

PROCEDURES MANUAL

North Africa International Bank

PROCEDURE NOTE

TITLE: Transfers, Cash Remittances and Withdrawals

Anti-Money Laundering (AML) and Counter-Terrorism Financing (C.T.F) Combating Procedures.

1- Parties involved:

- * Banking Operations Department.
- * Treasury Department.
- * Branches.
- * Internal Audit Department.
- * Quality and Compliance Department.
- * Customer Support Officers.
- * Information Technology Department
- * AML/CTF Department.

2- Procedure's Subject:

The present procedure consists in the development of the special instructions aiming at detecting the techniques and mechanisms used in terrorism-related financing activities, describing the approach tending to combat Money Laundering and introducing protection methods against attempts to use the bank as a vehicle for such purposes and to overall protect the bank from being subject to Customer and Counterparty Risks mainly Reputational, Operational, Compliance and Legal Risks which are solidly interrelated.

3- General Recommendations:

A- To capture a List UNO - Central Bank of Tunisia and "Blacklist" countries and individuals as per Financial Action Task Force (FATF) and other sources in order to enable the Bank's Information System to detect the presence of any suspect entity in the Bank's overall activities.

B- To implement a surveillance system with automatic screening and filtration of all financial Inflows and Outflows exceeding the threshold amount of 100 Thousand Tunisian Dinars.

C- To perfectly know the entire Bank's customers by capturing, examining and continuously monitoring all the information related to them.

D- To keep all the papers and documents justifying all transactions and operations for 10 years.

E- To continuously keep Front-Office and Branches' personnel well informed and trained about techniques used in Money-Laundering activities.

F- To daily control adequacy of customers' transactions by monitoring noteworthy operations which are in excess of the threshold amount as integrated in the Filtration System.

G- To check and confirm Information System Data as to the possibility of the presence of a suspicious entity in the transaction .

H- To strictly compel transaction-handling Agents to revert to their Higher-Ranking Superiors, the Internal Audit Department, the AML/CTF Department and the General Management.

I- To inform the relevant authorities.

4- References:

- Law n° 2003-75 dated December 10, 2003 related to supporting AML-ATF international efforts.
- Decree of the Finance Minister dated September 10, 2004 related to the fixed amounts according to the articles 70, 74 and 76 of the law n° 2003-75 dated December 10, 2003.
- Decision n° 2006-1 dated April 20, 2006 of Tunisian Financial Analysis Commission.
- Decision n° 2006-2 dated April 20, 2006 of Tunisian Financial Analysis Commission.
- Law n° 2009-65 dated August 12, 2009 modifying and completing Law n° 2003-75 dated December 10, 2003 related to supporting AML-ATF international efforts
- The Forty Financial Action Task Force (FATF) AML recommendations.
- The Nine Financial Action Task Force (FATF) CTF recommendations.
- The Wolfsberg Group Guidance for Managing Money Laundering Risks.

5-Carrying out of operations:

**** Account Opening and KYC due diligence:***

The personnel in charge of account opening must:

1- Conform strictly, when receiving the required Account Opening Documents, to the compulsory verifications of the Original Documents. Plausible answers must be obtained regarding the reason of the choice of the Bank and the nature of the activity and operations to be transacted. The most important factor in AML/CTF is the perfect knowledge of the customer (KYC Due Diligence). This is perfectly applicable to all types and phase of Money Laundering: Placement, Structuring and Integration

The verifications and Inquiries will be enhanced (Enhanced Due Diligence) in case the customer is a PEP (Politically Exposed Person) or situated in a Risky Geographical Zone.

If a doubt arises as to the possibility of an AML/CTF link, the opening of the account will be rejected and the AML/CTF Department will be advised.

This verification must be carried out as follows:

A- If the customer is an **Individual**, on the base of the Identity Card for Tunisian Nationals and documents justifying the identity (passport, residence card), acknowledged by Tunisian Authorities bearing the photograph, address and activity for foreigners.

B- If the customer is a **Corporate Body**, based on official documents certifying:

* Its Constitution, Legal Status or Social Denomination, Legal Form, Head Office registered address and its activity;

* Identity and place of residence of its managers and any other persons mandated to run the accounts and liable on behalf of the said entity.

* Identity and place of residence of the principal shareholders or senior partners.

2- File copies of all said documents and update them whenever necessary.

3- Capture all the relevant information on the **Customer's System File** on the Bank's Information System.

4- Edit the **Customer's System File** and have it signed by the Branch Control Officer after verification of conformity between the stored information and the **Material File** of the customer.

- 5- Forward the whole **Material File** to the Branch Manager for acceptance.
- 6- Keep copies of all customers' official documents, certified as original by the account opening agent, in the **Material File** of the customer.
- 7- Regularly update the information related to the customer.
- 8- Accomplish fresh investigations about any customer in case Money Laundering or Terrorism Financing doubts arise.
- 9- Properly classify the **Material File** of the customer in order to facilitate an easy Grasp of Information; this task should be done by one sole person in order to avoid any risk of loss or misuse.
- 10- Preserve all the customers' **Material Files** and the documents related to their identity for a 10 year-period at least as from the end of relation date.
- 11- Preserve documents and information related to the executed operations and transactions on an electronic medium or as documents (papers) for 10 years taking effect as from their realization date, without excluding the possibility of their consultation whenever needed. KYC is a life time customer monitored process.

The Branch Managers and their respective Front Line Offices must be watchful when:

- * Many accounts for the same entity are opened; they should be able to take adequate measures and to evaluate the real opportunities offered to this entity.
- * The multiplicity of addresses or domiciles of a group without plausible reasons.
- * The absence of apparent relation between the account holder and the mandated person running the account.
- * The flagrant incoherence between the real activity and the company's legal framework.
- * The opening of accounts does not correspond to the head office's address and/or to a local activity.
- * The existence of a head office abroad notably in a Risk Country.
- * The remittance of checks to the bearer.
- * The reluctance of the customer to provide information.
- * The provision of false information or information which is difficult to verify.
- * The execution of operations with Risk Countries.
- * The frequency of Cash Withdrawals or Cash Remittances with amounts inferior to the detectable threshold of noteworthy operations.
- * The execution of exceptional operations noteworthy by the importance of their amounts or execution methods (filtration Process system for transactions exceeding 100 thousand Dinars).
- * The execution of a transfer further to multiple items collections.
- * The frequent access of the customer to the personal safe deposit box followed by Front-Office transactions.

Obligation of verifying the identity of Foreign Correspondent Banks:

The appropriate measures must be taken:

- * To make certain that the Correspondent Bank is an Authorized Bank and controlled by the relevant authorities of its country of origin or the country where it is established.
- * To collect enough information about the Correspondent Bank in order to identify the type of its activity and to assess, by referring to information available, its reputation and the efficiency of the controls it is submitted to.
- * To verify if the Correspondent Bank was an object of an AML ó CTF inquiry or an intervention by the Relevant Control Authority.
- * To assess its Internal Control System within AML ó ATF context.
- * To obtain the agreement of the General Management before initiating a relation with a new Correspondent Bank.
- * To define by writing all the responsibilities of the Correspondent Bank.

Verification of Foreign Incoming Financial Transfers and Cash Remittances:

- * The person in charge of Money Transfers Operations must be vigilant notably in the following cases:

- 1- Operations with Correspondent Banks located in a Risk Country.
- 2- Operations with countries where the customer does not have a known activity.
- 3- Collections or Transfers coming from or forwarded to Risk Countries.
- 4- Unidentified Transfer Ordering Parties or Beneficiaries.

When the dubious nature of the transaction is ascertained, the person in charge of transfers gives notice to the Higher-Ranking Superior and defers the execution of the transaction; if the doubt persists, the Higher-Ranking Superior informs the AML/CTF Department, the Internal Audit Department and the General Management.

The AML/CTF Department will advise the Correspondent AML/CTF to declare the suspicious operations to the Tunisian Financial Analysis Commission according to the model annexed to the Commission's decision n°2006-01 dated April 20, 2006.

Under the orders of the Tunisian Financial Analysis Commission, The Bank must freeze the funds object of the declaration and capture them in a stand-by account.

If the Commission doesn't communicate the results of its enquiry to the Bank within five working days from the date of the declaration, its silence is an implicit authorization to unfreeze funds.

The person in charge of handling Money Transfers must carry out monthly controls based on an edited statement of all Incoming Transfers during that period with the complete identity profiles of beneficiaries. This control will be made according to the frequency of transfers in favour of the same entities and the degree of relevance to the customer's activities; these findings will be communicated to the Higher-Ranking Superior who must inform the Internal Audit Department for further inspection.

The information will be examined by the Internal Audit Department. In case dubious transactions are noticed, a report must follow-up to the General Management together with a copy to the AML/CTF Department which will advise the Correspondent AML/CTF to make a declaration to the Tunisian Financial Analysis Commission.

Cash Remittances and Withdrawals:

Deposits to and Cash Withdrawal from Non-profit Organisations' accounts can be related to Money Laundering.

Acts of control and verification of the conformity of the client's identity are particularly applied to occasional customers for each Cash Operation when its value is equal or superior to TND 10.000 or a Foreign Currency Operation for the same value; the Agent in charge must keep a copy of each beneficiary's Identity Document when this latter doesn't have any account in one of the North Africa International Bank (NAIB) Branches. This concerns notably Cash Withdrawals, Cash Remittances and Foreign Cash Exchange.

Are not concerned, all operations the value of which is inferior to the fixed amounts according to the previous paragraph, unless in case of suspicion or recurrence of these operations by the same individual.

Is meant by Occasional Customer, as per the present directives, every person realising an operation without having a contractual or usual relation with the Bank.

The persons in charge of such operations must be vigilant when conducting their work, notably as concerns, on one hand, the respect of the bank's legal obligations according to the Law n° 2003-75 the Law n° 2009-65 and the decree of the Finance Minister dated September 10, 2004 and, on the other hand, the discretion and know-how necessary in handling and conducting customer's daily operations..

AML - CTF is everyone's business as it is the case for Customer Support Officers who must:

- Examine the origin of funds.

- Control if the operation is within the activity and the Patrimony of the customer.
- Ask the concerned customer about the origin of funds, to explain the operation and the Identity of the Beneficiary
- Keep, in case of unconvincing answers, plausible justifications for the transaction.
- Inform the relevant hierarchy and the AML/CTF Department about unusual transactions, complex conditions and transactions without evident economic justifications or licit object.

Additionally, the Branch Managers must declare, monthly, to the Audit and Inspection Department all the Cash Withdrawals and Remittances done in amounts inferior to the Finance Minister limited maximal amount fixed by decree in case of a repetitive and unjustified character and without correlation to the normal activity of the concerned customer.

The Internal Audit and Inspection Department examines these operations in the framework of the prevailing regulations and reports to the General Management whenever suspicious transactions are noticed. The AML/CTF Department will also be informed. This latter will charge the Correspondent AML/CTF with the declaration of these suspicious operations to Tunisian Financial Analysis Commission.

*** Capture of UNO-FATF-CBT lists :**

• An active account of a person, whose name is ONU listed might reveal a possible link with Terrorist Activity

NAIB's Information System allows an identification of all parties Listed by ONU, Tunisian Central Bank or The Financial Action Task Force (FATF) and other Credible Sources (U.S OFAC list, World Bank, IMF, U.E and other Governmental and Non governmental Sources) as being involved in money Laundering or Terrorist Activities and High risk Countries. This system indicates to the persons in charge of Financial Transfers, Cash Withdrawals, Cash Remittances and Cash Exchanges, or any other Customer Current Transactions the presence of one or more suspicious parties (Ordering Party or Beneficiary), the possible dubious nature of a Particular Transaction, the presence of a Risk Country (Countries identified as being non-cooperative in the fight against Money laundering, lacking appropriate Money Laundering laws and regulations, subject to UN sanctions, having significant levels of corruption or criminal activity, supporting and financing Terrorism)

In this context, the Information Technology Department will capture, monitor and update these lists in the Bank's Data Base so as to permit real-time identification as the transaction is being carried-out.

*** Obligation of informing the hierarchy and Relative Authorities:**

When carrying out their duties and in case a dubious transaction or operation is identified, within the framework of the present procedure, the hierarchy must be immediately informed.

The Higher Ranking Superior will verify the veracity of information and whether the operation should be the object of a declaration to relevant authorities according to the prevailing regulations. If the doubt persists, the Declaration of Unusual or Dubious Transactions or Operations must be filled, remitted to the AML/CTF Department and in all cases a report about the said transaction will be written.

This report is addressed together with a copy of the declaration, within 24 hours from the initiation of the transaction, to the General Management and the Internal Audit Department.

It is worth noting that any person, having uncovered such transactions, will benefit total immunity even in the case of groundless doubt.

Nevertheless, work of this kind must be conducted in total secrecy and the involved customers should never be informed about the Suspicion Declaration filed against them.

END OF THE PROCEDURE.

This Procedure is updated quarterly.

Last reviewed: June 2010