Unofficial translation of
AML/ CFT Regulations for Banks

Introduction

The Central Bank of Egypt (CBE) issued on 19 November 2003 AML Regulations for Banks, according to the Anti money Laundering Law No. 80 of 2002. The Law defined the AML obligations for financial institutions, mainly Egyptian banks, branches thereof and branches of foreign banks operating in Egypt.

After the issuance of the regulations, new international developments have emerged in the arena of combating money laundering, due to which combating terrorist financing was added to AML. FATF Forty Recommendations were updated and issued in their new form in June 2003, and FATF issued the Nine Special Recommendations on Terrorist Financing. As a result, the Forty plus Nine Recommendations are now regarded as international standards that must be observed by countries in fighting these two phenomena.

In response, it has become a necessity to issue new regulations, taking into consideration such developments while instituting already existing practices of opening accounts and conducting banking transactions and the AML procedures related thereto. The new regulations aim at honing and activating efforts so as to keep pace with international developments in AML/CFT, while ensuring strict compliance of banks and branches of foreign banks operating in Egypt with such regulations.

These regulations shall apply to all branches and financial companies abroad affiliated to Egyptian banks. It should be noted that in case of any discrepancy between these regulations and those applied in the host country, the more strict regulations shall be applied, without prejudice to the legislations or regulations of the host country.

In case of failure to take proper AML/CFT measures due to such legislations or regulations, CBE should be notified.

First: Know Your Customer (KYC) Rules

When setting internal regulations for identifying customers, their legal status, be they natural or legal persons, beneficial owners and correspondent banks, KYC rules issued by the Money Laundering Combating Unit, pursuant to Item 13 Art. 3 of the Executive Regulations of AML Law, promulgated by the Prime Minister Decree no. 951 of 2003, should be followed.

Second: Money Laundering and Terrorist Financing Reporting Officer (MLRO)

MLRO is the compliance officer who is responsible for combating money laundering and terrorist financing in a bank. A substitute replacing MLRO when absent should be assigned. The Money Laundering Combating Unit (MLCU) should be notified in case of changing any of them. MLRO and his substitute should meet the following criteria, and be provided with the following warrants, powers and responsibilities:

1. MLRO Criteria

Banks should ensure that the MLRO and his substitute meet the following criteria:

A. Being of a senior job rank
B. Having adequate academic qualifications and sufficient expertise

2. Warrants and Powers of MLRO

In carrying out his responsibilities, MLRO should be independent, and be provided with adequate means ensuring effective performance of his duties. This entails:

- MLRO should not be assigned with tasks in conflict with his duties

- MLRO should be permitted to access all information, review all records or documents deemed necessary for examining unusual and suspicious transaction reports referred to him, and contact any bank staff whenever necessary for carrying out his assignments

- MLRO should be permitted to present reports to the bank's senior management, board of directors, or any sub-committee related thereto, so as to help ensure further improvement and effectiveness of AML/CFT systems and enhance staff compliance therewith.

- Secrecy should be guaranteed for all procedures as to receiving the referred to reports on unusual and suspicious transactions, their examination and reporting to the MLCU

3. Responsibilities of MLRO

MLRO responsibilities should be consistent with the bank's size, resources and applicable systems. Generally, MLRO should be assigned with the following tasks:

A. Examining disclosures on unusual transactions produced by bank internal systems; disclosures on suspicious transactions submitted by bank staff, substantiated with reasons of suspicion, and disclosures submitted by any other entity.
B. Reporting to MLCU transactions suspected of involving money laundering or terrorist financing on the forms designed for this purpose.
C. Taking decisions for filing reports on the transactions, wherein suspicion is found to be groundless, stating the reasons behind this decision.
D. Proposing measures deemed necessary for developing and updating the bank AML/CFT policies, and relevant systems and procedures, to enhance efficiency and effectiveness thereof, and keep pace with local and international developments.
E. Ensuring compliance of different bank branches with AML/CFT laws, regulations and internal systems, via off-site and on-site supervision.
F. Cooperating and coordinating with the competent administration at the bank to set AML/CFT training plans, proposing training programs necessary for carrying out such plans and follow up their implementation.
G. Preparing a periodical report -at least once a year- on the bank AML/CFT activities, and presenting it to the board of directors. The board of directors should review the report, make comments thereon and send it to MLCU, with its comments and decisions. The report must include at least the following:

    - Efforts exerted during the report period on unusual and suspicious transactions and the decisions taken in their regard.
    - Weaknesses found during the periodic review of the bank AML/CFT systems and procedures, and proposals to rectify such weaknesses, including the bank internal disclosures on unusual transactions.
    - Any amendments to the bank AML/CFT policies, internal systems, or procedures during the period covered by the report.

- Degree of commitment to the implementation of approved off-site and on-site supervision plans to assess compliance of different bank branches with AML/CFT laws, regulations and internal systems.
- The plan set for off-site and on-site supervision on bank branches for the period following the reporting period.
- Details of AML/CFT training programs for the bank staff during the reporting period.

Third: Procedures of Reporting Suspicious Transactions

1. Banks should report all transactions suspected of involving money laundering or terrorist financing, including attempted transactions, regardless of their volume.
2. The report should include detailed reasons and causes that led the bank to suspect the transaction.
3. The report shall be made in the unified form designed by MLCU for this purpose and which has been sent to the bank along with its fill-in instructions. All data and copies of the documents pertaining to the suspicious transaction should be attached with the form that has to be filled in according to the Instructions referred to above.
4. Where banks file transaction reports, at least copies of the following documentation should be attached:

    - Account opening application
    - Identification card
    - Supporting documents for the reported transaction

5. Procedures pertaining to reported transactions suspected of involving money laundering or terrorist financing, or data related thereto shall not be disclosed to the customer or beneficiary, or to any other entity, except to the authorities and entities responsible for enforcing the provisions of the Anti-Money Laundering Law and its amendments.

Fourth: Record Keeping

1. Types of Records and Documents that Should be Kept

Banks should keep the following documentation**:**

A. Records and documents of customers and beneficial owners, provided that such records and documents include account opening applications, copies of identification cards, for natural and legal persons and copies of correspondence therewith.
B. Records and documents pertaining to customer transactions, provided that such records and documents include data sufficient to reconstruct each transaction.
C. Unusual transaction disclosures and the documents proving review thereof.
D. Records and documents of suspicious transactions, provided that such records and documents include copies of reports sent to the MLCU and the relevant data and documents.
E. Records and documents of the disclosures, for which filing decisions have been taken by the MLRO
F. Records on training programs, provided that such records include data on all AML/CFT programs offered to bank staff, names of trainees, their divisions/departments, content and timeframe of training programs, and training entity, whether at home or abroad

2. Conditions for Record Keeping

Banks should observe the following conditions when keeping the records and documents referred to in the preceding Item**:**

A. Securely keeping all records, documents and reports, while maintaining backup copies thereof in another place.
B. Records, documents and reports should be kept in a manner ensuring that they are easily accessible and retrievable. Any data or information requested should be sufficiently provided without delay.

3. Period of Record Keeping

Records and documents should be kept for a minimum of five years. Starting date of such period varies according to record and document type as follows:

a- Records and Documents of Customers and Beneficial Owners

Records and documents of customers and beneficial owners should be retained for at least five years as of the date of closing the account, or transaction execution for customers with no bank accounts.

b- Records and Documents Pertaining to the Transactions Carried out with Customers

Records and documents pertaining to such transactions should be maintained for at least five years from date of closing the account, or transaction execution for customers with no bank accounts.

c- Other Records and Documents

The following records and documents should be retained for at least five years:

- Unusual transaction disclosures, as of date of production
- Records and documents of suspicious transaction reports submitted to the Unit, as of date of submission, or until a decision or final ruling thereon is issued, whichever is longer
- Records and documents of suspicious transaction reports, for which filing decisions were taken by MLRO, as of the date of taking the decision
- Records on training programs, as of the date of program completion

Fifth: Internal Control Systems

Banks should establish appropriate internal systems, ensuring sound application of legislation and regulations, including necessary AML/CFT policies and procedures. Such systems should be reviewed periodically to measure compliance therewith, find out any vulnerabilities or weaknesses and take measures necessary for rectifying such weaknesses. The following points should be observed:

1. Developing a clear AML/CFT policy approved by the board of directors or the regional manager of branches of foreign banks, ensuring sound application of relevant legislation and regulations, while updating such policy regularly
2. Setting detailed AML/CFT procedures in writing, defining exact duties and responsibilities according to the relevant policies

3. Ensuring that internal controls, policies and procedures can detect unusual transactions or transactions conducted with suspected customers and bring such transactions to the notice of MLRO
4. Developing a suitable mechanism to ensure compliance with the AML/CFT policies and procedures in place
5. Developing systems that enable the internal audit function, in coordination with MLRO, to examine existing systems and ensure effectiveness and efficiency thereof in AML/CFT, as well as propose whatever necessary to improve and upgrade such systems

Sixth: AML/CFT Training

Banks should develop continuous plans and training programs to train their staff in order to enhance compliance with AML/CFT rules and systems, and ensure that they are updated on the latest AML/CFT developments related to ML/TF methods and trends and systems for their prevention, and on the latest relevant developments on the regional and international levels. Developing and implementing such programs should be carried out in coordination with banks and MLCU. In this context, the following points should be observed:

1. Providing training to all bank staff and departments

2. Seeking assistance in the implementation of training programs from the Egyptian Banking Institute, or specialized institutes, established for this purpose, or those whose objective, inter alia, is training on combating money laundering and terrorist financing, locally or internationally, while benefiting from local and international experience in this respect. Such assistance should be consistent with the general policy set by MLCU.

3. Coordinating with MLRO on selecting staff to be nominated for attending training programs in this field.

4. Reporting to MLCU all data related to programs referred to in Section IV/1/f.

Seventh: AML/CFT Red Flags

1- Red Flags for ML Suspicious Transactions

Detecting transactions suspected of involving money laundering requires having an adequate knowledge for all bank staff of the Anti-Money Laundering Law, Executive Regulations thereof, and AML Supervisory Regulations, in addition to accumulated experience and knowledge acquired from training. Following are examples of transactions that require enhanced diligence to examine existence of suspicion:

A. Cash Transactions

- Large cash deposits not consistent with the customer business
- Frequent cash deposits, the total of which, within a specific timeframe, is inconsistent with the customer business
- Customers using multiple accounts in depositing cash amounts, the sum of which in a short period of time is large
- Large cash deposits transferred within a short period of time to other entities with no apparent connection to the customer business
- Frequent cash deposits by different persons or entities in a customer's accounts, for no apparent purpose, and with no relationship between such persons or entities and the customer
- Large cash deposits by customers using checks or other banking instruments or by those whose business is not cash intensive
- Frequent cash deposits in a number of branches of the same bank, in a short period of time, either through the account owner or others
- Large and unjustified increases in cash deposits, especially if such deposits are followed by transfers, during a short period of time, to other accounts with no apparent connection with the customer
- Large deposits or withdrawals by ATMs to avoid direct contact with bank staff, especially if such deposits or withdrawals are inconsistent with the customer business
- Large cash deposits and withdrawals from dormant or inactive accounts
- Frequent cash withdrawals shortly after being deposited, with no justification
- Customer using different ATMs to make cash transactions simultaneously on the same account

B. Large and Complex Transactions

- Conducting several interlinked transactions from a bank account to another, in a manner that funds return to the bank from which transactions was initiated.

- Presenting checks for collection in large sums, inconsistent with the customer business, absent of clear and justified relationship between the beneficiary, withdrawer or the person endorsing the check.
- Carrying out credit and debit cash movements on the same account during short periods of time, with no apparent justification

C. Transfers

- Receiving transfers in large amounts, especially for those accompanied by instructions to pay in cash, inconsistent with the customer business
- Frequent incoming or outgoing transfers from different parties with no clear relationship to the customer
- Frequent and large transfers from territories known for certain crimes as planting or trafficking drugs, or from countries with insufficient AML/CFT systems
- Receiving large transfers from abroad to dormant or inactive accounts
- Frequent outgoing transfers in large amounts, paid for in cash, which are inconsistent with the customer business
- Frequent transfers, the sum of which during a certain period of time is inconsistent with the customer business
- Customers using their accounts as an intermediary account for other parties or accounts

D. Letters of Credit and Bills for Collection

- Importing or exporting goods, the value and nature of which are inconsistent with the nature or volume of the customer business
- Indications of big differences in value of the goods written in LCs or bills for collection and their real value
- Requesting to amend the name of the beneficiary from the LC or bills for collection before effecting the payment, with no clear justification
- Issuing multiple LCs or transacting through bills for collection, in a manner inconsistent with the customer business
- Issuing LCs against financial collaterals which are inconsistent with the customer volume of business or with his previous transactions with the bank
- Unusual payment terms, or payment for third parties with no clear relationship with LC or bills for collection

E. Letters of Guarantee (LGs)

- Multiple LGs inconsistent with the customer volume or nature of business
- Beneficiary requests to liquidate LGs shortly after being issued by the bank, without any justification
- Issuing LGs against financial collaterals, inconsistent with the customer volume of business or his previous transactions with the bank

F. Credit

- Applying for loans guaranteed by assets owned by third parties, or borrowers presenting extra guarantees owned by third parties, with no clear relationship between them;
- Acquiring credit facilities against guarantees provided by a bank operating abroad, with no clear reason
- Customer requesting quick transfer of loan sum to other banks, with no clear purpose
- Unexpected and early repayment of debts by the customer or third parties, especially defaulted customers.

G. Credit Cards

- Unjustifiable overpayment on credit card account
- Frequent use of the full card limit, followed by full repayment of the debit balance
- Frequent withdrawals of the maximum daily cash limit

H. Foreign Exchange Transactions and Travelers Checks

- Purchasing and selling foreign currencies in large sums, inconsistent with the customer business
- Frequent purchasing or selling transactions of foreign currencies, the total sum of which during a specific period of time is inconsistent with the customer business
- Frequent unjustified requests to issue traveler checks, and other negotiable instruments;

I. Safe Deposit Services

- Frequent unusual visits by the customer to his safe box

- Unjustified renting of safe boxes by customers, not living in the precincts of the bank, specially when such service is provided by banks in the area where the customer resides
- Customers renting many safe boxes

J. Other Red Flags

- Unjustified exchange of small denomination banknotes with large denomination banknotes, in big amounts with no clear justification
- Customers refraining from providing sufficient or correct information. This includes personal or business information, such as purpose of dealing on the account, business nature or beneficial owners of dealing on the account
- Customers showing unusual interest in systems applied to detect unusual transactions, suspicion indicators or suspicious transactions reporting procedures
- Customers whose accounts are used in receiving or cashing large amounts of money without any clear purpose or relationship to the account owner or his business
- Customers avoiding direct or personal contact with the bank
- Accounts receiving frequent cash deposits or multiple transfers, closed or left dormant shortly thereafter
- Sudden change in one of the bank staff standard of living without clear justification

2- Terrorist Financing Red Flags

A. Accounts that receive deposits or transfers from non-profit local or foreign entities, especially if such entities are domiciled in countries known for supporting terrorism
B. Transactions conducted on the account of a non-profit organization, which are inconsistent with the pattern and size of the organization purpose or business
C. Large donations from a foreign entity to the account of a non-profit organization, especially absent of a clear relationship
D. Incoming or outgoing transfers to a country known for supporting terrorism
E. Incoming transfers for beneficiaries from countries associated with terrorist activities
F. Individual accounts receiving large transfers from unknown sources, the stated purpose of which is sustenance