) The Compliance Officer's own account shall be reviewed by the Chief Internal Auditor.
3) The AML/CFT performance review of staff shall be part of employees' annual performance appraisals.

PART-VII
MISCELLANEOUS PROVISIONS

44. Keeping of Records

1) Financial Institutions shall:
   (a) maintain all necessary records of transactions, both domestic and international, for at least ten years following completion of the transaction or longer if requested by other laws or by the Center in specific cases regardless of whether the account or business relationship is ongoing or has been terminated ;

(b) maintain records of the identification data, obtained through CDD measures, account files and business correspondence and results of any analysis undertaken for at least ten years following the termination of an account or business relationship or after the date of the occasional transaction or longer if required by other laws or by the Center in specific cases ;

(c) ensure that all customers-transaction records and information are available on a timely basis to the competent authorities ; and

(d) keep the necessary components of transaction-records sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity which shall include:

(i) customers' and beneficiary's names, physical addresses or other identifying information normally recorded by the intermediary;

(ii) the nature and date of the transaction;

(iii) the type and amount of currency involve; and

(iv) the type and identifying number of any account involved in the transaction.

2) Any information obtained during any meeting, discussion or other communication with the customers shall be recorded and kept in the customers' file to ensure that current customers' information is readily accessible to the Compliance Officers and the Center or to other competent and regulatory authority in accordance with the provision of the Proclamation.

3) Where maintenance of customers' records is outsourced to qualified service providers in accordance with Article 35 of these Directives, Financial Institutions shall take reasonable steps to ensure that such records are held in a manner that conforms to these Directives.

4) Financial Institutions shall maintain records of the dates of training sessions, a description of training provided and names of the employees that received training for a period of at least 10 years from the date on which training was received.

5) Financial Institutions shall maintain records of the annual report, and any other reports that highlight the level of compliance, deficiencies and actions, that it submits to senior management.

6) All records of transactions must comply with the provisions of Data Protection Laws of Ethiopia.

7) Financial Institutions shall not remove from specified area, to a place outside that specified area, any of their records and documents either physically or electronically relating to their business without the prior permission in writing of the Center.

45. Supervision of Financial Institutions

1) The Center may any time conduct inspect and supervise Financial Institutions' compliance with the AML/CFT requirements pursuant to the provisions of the Proclamation, these Directives, other subsisting laws, and the international core principles relevant for AML/CFT, including Basel Committee on Banking Supervision (BCBS) Principles 1-3, 5-9, 11-15, 26, and 29; International Association of Insurance Supervisors (IAIS) Principles 1, 3-11, 18, 21-23, and 25; and International Organization of Securities Commission (IOSCO) Principles 24, 28, 29 and 31; and Responsibilities A, B, C and D.

2) In doing the supervision under the provisions of this Article, the Center shall take into account in preventing criminals or their associates from holding (or being the beneficial

owner of) a significant or controlling interest, or holding a management function, in a financial institution business or profession.

3) The frequency and intensity of on-site and off-site AML/CFT supervision of Financial Institutions shall be determined on the basis of:
   (a) the money laundering, predicate offenses and terrorist financing risks and the policies, internal controls and procedures associated with the institution, business or profession, as identified by the Center's assessment of the institution's, business's or profession's risk profile;
   (b) the money laundering, predicate offenses and terrorist financing risks present in Ethiopia; and
   (c) the characteristics of the institution, business or profession, in particular the diversity and number of institutions, businesses or professions and the degree of discretion allowed to them under the risk-based approach.
4) The Center shall review the assessment of the money laundering and terrorism financing risk profile of Financial Institutions (including the risks of non-compliance) periodically, and when there are major events or developments in the management and operations of the institution, business or profession.

46. Sanctions for Non-Compliance

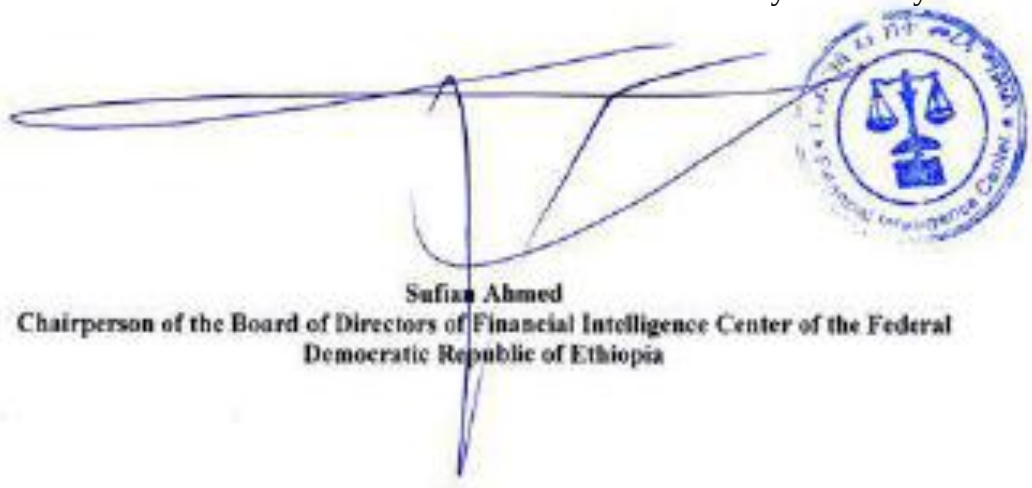
1) Failure to comply with the provisions of these Directives shall attract appropriate sanctions in accordance with the provisions of the Proclamation.
2) For purpose of emphasis, incidence of false declaration or false disclosure by the financial institution or its officers shall be subject to administrative review and appropriate sanctions meted out subject to the provisions of the Proclamation.

47. Repealed and Inapplicable Directives

1) Customer Due Diligence of Banks Directives Number SBB/46/2010 issued by the National Bank of Ethiopia is hereby repealed.
2) All other directives and procedures that are inconsistent with these directives may not apply on matters covered under these directives.

48. Effective Date

These Directives shall enter into force as of the 24th day of January 2014.



Sufian Ahmed
Chairperson of the Board of Directors of Financial Intelligence Center of the Federal Democratic Republic of Ethiopia