የኢትዮጵያ ብሔራዊ ባንክ
NATIONAL BANK OF ETHIOPIA
ADDIS ABABA

TELAGRAPHIC ADDRESS
N A T I O N B A N K
TELEX 21020
CODES USED
PETERSON 3rd & 4th ED.
BENTLEY'S 2nd PHRASE
A. B. C. 6th EDITION.

PLEASE ADDRESS ANY REPLY TO
P. O. Box 5550
ADDIS ABABA

LICENSING AND SUPERVISION OF BANKING BUSINESS

Customer Due Diligence of Banks
Directives No. SBB/46/2010

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

WHEREAS, there is a need to strengthen internal control and risk management systems of banks 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 banks;

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

Now, therefore, in accordance with article 53 of Banking Business Proclamation Number. 592/2008 and articles 3(2) and 3(3) of Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation number 657/2009, `the National Bank of Ethiopia hereby issues these directives.

1. Short Title

These directives may be cited as "Customer Due Diligence of Banks Directives No. SBB/46/ 2010".

2. Definitions

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

1) "beneficial owner" refers to the natural person(s) who ultimately owns or controls a bank customer, in case the customer is legal person or arrangement, and/or the person on whose behalf a transaction is being conducted;

2) "correspondent banking" is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank);

3) "cross-border transfer" means any wire transfer where the originator and beneficiary persons are located in different jurisdictions at the time of initiating the transfer. This term also refers to any chain of wire transfers that has at least one cross-border element;

4) "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. This term, therefore, refers to 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;

5) "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 the bank and the activity in the account. Such categories shall include, but not be limited to:

   (a) complex, unusual or large transactions,
   (b) relationships or transactions with countries known to have material deficiencies in anti money laundering and terrorist financing strategies,
   (c) politically exposed persons,
   (d) non-resident customers such as those staying in the country for less than one year or those in short visit or travel,
   (e) legal persons or arrangements such as trusts that are personal asset holding vehicles, and
   (f) Companies that have shares in bearer form;

6) "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;

7) "Money laundering" shall have the meaning ascribed under article 2(10) of the Proclamation to provide for Prevention and Suppression of Money Laundering and Financing of Terrorism number 657/2009;
8) "Originator" is bank account holder, or where there is no account, the person that places an order with the bank or other financial institution to perform the wire transfer;
9) "Payable-through accounts" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf;
10) "person" means any natural or juridical person;
11) "politically exposed persons"are individuals in a foreign country who are or have been entrusted with senior government functions, such as heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials;
12) "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.
13) "senior management" means a team of executives at the highest level who have the day-to-day responsibilities of managing a bank as defined by each bank;
14) "terrorist financing" means an offence defined under article 5(1)(d) of Anti-Terrorism Proclamation number 652/2009;
15) "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.

3. Customer Acceptance Policy, Procedure, and Compliance Arrangement

a. Banks shall establish and maintain internal procedures, policies and controls to prevent money laundering and terrorist financing, and communicate these to their employees and the National Bank of Ethiopia; at a minimum these procedures, policies and controls shall cover:

a) explicit criteria for identification and acceptance of customers,
b) appropriate risk management systems to determine whether a potential customer, an existing customer or beneficial owner is a politically exposed person or high risk categories of customers,
c) record retention techniques, methods and period ;
d) unusual and suspicious transactions detection, techniques, methods and the reporting obligation;

e) measures to be taken to prevent the misuse of technological developments in money laundering or terrorist financing schemes; and
f) specific risks associated with non-face to face business relationships or transactions.

b. Banks shall develop appropriate compliance management arrangements which at a minimum include:

i. designation of a compliance officer at the management level; and

ii. ensure application of all laws related to anti-money laundering and combating terrorist financing; these directives; and internal policies, procedures and controls when establishing customer relationships and conducting ongoing due diligence.

c. Banks shall maintain an adequately resourced and independent internal audit function to test compliance with laws; directives of the National Bank of Ethiopia; and internal policies, procedures and controls.

4. Customer Identification and Due Diligence

1) banks may not keep anonymous accounts or accounts in fictitious names;
2) Banks shall not enter into, or continue, correspondent banking relationships with shell banks.
3) Banks shall undertake customer due diligence measures when:
   i. establishing business relations with a customer;
   ii. carrying out occasional cash transaction with a customer, which at a minimum exceeds Birr 200,000, USD 10,000 or equivalent in other foreign currencies; 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;
   iii. there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or thresholds that are referred to under these directives; and
   iv. they have doubts about the veracity or adequacy of previously obtained customer identification data.
4) Banks shall identify the customer, whether regular or occasional, natural or legal person or legal arrangement, and verify that customer's identity using as much as possible reliable, independent source documents, data or information.
5) Identification requirements for natural persons shall include, at a minimum:
   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.

6) For customers that are legal persons or legal arrangements, banks 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 legal person or legal arrangement at a minimum by obtaining proof of incorporation or similar evidence of establishment or existence and information concerning the legal person's or legal arrangement's :
      i. name,
      ii. legal form,
      iii. some form of official identification number such as tax identification number (if available),
      iv. address which includes country, city/town/kebele in which the head office is located and if available, house number, mailing address, telephone number and fax number,
      v. names of directors, if applicable, and the chief executive officer,
      vi. provisions regulating the power to bind the legal person or arrangement;
      vii. the resolution of the board of directors (if applicable) or any other authorized body or person to open an account; and
      viii. identification of those who have authority to operate the accounts.

7) In carrying out transactions with any person, a bank 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 bank is satisfied that it knows who the beneficial owner is; particularly, for all customers, the bank shall determine whether the customer is acting on behalf of another person, and shall then take reasonable steps to obtain sufficient identification data to verify the identity of that other person.

8) Establishment of a bank's new business relationship with a politically exposed person shall be approved by a senior management member of the bank.
9) Where a customer has been accepted and the customer or beneficial owner 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.
10) Banks shall take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as politically exposed persons.
11) Banks shall obtain information on the purpose and intended nature of the business relationship.
12) Banks shall perform enhanced due diligence on high risk categories of customers, business relationships or transactions.
13) Banks shall give special attention to business relationships and transactions with persons, including legal persons and other financial institutions, from or in countries which do not or insufficiently apply anti-money laundering and combating terrorist financing laws.

5. Account Monitoring

1) Banks shall conduct ongoing due diligence measure on existing customers and business relationships, including scrutiny of transactions undertaken throughout the course of that relationship, to ensure that:

    a) the transactions being conducted are consistent with the bank's knowledge of the customers, their business and risk profile, and where necessary, the source of funds; and

    b) documents, data or information collected under the due diligence process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

2) Where banks are in a business relationship with a politically exposed person, they shall conduct enhanced ongoing monitoring.
3) Banks shall pay special attention to all complex, unusually large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose such as significant transactions relative to a relationship, transactions that exceed certain limits, very high account turnover inconsistent with the size of the balance, or transactions which fall out of the regular pattern of the account's activity.

4) Banks shall examine as far as possible the background and purpose of transactions specified under sub article 5.3 herein above and set forth their findings in writing.

6. Cross Border Correspondent Banking

1) With respect to cross-border correspondent banking and other similar relationships, banks, in addition to performing normal customer due diligence 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) document the respective anti-money laundering and combating terrorist financing responsibilities of each institution;

2) Where a correspondent relationship involves the maintenance of "payable-through accounts", banks shall be satisfied that:
    a) their respondent financial institution has performed all the normal customer due diligence obligations set out in these directives on those of its customers that have direct access to the accounts of the correspondent financial institution; and
    b) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent bank.

3) Where a correspondent bank fails to comply with national anti-money laundering and combating terrorist financing laws, banks 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.
4) Banks shall satisfy themselves that respondent financial institutions in foreign countries do not allow business relationship with shell banks.

7. Wire Transfers

1) For all wire transfers, of Birr 10,000 or USD 1000 or more, ordering banks shall be required to obtain and maintain the originator's:
    a) full name,
    b) account number or a unique reference number, if no account number exists,

c) complete address, and
d) date and place of birth (if possible).

2) For cross-border wire transfers of USD 1,000 or more or for domestic transfers of Birr 10,000 or more, the ordering financial institution or bank shall be required to include full originator information in the message or payment form accompanying the wire transfer.
3) Where several individual cross-border wire transfers of USD 1 000 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.
4) Banks shall adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information.

8. 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 laws and regulations;
2) Credit and debit card transactions are exempted from standard customer due diligence, provided that they are not used as a payment tools to effect a money transfer.

9. Record Keeping

1) Banks shall maintain all necessary records on transactions, both domestic and international, as stipulated in Ethiopian National Archives and Library Proclamation No. 179/1999.
2) Transaction records to be maintained by banks shall be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.
3) Banks shall ensure that all customer and transaction records and information are available on a timely basis to the National Bank of Ethiopia and other competent law enforcement authorities.

10. Reporting

A bank shall report to Financial Intelligence Center of Federal Democratic Republic of Ethiopia

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

11. Training programs

1) Banks shall establish ongoing employee training programs which at a minimum incorporate:

a) responsibilities under the bank's arrangements for money laundering and terrorist financing prevention;
b) policies, procedures 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;
c) audit function to ensure the bank's compliance with anti-money laundering and combating terrorist financing laws, directives, and internal policies and procedures;
d) domestic laws and bank standards related to money laundering and terrorist financing;
e) relevant typologies of money laundering and terrorist financing; and
f) potential risks, including reputational, operational, legal and concentration risks of becoming involved in laundering the proceeds of crime or terrorist financing.

2) A bank shall provide to the National Bank of Ethiopia the dates and descriptions of all anti-money laundering and combating terrorist financing staff training events, at the beginning of each financial year of the bank.

12. Effective Date

This Directive shall enter into force as of the 4th day of March 2010.