

BANK'S POLICY ON ANTY-MONEY LAUNDRING (AML)

The Principle Of Know Your Customer

(KYC)

The struggle against funding of terrorism and accurate registration of

The information of customers

Al Baraka Bank S.A.L - Lebanon

Beirut - Lebanon

AL BARAKA BANK POLICY ON ANTI-MONEY LAUNDRING (AML)

THE PRINCIPLE OF KNOW YOUR CUSTOMER (KYC)

The Struggle against funding of terrorism and accurate registration of the information of customers

Such policies, procedures and control methods of AL Baraka Bank S.A.L. applying to all of its shareholders and employees in the light of the principles of Anti Money Laundering, blocking the funds for terrorism and "Know Your customer", and in the framework of prevailing Lebanese laws and regulations and the Diligence and prudence agreements for which Lebanon is a part of.

1. Purpose:

- a) To prevent funding of terrorism and anti-money laundering through the abuse of our Bank.
- b) To declare legal and administrative responsibilities of the Bank and all the staff.
- c) To ensure the consistency and compliance with policies, procedures and control methods of our Bank to the laws regulations which are empowered by the law.
- d) To reach conformity and cooperation in correspondent banking and international agreements.
- e) To continue the activities of the Bank in a safe way and to preserve the quality of its customers and its reputation.

2. Scope:

This policy, control methods and procedures comprise the Head Office and the whole branches.

3. General Framework:

The bank and the whole staff should have a standard level of knowledge and information about the following topics.

- a. Concepts of criminal activity and the laundering of money.
- b. Levels of money laundering.
- c. Methods of money laundering.
- d. Blocking the Funding of Terrorism.

Taking into consideration the types of services which would be presented to people and the Institutions with whom a temporary or permanent relationship is to be established, a comparison and check of the local and international blacklists will certainly be realized, additionally.

The protection against transactions of money laundering originating from international Crimes is going to be realized as a result of adoption and application of the principles in this policy document by all the employees of the Bank.

A maximum attention and care will be taken in the acceptance of people and institutions as Customers whose wealth and funds are subject to the suspicion of illegality.

In line with the general principal that a relationship with customers should be based on mutual trust, sincerity and mutual exchange of information, institutions or people who refrain from filling the documents and identification forms will not be accepted as customers.

On the basis of the principle that "customer accounts should be opened only in the name of real clients", it will be made sure that no accounts are opened under aliases or Unknown names on behalf of third parties even if the real clients desire so.

A continuous surveillance will be done to observe whether or not the person himself /herself accurately uses the account which is opened on behalf of him/her.

The demands of third parties to open an account in the name of proxy or more than one person will not be accepted, unless the purpose and necessity to open the account is explained and it is documented that they are clearly and legally authorized by the real client. (The accounts which are opened for people or children who are under guardianship are exceptions).

No relationship with possible clients will be instituted if prior assessment provides suspicion, document or information about the physical assets of these people.

Irreversible and risky banking services such as renting safe deposit boxes, cashing individual foreign exchange checks, or giving letters of guarantee in transactions will not be provided except the cases in which those customers are very well known and target ones.

b) Admission of the Customer and Responsibilities:

During the process of acquiring new customers or acting as an intermediary for the transactions of third parties, a determination of the identities of customers, a record of the stated addresses, and legally necessary documents and data are maintained. Ratification of these data is realized and they are kept in physically or electronically safe places.

B1) Method of: Identity Determination and Recording the Stated Addresses.

Identities are determined and stated addresses are recorded according to the types of customers and levels of banking service. Copies of records are attached to transaction papers and are saved in the system seeing the original samples of legally required identity documents.

- The information and data about legal entity and structure of the customer, his real name and company name, his administrators and address, the documents which authorize the legal personality is ratified by reference to official records.

A ratification of authority and a determination of identity are performed about the person who claims that he/she acts in the name of the customer.

- The act of identity determination is performed in line with the documents and responsibilities which are stated in the law.
- The data about the identity of payment customers is updated. Changes of authority and conditions are forwarded from the Special Investigation Committee and kept in the system
- The account can be opened after getting the true information about the customer and after a ratification of the data and documents.

B2) Persons and Institutions who cannot be accepted as Customers.

- Persons whose Real Identity and Addresses could not be established.
- Persons and institutions who desire to open an account under a name which differs from their original and real names, who abstain to fill the documents of identity, who are unwilling and misleading about this subject or who provide data which cannot be ratified are not accepted as customers. These persons and Institutions are not considered as target customers once again.
- Persons and Institutions in the Blacklists on Terrorism and Anti-Money Laundering which are issued by Public Authorities.

Shell Banks

Organizations (shell banks) that have no physical address in a given country, have no employee to work at least full day or is not subjected to the permission and control of a public authority in terms of banking transactions and records, that are not branches of any esteemed bank which is subjected to acceptable procedures and control mechanisms in terms of banking transactions and prevention of money laundering are not accepted as Customers and their direct or indirect transactions are not mediate.

B3) Real and Legal Persons who's Demands are to be accepted as Customers should be considered with due diligence and utmost Care.

A high level of attention is paid when admitting transactions of customers whose activities are in risky fields like fuel oil stations and private foreign exchange offices. Especially money orders of private foreign exchange offices are realized after utmost assessment.

Correspondent Banking

The points to take into account when establishing a correspondent banking relationship are stated below. About the bank with which the relationship would be established; the methods that the bank uses to prevent money laundering and funding of Terrorism are checked and its level of appropriateness to the necessity of "know your customer" is assessed.

The approval of high level executives is received before installing a new relationship of correspondence. It is assessed whether the correspondent bank has some customers who can directly reach the accounts, and if so, whether the obligations of attention to these customers are fulfilled. With this aim, financial institutions who demand to open a correspondent account are required to fill the questionnaires in which aforementioned data are entered.

Exceptional attention

An exceptional attention is paid when opening an account for the following Profession groups and Sectors. Identity of the customer and the data about the sector are registered in a careful and complete way and the accounts of Customers are kept under a continuous control.

- = Private foreign exchange offices.
- = Goldsmiths, jewelers and traders of precious stones.
- = People who are settled abroad. (Especially settled in geographically risky regions).
- = Travel agencies, carrying passengers and cargo.

- = Casinos, operators of the gambling houses.
- = Owners of auto galleries who sell luxury vehicles.
- = Dealers in antiques, art galleries and carpet sellers.
- = Significant real-estate agents and their representatives, agencies and commercial proxies.
- = People who provide the service of renting for air and naval vehicles.
- = People who produce and trade leather articles.
- = People who produce and trade auto spare parts.
- = People who act in job branches in which use of cash is intensive (operators of parking lots/buildings, restaurants, gas station, lottery and newspaper distributors, people who trade stationary goods and toys) Factoring firms.

Cash Operations

In case a transaction normally effected as a payment on account is desired to be effected as a cash operation by the customer, controls and documentations are made in a more careful manner.

Electronic Transfers

Full names and addresses of beneficiaries and orders are detailed in transfer messages for transactions of money orders which are sent. If the information about orders and beneficiaries of money transfers which are received is incomplete, these transfers are interpreted as suspicious and further investigated. Identity and address determination of persons and institutions that are paid, are carefully realized and documents are kept by the unit who paid the money orders to the beneficiaries. If necessary, suspicious transaction declaration form is filled and sent to Compliance Dept.

Detection and Announcement of Suspicious Transactions:

Employees of the Bank should show extreme attention while working with customers:

- Who demand transactions that visibly have no legal or economic aim whose income is not directly related to and proportional with his/her Business.
- Who are unwilling or abstaining to provide information and documents in the framework of responsibilities that are stated in the law; who abstain from keeping the required records and reports.
- Who give misleading information or data that are impossible to confirm.

- Who demand credits with no economic logic or without stating the purpose for the credits.
- Who make transfers of money in large scales and in extraordinary amounts to geographically risky countries and territories.

In case of such transactions the related data and documents are gathered to provide to Compliance Dept.

Description of the Suspicious Transaction

A suspicious transaction is the existence of a suspicion that the money or assets about the transaction is earned through illegal ways. The responsibility of the announcement of a suspicious transaction comprises the agencies, branches and representatives of the responsible persons. A transaction is described as 'suspicious' in case there are concrete doubts about whether the income of the customer is legal or not, or if there are serious evidence indicating an illegal action is done by the customer.

Different Types of Suspicious Transactions

1. Unwillingness to provide the usual information given by all customers for transactions. Presenting a doubtful document and providing false financial information. The incongruity of the transaction with the announced goal of the customer.
2. Transfers of unusual and large amount of funds from and to offshore centers and Countries where terrorist institutions, illegal drug trafficking and smuggling exist.
3. Detection of an unusual increase in the bank accounts of the person or existence of large amounts of idle money in these accounts.
4. Transfers of considerable amount of money to the accounts and addresses with whom the customer has no permanent business relationship.
5. Big amounts of cash movements from abroad of from within the country to the accounts of a person who has no commercial past and background, who has no clear source of business and who has a bad reputation.
6. Electronic fund transfers without an explanation and a request to receive them as cash, considerable amount of money transfers to or from abroad generally without using an account.
7. Keeping multiple accounts in which exist unusually big sums when considered altogether or several accounts that have small amounts which could be merged in one account, or continuously making transactions of smaller amounts so that each transaction is below reporting threshold.
8. Payment of many people to the same account without reasonable explanation, or transfers from many accounts to the same account.
9. Existence of accounts, that are disproportionate with the activities of the firm, and transfers among these accounts, transactions from these accounts that obviously

have no commercial motives, unusual and irregular payments to persons who have no clear relationship with the firm or the customer.

10. Receiving large amounts of money or credits as loan and repayment of this loan in a very short time without a reasonable explanation.
11. Receiving a credit within the country by stating an abroad account as collateral, and then, not paying this credit and thus causing a situation where the institution who gave the credit has to seize the bank account and has to transfer the money to the country, or paying a credit received within the country through transfers from abroad Off-shore banks.
12. Not providing information about the question of where the credit is to be used and when the credit will be paid back during the process of demanding a credit.
13. Movement of similar amounts of money in similar dates in and out of the country.
14. Others.

Rules for Reporting to the Compliance Officer and Responsibilities

After a short investigation of the suspicious transaction by the employee who realized the transaction, a detection of the identity of customer is necessary and the suspicious transaction announcement document is filled and with two signatures, those of the branch Manager and the branch Manager and the employee who realized the transaction, and is then sent to the Compliance Officer and then sent to:

**** Notifying the Local Authorities:**

Suspicious transactions are notified to the special investigation committee.

**** Secrecy and Confidentiality:**

No information is provided to third parties or to persons who are related to the suspicious transactions, except to the authorities who are not deemed by the law as objectionable in terms of being informed.

** Keeping the Records:

Documents and records that related to the transaction are kept for ten years regardless of whether they are subject to announcement or not.

** Surveillance, Internal Control and Reporting Activities:

The special Committee for fighting anti money laundering is responsible for tracking the suspicious transactions in order to determine and to prevent them through the activities of conforming to the requirements and responsibilities against money laundering. The related reports are sent to the Compliance Officer.

The Compliance Officer informs the members of the Internal Control Center and the Audit Committee about the changing rules and legislation to make better control and conformity of the activities with the related principles.