



Wegagen Bank, S.C.

Anti-Money Laundering and Anti-Terrorist
Financing Policy

August 2010

Table of Contents

1. Preamble.....	1
2. Scope	3
2.1 Applicability	3
2.2 Definition of Money Laundering.....	4
2.2 Definition of Terrorist Financing	5
3. Know Your Customer.....	6
4. Reporting	8
5. Record Keeping.....	8
6. Assignment of a Compliance Officer.....	8
7. Training	9
8. Monitoring Compliance with this Policy	9



1. Preamble

WHEREAS, the effort to combat money laundering and terrorist financing is being undertaken both internationally and nationally and Wegagen Bank is part thereof;

WHEREAS, the National Bank of Ethiopia (NBE), through the Customer Due Diligence of Banks Directives No. SBB/46/2010, requires banks to establish and maintain internal procedures, policies and controls to prevent money laundering and terrorist financing and the Bank is part thereof;

WHEREAS, the bank has to report and take swift action, upon detecting the suspicious activity involving shades of money laundering and terrorist financing as directed by National Bank of Ethiopia (NBE) from time to time.

WHEREAS, the Bank complies with applicable laws in Ethiopia with reference to Money Laundering and terrorist financing and adhere to standards accepted internationally by the financial world on the subject such as recommendations given by Financial Action Task Force (FATF)¹.

1 The FATF is an inter-governmental body which sets standards, and develops and promotes policies to combat money laundering and terrorist financing. It currently has 33 members: 31 countries and governments and two international organizations; and more than 20 observers: five FATF-style regional bodies and more than 15 other international organizations or bodies.



WHEREAS, the Bank is committed to the highest standards of anti-money laundering (AML) and terrorist financing compliance and requires management and employees to adhere to these standards to prevent use of the bank as a channel for money laundering and terrorist financing;

WHEREAS, the Bank commits itself for examination of its Anti Money Laundering and Terrorist Financing strategies, goals and objectives on an ongoing basis;

WHEREAS, the bank recognizes that illegal activities that often involve money laundering and terrorist financing includes, but not limited to, drug trafficking, terrorism, smuggling, fraud, bribery, robbery, embezzlement, and illegal gambling;

WHEREAS, the Bank's Anti-Money Laundering and Terrorist Financing Program includes client screening and monitoring requirements, "know your customer" policies (including the requirement to establish the identity of beneficial owners), record keeping requirements, the reporting of suspicious circumstances in accordance with relevant laws and regulations, and training;

WHEREAS, the standards set out in this Policy are minimum requirements based on applicable legal and regulatory requirements and apply for all branches of the bank and other concerned business units;



Now, therefore, pursuant to Article 12 of the Memorandum of Association of the Bank, the Board of Directors hereby issues this Anti-Money Laundering and Terrorist Financing Policy and its related procedure.

2. Scope

2.1 Applicability

According to article 53 of Banking Business Proclamation number 592/2008 and article 3(2) and 3(3) of Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation number 657/2009, and the National Bank of Ethiopia's (NBE) Customer Due Diligence of Banks Directive No. SBB/46/2010, every commercial bank in the country must ensure that the legal duties resulting from the proclamations and directives are fulfilled by all branches of banks. Wegagen Bank, being one of the private commercial banks has to abide by the proclamations and directives issued by the NBE, and hence have to draft anti money laundering policy and procedure. Moreover, the current recommendations of Financial Action Task Force on Money Laundering (FATF) and other additional precautionary measures issued by concerned international organizations such as the UN as well as recommendations from other governments are taken care of in drafting this policy.

Wherever local regulations are stricter than the requirements set out in this Policy, the stricter standard has to be applied. If any applicable laws are in conflict with this Policy, the relevant Bank entity must consult with the local legal department and the Compliance Officer to resolve the conflict.



If the minimum requirements set out in this Policy cannot be applied in a certain country's banks because application would be against local law or cannot be enforced due to other than legal reasons, the Bank has to assure that it will not

- enter into a business relationship,
- continue a business relationship or
- Carry out any transactions.

If business relations already exist in that country, the Bank has to assure that the business relationship is terminated regardless of other contractual or legal obligations.

2.2 Definition of Money Laundering

Money laundering is defined in one of the following ways:

- 1) It is the introduction of illegally obtained currency into the banking system.
- 2) It is using the banking system to illegally hide currency that was lawfully obtained.

Generally speaking, the money laundering process consists of three "stages":

Placement: The introduction of illegally obtained monies or other valuables into financial or non-financial institutions.

Layering: Separating the proceeds of criminal activity from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

Integration: Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.



These “stages” are not static and overlap broadly. Financial institutions may be misused at any point in the money laundering process.

It is not hard for criminals to obtain currency. However, until the currency is deposited into the banking system, their ability to utilize it is restricted. When banks knowingly accept the cash deposits of criminals, they legitimize (or launder) the proceeds. Accordingly, criminals must do business with banks. And banks like Wegagen must be diligent in detecting and reporting suspicious activity.

2.2 Definition of Terrorist Financing

Terrorist financing is a terrorist activity which involves funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. However, financial transactions associated with terrorist financing tend to be in smaller amounts than is the case with money laundering, and when terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult.

To move their funds, terrorists use the formal banking system, informal value-transfer systems, Hawalas and, the oldest method of asset-transfer, the physical transportation of cash, gold and other valuables through smuggling routes.

3. Know Your Customer

In the context of 'Money Laundering', it is appropriate that the bank lays down appropriate guidelines regarding whom it shall accept, or more precisely, whom it shall not accept as its customers as also suitable set of 'Know Your Customer' norms and formalities for accepting a customer. It will be desirable to eliminate the possibility of accepting as customers, persons, institutions or parties where there may be reasonable apprehension that the account could be used for money laundering or terrorist activities. As a preventive and as a prudential measure the bank may not open accounts in such cases as the following:

- Where the customer's identification is not established to the satisfaction of the bank;
- Where there is reasonably reliable information that the prospective customer has a doubtful past;
- Bank accounts expressly forbidden by the NBE.
- Accounts of terrorist individuals/organizations as advised by the NBE or other authorities and persons related/connected to/with them.

In general, all Wegagen Bank branches have to comply with the following basic principles:

3.1 Ascertainment of customer identity:

- When entering into a lasting business relationship,
- When performing a single transaction or deal,
- Before accepting cash or other physical values worth 10,000 USD or Birr 200,000 or more (or equivalent)



3.2 Establishment of purpose of business relationship: When entering into a lasting business relationship, The Bank must obtain information on kind and purpose thereof, if this is not clear from the business relationship itself.

3.3 Identification of Ultimate Beneficial Owner: Whenever The Bank is required to identify a customer, it must establish and verify the identity of the ultimate natural person,

- who owns or
- controls the customer or its assets or
- on whose behalf the transaction is carried out or the business relationship is established

3.4 Client account monitoring: A permanent monitoring of clients' accounts must be implemented to detect unusual/suspicious transactions. Monitoring must be effected for applicable business areas using adequate processes and systems.

3.5 Correspondent banking: Special attention must be paid to correspondent banking business and adequate security measures must be implemented.

3.6 Forbidden business: Payable through accounts and relationships with shell banks² are forbidden for Wegagen Bank and Wegagen Bank's correspondent banks

3.7 Staff reliability: The Bank must employ reliable staffs and properly manage them putting in place appropriate systems tailored towards this objective.

3.8 Embargo Requirements: The Bank will adhere to all applicable embargo requirements and will check clients and transactions against applicable embargo lists.

² Shell Bank, as defined in NBE's Customer Due Diligence of Banks Directives No. SBB/46/2010, 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.

4. Reporting

Suspicious circumstances/transactions must be reported to the competent authorities according to local law. The Bank's Compliance Officer must be informed about all suspicious events.

5. Record Keeping

In terms of the Banking Regulation Act, records such as Account Opening Forms, vouchers, ledgers, registers, etc., pertaining to Banking Transactions for specified periods are required to be maintained at the end of business relationship with the customer, which in any case shall not be less than 10 years. In other words, all financial transaction records are to be retained for at least 10 years after the transaction has taken place and are to be made available for scrutiny of law enforcing agencies, audit functionaries as well as regulators, as and when required.

6. Assignment of a Compliance Officer

The Bank shall assign a senior officer as the Bank's Compliance Officer with sufficient operational experience and investigative mind. He/she would have the necessary freedom to act on his/her own authority, should be provided with the necessary resources to effectively run the compliance function and shall be accountable to the Chief Executive Officer /President of the Bank.



The Compliance Officer must ensure by adequate customer- and business related controls that all applicable AML requirements are being adhered to and security measures are properly functioning.

7. Training

All employees (including trainees and temporary personnel) responsible for carrying out transactions and/or for initiating and/or establishing business relationships must undergo anti money laundering training. The Bank has decided to extend the target audience for AML to cover all staff. Initial training must be attended within three months after an employee has joined The Bank and subsequently every two years.

8. Monitoring Compliance with this Policy

A minimum of once a year, the bank's internal auditor or an independent third party will review the Compliance Officer's suspicious activity file. The auditor will ensure that all identified suspicious activity was reviewed and appropriately handled. The auditor will also use the Transaction Monitor System to search for suspicious activity that the Compliance Officer may have missed.



Wegagen Bank, S.C.

Anti-Money Laundering and Anti-Terrorist
Financing Procedure Manual

August 2010



Contents

1. Introduction	1
2. Money Laundering	1
3. Risk Based Approach.....	3
4. Customer Acceptance Policy.....	5
5. Know Your Customer (KYC)	6
5.1 Introduction	6
5.2 Customer Identification and Due Diligence.....	7
5.3 Identification of suspicious transactions	12
5.4 Financing of Terrorism	13
6. Cross Border Correspondent Banking.....	13
7. Wire Transfers	15
8. Reporting System for High Value Cash/Suspicious Transactions	15
9. Evaluation of the Compliance function by an Auditor	17
10. Retention of Records.....	17
11. Training.....	18
12. The Importance of KYC to the Employees.....	19
13. Transactions Monitoring.....	19
13.1 Offshore Transactions	20
13.2 Trade Services	20
13.3 General Accounts.....	21
13.4 Loan/ Credit transactions.....	22
13.5 Correspondent Bank Transactions.....	22
14. Assignment of a Compliance Officer	24
15. Staff Accountability with Regard to ‘Know Your Customer’ and ‘Anti Money Laundering’	25
16. Prohibition against Disclosing Suspicious Transaction Report (STR).....	26



1. Introduction

Money Laundering (ML) is a serious threat to financial system of all countries and leads to destruction of a country's sovereignty and character. This has been widely recognized at the international level. The recognition has culminated in concerted efforts all over the world to fight this ultra-criminal activity through enactment of stringent laws, regulations and measures aimed at securing financial systems against money laundering. Financial Action Task Force (FATF) was constituted in 1989 and is a concrete step initiated at the global level. The three basic tenets of Anti Money Laundering i.e., Know Your Customer (KYC), Source of funds and End use/destination of funds have been covered in this document.

This manual is aimed at increasing awareness of money laundering activity and its ill effects and to simultaneously contribute, on the part of Wegagen Bank staff members to counter ML in a significant way, including guarding against ML at all times.

2. Money Laundering

Money Laundering is any transaction or series of transactions undertaken to conceal or disguise the nature and source of funds that have been obtained from illegal activity. The main objective of the money launderer is to transform 'dirty'



money into seemingly clean money or other assets in a way to leave as little trace as possible of the transformation. Examples of illegal activities that often involve money laundering and terrorist financing are: drug trafficking, terrorism, smuggling, fraud, bribery, robbery, embezzlement, and illegal gambling. There are three recognized forms of the money laundering process:

2.1 Placement – Physically depositing “cash” into banks and non-bank financial institutions such as currency exchanges; converting “cash” into other financial instruments such as by purchasing monetary instruments (travelers’ checks, payment orders); or using “cash” to purchase expensive items that can be resold. Launderers often seek to deposit cash into banks in less regulated countries and then transfer these funds to banks in regulated environments as “clean”. They also use smurfing , which is a form of placement where the launderer makes many small cash deposits instead of a large one to evade local regulatory reporting requirements applicable to cash transactions.

2.2 Layering – Separating the proceeds of criminal activity from their source through the use of layers of financial transactions (multiple transfers of funds among financial institutions, early surrender of an annuity without regard to penalties, cash collateralized loans, L/Cs with false invoices/bills of lading, etc.) to disguise the origin of the funds, disrupt any audit trail, and provide anonymity. Launderers want to move funds around, changing both the form of the funds and



their location in order to make it harder for law enforcement authorities to identify “dirty” money.

2.3 Integration – The final link in money laundering process is sometimes called the integration stage. This occurs when the laundered or cleaned up money is legitimately brought back into financial systems operated by end user and when it is safe and insulated from enquiry by any agency with a legitimate reason for querying the existence of money. E.g. Loan back technique or loan-default technique where the lender bank seeks to recover its assets (loans to money launderers) by attaching the securities held by bank which exist in the form of black money.

It is important for all staff members to be conversant and be absolutely familiar with the ML process as they must be vigilant all the times and should any of the aspects involved in ML process touch/surface our business, they must be able to read the danger signal and blow the whistle.

3. Risk Based Approach

Identification of the money laundering risks of customers and transactions, by The Bank, allows in determining and implementing proportionate measures and controls to mitigate these risks. We use the following criteria in identifying money laundering risks:



3.1 Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering risks. Factors that may result in a determination that a country poses a higher risk include:

- Countries subject to sanctions, embargoes or similar measures;
- countries identified by the Financial Action Task Force ("FATF") as non-cooperative in the fight against money laundering or identified by credible sources as lacking appropriate money laundering laws and regulations;
- countries identified by credible sources as providing funding or support for terrorist activities;
- countries identified by credible sources as having significant levels of corruption, or non-transparent tax environment.

3.2 Customer risk - there is no universal consensus as to which customers pose a higher risk, but the below listed characteristics of customers have been identified with potentially higher money laundering risks:

- armament manufactures,
- cash intensive businesses;
- unregulated charities and other unregulated "non profit" organizations;
- dealers in high value precious goods;
- "Politically Exposed Persons" (frequently abbreviated as "PEPs"), referring to individuals in a foreign country who are holding or having held positions of public trust, such as government officials, senior executives of government



corporations, politicians, senior judicial or military officials, important political party officials, etc., as well as their families and close associates;

- Companies that have shares in bearer form;
- Non-resident customers such as those staying in a country for less than one year or those in short visit or travel;
- Legal persons or arrangements such as trusts that are personal asset holding Institutions;

3.3 Services risk. Determining the money laundering risks of services should include a consideration of such factors as:

- services identified by regulators, governmental authorities or other credible sources as being potentially high risk for money laundering;
- Services involving banknote and precious metals trading and delivery.

4. Customer Acceptance Policy

In the context of the concerns regarding ‘Money Laundering’, it is appropriate that the bank lays down appropriate guidelines regarding whom it shall accept, or more precisely, whom it shall not accept as its customers as also suitable set of ‘Know Your Customer’ norms and formalities for accepting a customer. It will be desirable to eliminate the possibility of accepting as customers, persons, institutions or parties where there may be reasonable apprehension that the account could be used for money laundering or terrorist activities. As a preventive and as a prudential measure the bank may not open accounts in such cases as the following:



- Where the customer's identification is not established to the satisfaction of the bank;
- Where there is reasonably reliable information that the prospective customer has a doubtful past track record;
- Bank accounts expressly forbidden by the NBE.
- Accounts of terrorist individuals/organizations as advised by the NBE or other authorities and persons related/connected to/with them.

The responsibility for screening the customer will be with the respective Front Office Personal Banker and with respective Branch Managers/Assistant Branch Managers and in cases of doubt the Manager, Domestic Banking Operations may be consulted, before taking a decision.

5. Know Your Customer (KYC)

5.1 Introduction

The importance of KYC approach, a very essential and preliminary aspect, need not be over emphasized. The issuance of a comprehensive directive (Directive No. SBB/46/2010) by the National Bank of Ethiopia in March 2010 on this approach depicts the seriousness and recognition attached to KYC principle in guiding the Ethiopian commercial banks in this regard.



The KYC principles aim:

- To establish procedures to verify the bonafide documents identification of individuals/corporate office accounts.
- To establish process and procedures to monitor high value transactions and suspicious transactions.
- To establish systems for conducting due diligence and reporting of such activities.

The focus of KYC is 'back to basics' where elaborate standard for obtaining detailed information regarding new customers at the initial stage and that of existing customers over a period of time would be achieved. This would help in establishing the genuineness and bonafideness of customers and keeping a watch over transactions, particularly those of a suspicious nature, and reporting these to the regulators/law enforcers.

5.2 Customer Identification and Due Diligence

The Bank will identify the customer, whether regular or occasional, if natural or legal person or there is a legal arrangement, and verify that customer's identity using as much as possible reliable and independent source documents, data or information. Different categories of customers of the Bank are identified as described below, before the bank opens an account for them or make a business transaction with them (As per the details provided in the Domestic Banking Procedure Manual of the Bank).



(a) Identifying natural persons for opening accounts

- Bank accounts are opened for individuals by obtaining official, valid and recent Identification Documents (ID) or valid passport issued by local government administrative bodies, after ascertaining that they are legally qualified to have such accounts and that there is nothing precluding banking with them. Utmost care is exercised to make sure that the documents provided are true and valid.
- Opening bank accounts must be applied for by means of the forms used by the bank and to obtain all information required in the form, particularly full name, nationality, profession, permanent address, type of business, date and place of birth, telephone number, fax number, e-mail address, occupation, public position held and/or name of employer, type of account and signed statement certifying the accuracy of the information provided; and not to ignore any information supposed to be provided in the printed form. The client must also undertake to regularly update (at least every 3 years) the information introduced in the form shall there be any change in the client's type of business or transactions.
- In case the Bank desires to have correspondences forwarded to an address other than the permanent one, a reasonable reason should be given.



- In case there is no permanent address provided, the address and identification details of a person related to the client should be obtained in order to be able to communicate with the client through correspondence.
- A clear copy of the ID documents should be obtained and indicate on such copies that they are true copies of the originals.
- In case it is not possible to check the official identification documents or if they are inadequate, the reason should be indicated. In such a case a bank account may be approved and opened but the client shall not be allowed to use it until the required official documents are provided. The matter shall be referred to a higher supervisory level and the documents required to be fully obtained.
- In case of opening more than one account by one client, the client must provide reason and indicate such reasons in the application form and such reasons must also be recorded on the computer and properly maintained.
- In case of opening an account by means of a proxy, it must be ascertained that the proxy is an official one duly notarized. Sufficient information of the proxy's identification, address, telephone number and type of business practiced must be obtained. The same procedure is followed for authorizations processed at the bank.
- The information related to the clients must be regularly checked and updated every 3 years or whenever there is reason to do so by respective branches.



- In case long-time (old) clients make their accounts active again, they have to update all information related to them.
- The details of identification must be sufficient and supported by official documents of all persons having the rights to use the account and a good copy of all such documents must be obtained.
- Clients abroad may have accounts opened for them via the correspondents of the bank by providing all information required, such as the ID, office and resident addresses, telephone numbers and types of businesses practiced by clients. All such information must be substantiated by right and valid documents as set in the rules for the identification of clients.
- Acknowledgement showing that the client is the principal holder and sole beneficiary of the account and that he/she shall not make or accept depositing any amounts of unknown or suspicious source.

(b) Identifying legal persons for opening accounts

- Taking 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.
- Reviewing the official documents, which show the legal form, nature of the activity, the commercial name as well as obtaining an original copy of these documents



- Ascertaining of the registered name of the company, its head office address and its branches. Also the issued approvals for the establishment and practicing the activity in addition to the required data about the owners of these companies.
- As appropriate, by referring to the constitutive document of the company, determines the individuals allowed to open an account at the bank along with determining the individuals who are permitted to use the account, as well as reviewing the ID documents related to them and to obtain copies of them.
- Regarding companies under establishment, the required procedures should be available for the foundation of the company and following the rules set in the company's law.
- As for individual companies, the identity and the addresses should be affirmed to all the joint, limited and responsible partners of signing the accounts as well obtaining copies of them.
- As for accounts opened for governmental bodies after obtaining the required approvals, this has to be done according to an issued book carrying the name of the requesting body, including names, positions, and usage capacities of persons authorized to use the accounts obtaining the ID of these individuals from the official documents. Each adjustment has to be done on a book carrying the name of the requesting body and the signatures of the person in charge of the accounts.



- Regarding non-profit organizations, documents related to its establishment should be available as well its nature of activity and the ones responsible for its management, then to be ratified from the specialized official bodies which control them and the needed approvals allowing them to have accounts with banks.

(c) Establishment of the bank's new business relationship with a politically exposed person shall be approved by a senior management member of the bank. Where a customer has been accepted and the customer is subsequently found to be, or subsequently becomes a politically exposed person, continuation of business relationship with such person shall be approved by a senior management member of the bank.

Operating staff should exercise due diligence and care while opening an account in terms of NBE guidelines/regulations and legal compliance in force. It must also be ensured that KYC guidelines are made applicable to new and existing account holders.

5.3 Identification of suspicious transactions

For identification of suspicious transactions, we should take precautions by assigning staffs having good integrity. Some of the indicators of suspicious transaction are:

- i. Involvement of funds for illegal activity.
- ii. Intending to hide or disguise assets derived from illegal activities.



- iii. Intention to evade anti-money laundering guidelines.
- iv. Customer has no business or apparent lawful purpose and has no linkage with such businesses.

5.4 Financing of Terrorism

NBE has circulated and will circulate from time to time a list of Terrorists and Terrorist organizations, which will require to be referred to, to check existence of such accounts of Terrorist organizations and initiate appropriate action before opening an account. The list of Terrorist organizations will be installed in the core banking system and will ‘pop-up’ at the time an account is being input into the system so that the staff inputting the data can access such list. If any such name does come up, the agencies/regulators should immediately be informed.

6. Cross Border Correspondent Banking

- 6.1 With respect to cross-border correspondent banking and other similar relationships, the Bank, in addition to performing normal customer due diligence measures, will:
 - 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 a new correspondent relationships; and
 - d. Document the respective anti-money laundering and combating terrorist financing responsibilities of each institution.
- 6.2 Where a correspondent relationship involves the maintenance of "Payable-through accounts¹", The Bank has to make sure that:
- a. The respondent financial institution has performed all the normal customer due diligence obligation on those of its customers that have direct access to the accounts of the correspondent financial institutions; and
 - b. The respondent financial institution is able to provide relevant customer identification data upon request to the correspondent bank.
- 6.3 Where a correspondent bank fails to comply with national anti-money laundering and combating terrorist financing laws, the bank shall not open an account, commence business relations or perform transaction or shall terminate the business relationship with such correspondent financial institutions and shall consider making a suspicious transaction report in relation to correspondent financial institutions.

¹ Payable Through Account (PTA) is a demand deposit account through which banking agencies (located in the USA) extends check writing privileges to the customers of other institutions, often foreign banks.



6.4 The bank shall satisfy itself that the respondent financial institutions in foreign countries do not allow business relationship with shell banks.

7. Wire Transfers

For wire transfers of Birr 10,000 or USD 1000 or more, ordering banks are required to obtain and maintain the originator's full name, account number or a unique reference number, if no account number exists, complete address, data and place of birth (if possible). Moreover, in such cases the ordering financial institution or the bank should be required to include full originator information in the message or payment form accompanying the wire transfer. However, where several individual cross-border wire transfers of USD1,000 or more from a single originator are bundled in a batch file for transmission to beneficiaries in Ethiopia, the ordering foreign financial institution only needs to include the originator's account number or unique identifier on each individual cross-border wire transfer, provided that the batch file (in which the individual transfers are batched) contains full originator information that is fully traceable.

8. Reporting System for High Value Cash/Suspicious Transactions

Wegagen Bank will report to the Financial Intelligence Center of the Federal Democratic Republic of Ethiopia when it encounters the following:



- All cash deposits or withdrawals exceeding Birr 200,000 and/or USD 10,000 or its equivalent in other foreign currency.
- All suspicious transactions, including attempted transactions regardless of the amount of the transaction
- When it suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity.
- Where there are reasonable grounds that funds are linked or related to, or to be used for terrorisms, terrorist acts or by terrorist organizations or those who finance terrorism

To observe “Four Eyes” concept in reporting suspicious transactions at branch level, first the Personal Banker at the branch will report to the Branch Manager who will get himself satisfied about existence of a suspicious activity/nature and then himself report to the manager of Domestic Banking Department who will bring this to the notice of the Chief Executive/President.

Further course of action is to be decided by the Management in consultation with Legal Services Department to take up the matter with the appropriate law enforcing authorities designated under the relevant laws governing such activities.

In case the name of any banned organization appearing as payee/endorsee/applicant, it will be our endeavor to ensure that the computer will



throw a caution. Reporting of such transactions as and when detected will be as above.

9. Evaluation of the Compliance function by an Auditor

An independent evaluation of AML compliance would require to be carried out by an Auditor. The auditor would be required to comment on the effectiveness for measures taken by branches for implementation of KYC principles and prevention of money laundering. It is also the Internal Auditor who provides reasonable assurance to management as to the proper functioning of the compliance function of the Bank.

10. Retention of Records

In terms of the Banking Regulation Act, records such as Account Opening Forms, vouchers, ledgers, registers, etc., pertaining to Banking Transactions for specified periods are required to be maintained. In addition, the following documents in respect of accounts, which have been reported for suspicious activities, are required to be retained at the end of business relationship with the customer, which in any case shall not be less than 10 years.

- Customer Profiles
- Reports made to government authorities concerning suspicious customer activity relating to possible money laundering or other criminal conduct together with supporting documentation.



- Any other documents required to be retained under applicable money laundering laws/regulations.

All financial transaction records are to be retained for at least 10 years after the transaction has taken place and are to be made available for scrutiny of law enforcing agencies, audit functionaries as well as regulators, as and when required.

11. Training

All operation staffs need to be trained on an ongoing basis for strict implementation of KYC guidelines and AML measures. The training should incorporate:

- Responsibilities under the bank's arrangements for money laundering and terrorist financing prevention;
- Policies, procedures and controls and practices for obtaining identification evidence; applying "know your customer" standard; account monitoring; enhanced due diligence; record keeping; and reporting knowledge or suspicion of money laundering and terrorist financing;
- Audit function to ensure the bank's compliance with anti-money laundering and combating terrorist financing laws, directives, and internal policies and procedures;
- Domestic laws and bank standards related to money laundering and terrorist financing;
- Relevant typologies of Money laundering and terrorist financing.



- Potential risks, including reputational, operational, legal, and concentration risks of becoming involved in laundering the proceeds of crime or terrorist financing.

Employees should also receive periodic updates to their training, particularly when there are changes in regulations.

12. The Importance of KYC to the Employees

The Bank employees will conduct themselves in accordance with the highest ethical standards and in accordance with the extant regulatory requirements and laws. Staff should not provide advice or other assistance to individuals who are indulging in money laundering activities. Money laundering activities cover not only the criminals who try to launder their ill-gotten gains, but also the banks/ financial institutions and their employees who participate in those transactions and have knowledge that the property is criminally derived. “Knowledge” includes the concepts of “conscious avoidance of knowledge.

13. Transactions Monitoring

A customer’s account opened with proper and reasonable identification requires active and careful review on an on-going basis by verification of transactions. The



following transactions deserve monitoring so as to be able to detect and deter money laundering and terrorist financing activities:

13.1 Offshore Transactions

1. Our bank does not enter into or continue correspondent banking relationships with shell banks.
2. Loans made on the strength of a borrower's financials which reflect large investments in and income from businesses incorporated in Bank secrecy havens countries or non-cooperative countries and territories.

13.2 Trade Services

1. Transactions not providing clear description of goods/technology being shipped.
2. Transfer of Documentary Credit reflecting unreasonable profit margin in the underlying transaction or names of an offshore financial institution.
3. Commercial L/C or collection item, not with precise presentation of transport document.
4. L/C designating place of payment other than beneficiary's stated location.
5. L/C amended (just before the payment) with reference to Beneficiary's name/address, or including assignment of proceeds and transfers at the time of presentation of documents.
6. Standby letters of credits used as bid bonds or performance bonds without the reference to underlying projects or contract.
7. L/C involving unusual intermediary or number of intermediary/ies.



8. L/Cs requiring the Bank to allow payment request by beneficiary in the same country without presentation of documents to be sent to opening Bank.
9. Witnessing international transactions in the accounts of customers with no such history of international transactions or irrelevant to stated business.
10. Irrational or unusual payment terms/prices or interest rates and penalties and compensations in L/C.
11. L/C for transactions of large size involving high risk countries.
12. B/L mentioning containerized cargo/es without container/s numbers/or sequential numbers.
13. Exceptional degree of secrecy/confidentiality with respect to L/C transactions, required by customer.
14. L/C requesting consignee's name in Bill of Lading with a vague clause e.g. to be advised or determined between applicant and beneficiary, rather than the established practices in Documentary Credit.

13.3 General Accounts

1. High transactions but low balances,
2. Insensitivity to transaction fees
3. Alterations in account activity/patterns inconsistent with account history.
4. Customers desiring unnecessarily complex transactions,
5. References to/by persons impossible to verify or difficult to access.
6. Unusual documentation.
7. Credit transactions by cheques/all cash withdrawals.



13.4 Loan/ Credit transactions

1. Customer uses cash collateral / parked offshore to obtain loan/facility.
2. Purpose of loan not recorded or ambiguous.
3. End use of loan proceeds not consistent with purpose advised to Bank.
4. Borrower settling “problem” loans by large amounts of cash suddenly with no reasonable explanation of funds/source.
5. Purpose of loan does not make economic sense; or provision of cash collateral but non-disclosure of purpose of loan.
6. Loan proceeds unexpectedly channeled offshore.

13.5 Correspondent Bank Transactions

Transactions conducted through correspondent relationships need to be managed taking a risk based approach.

- a. Remittances received without remitter’s name, details of originating bank should be carefully monitored irrespective of beneficiary account and type.
- b. Similarly, while issuing FIRC’s (Foreign Inward Remittance Certificates) against drafts, the staff will ascertain the remitter’s name/location from overseas branches. (Since the beneficiary is allowed to declare the remitter’s name and purpose of remittance, it is likely that a launderer will mislead the Bank to destroy the audit trails.)
- c. Arrangements should be made to ensure that correspondents advise the Bank of any local exchange control regulations and restrictions on international transfers. Similarly, it should be ascertained whether correspondent bank themselves are

regulated for money laundering prevention in their country and if so, whether the correspondent is required to identify their customers in comparable standards which are at least at par with Ethiopian Banking industry's practices.

d. The following checkpoints will be applied, inevitably, to ensure that a known entity for a known and permitted bonafide purpose effects on outward remittance (by drafts/telegraphic transfers) to a known beneficiary through a bank account abroad.

- Beneficiary is an acceptable person (Natural or legal)
- Establishment of prima facie connection or locus standi between remitter and beneficiary.
- Purpose; the underlying transaction or motive behind the transaction is not sham and illusory or vexatious. End use of funds with reference to beneficiary bears out well with documents produced and the status of remitter.
- Transaction is borne by complete set of documents or any other formality bank requires the remitter to fulfill, is complied with without haphazardness or any haggling and irrational references.
- NBE directives clearly permit the transaction with reference to quantum and conditions.
- Pattern of the remittances commensurate to customer's nature of business as disclosed at the time of setting up account/s.



14. Assignment of a Compliance Officer

The Bank shall assign a senior officer with sufficient operational experience and investigative mind. The NBE directive also requires the designation of a compliance officer at the management level. He/she would have the necessary freedom to act on his/her own authority, should be provided with resources to effectively run the compliance function and shall be accountable to the Chief Executive Officer /President of the Bank.

1. The Compliance Officer's role is to maintain controls and procedures aimed at deterring criminal elements from using the products and services of the Bank and implement this policy.
2. He/She will also be instrumental in adhering to KYC principle and effective customer identification and should provide necessary guidance to operating staff.
3. His/Her vigilance in computerized and non-computerized transactions and track patterns would be important.
4. He/She shall keep himself/herself abreast of all latest developments in AML area in other organizations and countries and effect the changes in AML measures suitably to improve AML exercise in the Bank.
5. The Compliance officer will
 1. Maintain up-to-date list of high risk countries,
 2. maintain up-to-date list of terrorists and terrorist organizations sent from NBE from Time to time



3. Identify for the Bank, the high, moderate and low risk activities from AML angle.
4. Identify unusual transactions.
6. Depending on the Suspicious Transaction Report (STR), he/she shall co-ordinate with senior management to decide on continuing account relationship with increased caution/alert. In this context, he/she would decide to report the suspicious transaction to Regulatory law enforcement agencies.
7. He/She shall arrange to conduct training for staff with latest course material on AML and case studies.
8. The Compliance Officer will report to Chief Executive/President once in half year, the progress and status of the AML measures in vogue and improvements, findings and Bank's on-going preparedness on AML activity.

15. Staff Accountability with Regard to 'Know Your Customer' and 'Anti Money Laundering'

It is important to ensure that the guidelines/instructions lay down with regard to 'Know Your Customer' and 'Anti Money Laundering' is followed in letter and spirit.

Therefore, the staff entrusted with this responsibility is urged to get themselves fully conversant therewith and implement them carefully and diligently. Besides, the internal auditors should be requested to audit 100% of the new account mandates and to report any deficiencies or deviations observed. They should also audit the



large value transactions and report any deficiencies or deviations observed in the compliance of 'Anti Money Laundering' Policy. They should also issue/incorporate separate certificates in their quarterly reports whether the provisions of the 'Know Your Customer' and 'Anti Money Laundering' Policies are being fully complied with. In the event of any discrepancies or deviations observed (whether in the reports submitted by the auditors, the reports submitted by the Compliance Officer or otherwise), it is important to ascertain the possible consequences thereof and set the position right within a short time frame and to avoid any adverse repercussions. At the same time it is also necessary to analyze such cases and to determine whether the same were caused by any shortcomings in the exercise of due diligence on the part of the bank's officials/staff. The Chief Executive Officer will examine all such cases as he may consider appropriate with the causes, responsibility and consequences of the deficiencies or deviations and initiate such action as may be appropriate including with regard to staff accountability.

16. Prohibition against Disclosing Suspicious Transaction Report (STR)

In no circumstances, employees must alert a client or his representative/s about the suspicious transactions/dealings or about which an STR is underway for reporting to Compliance Officer (tipping off).



The list of suspicious transactions furnished here is not exclusive and staff members would be always expected to monitor transactions of all types which pass through their desks with fair amount of judgment and vigilance over and above the normal.