Anti-Money Laundering & Counter Terrorist Financing Policy

Compliance Department

2016

Contents

1. Introduction

Money Laundering and Terrorism Financing are one of the alarming criminal phenomena at the international level given their close link with organized crime mainly drug trafficking. Lawbreakers have greatly benefited from the rapid advancements in IT and communications as well as transportation in addition to the exponential growth in the trade activity which led to huge cross-country flow of goods of services.

Money Laundering and Terrorism Financing are considered as one face for the same coin: Studies have proved that the majority of terrorism financing comes through money laundering.

Money launderers have taken advantage of the mergers in international capital markets and the technological developments in the banking and financial systems that have become major channels to transfer the dirty money anywhere in the world, hence disguising their illegal sources.

Given that commercial banks represent a haven for most money laundering and terrorism financing crimes, banks need to exercise a stringent monitoring role to detect and report suspicious transactions which constitute the most important practical means for combating money-laundering and terrorist acts. This requires putting in place clear Procedures and policies that mainly aim at protecting the bank's reputation and eliminating potential operational risks should the bank be used as a channel for money laundering operations. Local laws and monetary regulations that have been issued represent the general framework to be adhered to and adopt the necessary Procedures to ensure full compliance therewith. This is in addition to international requirements and laws that place conditions on internal and external banking transactions with correspondent banks

The efforts exerted by Bank of Jordan to implement those Procedures to ensure that money generated from suspicious activities does not pass through the bank's financial system will reflect positively on the bank's local and external image. It will also help the bank avoid any obstacles in managing its financial and banking operations.

2. *The Legal Framework for the Anti-Money Laundering and Counter-Terrorism Financing (AML-CTF) Act Policy*

Branches Operating in Jordan

1- Local Laws

- Law No.16 of 2007 amending Penal Code No.16 of 1960, Article 147(2).
- Banks' Law No.28 of 2000 Article 93 and 99/B

Anti-Money Laundering and Counter-Terrorism Financing Law No.(46) of 2007

2- Central Bank of Jordan (CBJ) Regulations

- Memorandum No. 51/2010 dated 23/11/2010

3- Instruction issued by the Anti-Money Laundering and Counter-Terrorism Financing Unit in accordance with the provisions of Laws and Bylaws

Branches Operating Abroad:

- Implement the Procedures adopted by the bank to the extent permissible by laws, bylaws, and regulations in the host country

- Wherever regulations in the host country are stricter than the requirements in the mother country, the stricter standards shall be applied. The bank shall notify CBJ of any restrictions or constraints that might limit or prevent the enforcement of the provisions of those regulations.

Affiliates of Jordanian Banks inside the Kingdom and Abroad

- Affiliates of Jordanian banks operating in the Kingdom unless those companies are under the supervision of another monitory body outside the Kingdom and which have issued AML/CTF regulations
- Companies affiliated with Jordanian banks outside the Kingdom to the extent permissible by effective laws and bylaws in the host countries. Wherever regulations in the host country are stricter than the requirements in the mother country, the stricter standards shall be applied. The bank shall notify the CBJ of any restrictions or constraints that might limit or prevent the enforcement of the provisions of those regulations.

3. Anti-Money Laundering and Terrorism Financing Definition

Anti-Money Laundering is defined as every criminal practice that aims at disguising the real source of money generated illegally through engaging into a series of consecutive operations that would eventually show that the money has originated from legitimate activities.

Terrorism Financing is defined as any banking operation including money depositing at any bank or financial institution that carries out banking operations or transfer to any party in order to make this money available to an individual, a group or an organization with intent to use such money in carrying out terrorist acts to disrupt public order or threaten the integrity of the society.

Thus, money laundering involves:

- Illegal possession or use of illegitimate money
- Investment of illegitimate money by any means through a series of banking operations or the purchase of non-fixed and fixed assets
- Provision of falsified information about the source of money to disguise the real source of illegitimate money.

Why is Money Laundered?

People holding illegal money need to give a reasonable justification of their source or otherwise their crime is exposed. Therefore, they engage themselves in a series of transactions and activities that would eventually be shown as the real source of their money.

Stages of Money Laundering:

The operations carried out for the purposes of money laundering are sometimes complicated and varied and they might not involve cash operations. In general, however, they undergo three main stages:

1. Placement:

During this stage, money generated through a crime or an illegitimate act is placed or invested, or it might enter the financial system through cash deposits or through the purchase of the various types of derivatives. This is considered the most difficult stage for money launderers since the dirty money is subject to detection of its illegal source. These operations are not necessarily carried out by real owners of the dirty money; a customer's account might be used as an intermediary to serve the real owner of the money against a commission.

2. Layering:

During this phase the relation between money and its illegitimate sources is concealed or disguised through carrying out a complicated chain of consecutive operations involving the purchase, sale, and transfer and any financial and non-financial activities that are difficult to track.

3. Integration

During this phase, laundered money is integrated into the economy making it difficult to distinguish laundered money from money generated from legal resources (showing money within the legitimate economic system)

4- Crimes Connected with Money Laundering

Crimes that can be the source of dirty money whose owners seek to disguise and detach from its original source vary, and they may include:

- Trafficking in illicit goods and services that are banned under internationally or locally mainly growing, trading, and manufacturing of drugs and narcotics.
- Cross-border smuggling activities of legal goods in efforts to evade paying customs fees and smuggling of illicit goods such as weapons.
- Embezzlement, theft, and scam
- Counterfeit of money, gold, and precious minerals and forgery
- Theft of antiquities and valuable belongings and armed robbery
- Espionage
- Political and administrative corruption and bribes through the illicit exploitation of public office in order to achieve personal gains.
- Tax evasion
- Black market operations
- Abduction, piracy, and terrorism
- Damage to the environment
- -Prostitution and gambling

5- Know Your Customer (KYC) Policy

Identifying the form of suspicious transactions cannot be regarded as the only preemptive measure against suspicious transactions. Neither should they be relied upon separately from the customer and the nature of activities performed by that customer. They could be significant signs but they do not necessarily mean that the underlying operation involves ML/TF. Thus, the form of suspicious operations should be linked with additional information related to the customer's personality, nationality, domicile, and the type and size of his activities, in addition to any other information that may provide a comprehensive understanding of the nature and type of transactions and the relations with the customer and his activities.

Main Elements of KYC's Policies (Customer Due Diligence):-

Customer Due Diligence refers to identifying the customer, checking his legal status, activities and purpose of the business relation, and the real beneficiary (if any), and verification of all the above information. It also refers to the ongoing follow-up of operations carried out within a continued relationship through any means specified in the respective legislation. It also entails identifying the nature of the future relationship between the bank and the customer and the underlying purpose.

The following elements constitute the main part and most important factor in eliminating ML/TF operations. They also serve as the backbone of operational risk management in the bank:

1- Customer acceptance
2- Risk based classification of customers
3- customer identification
4- Ongoing monitoring of high-risk accounts

1- Customer Acceptance -:

Customer Acceptance policy is considered the first firewall for avoiding potential risks arising from dealing with the customer. At this stage, it is possible to reject dealing with the customer altogether or assess the level of risks associated with that customer based on a number of factors: economic activity or nationality, political position, or public office. Following are the policies related to customer acceptance policies.

1. KYC's Procedures:(Customer Due Diligence)

1.1 Natural Persons' KYC Procedures:

1.1.1 Identification data must include the full name of the customer, his nationality, the permanent residence address, phone number, work address, type of activity, the purpose and nature of the business relation. The name of authorized signatories appointed by the customer to manage the account, their nationalities, and any other information deemed necessary by the bank.

1.1.2 For people who lack legal capacity such as minors, the bank must be furnished with relevant documents of their legal custodians in charge in handling such accounts.

1.1.3 In the case of persons dealing with the bank on behalf of the customer, a power of attorney or an authorization approved by the bank shall be provided as approved by the legal department. The legal department shall keep the original document or a certified copy thereof. The authorized agent shall be identified in accordance with the KYC's procedures as stated in Article (1).

1.2 Legal Persons' KYC Procedures

1.2.1 The identification data shall include the name of the legal person, legal form, names of owners, equities, authorized signatories, registered address, type of activity, capital, registration date and number, tax number, national ID of the establishment, names and nationalities of those authorized to manage the account, phone numbers and the purpose of the business relation. The bank shall be informed with the equity structure and provisions regulating decision-making powers that bide the legal person and any other information deemed necessary by the bank.

1.2.2 The existence and legal status of the corporate body, the name of its owners, and authorized signers shall be verified through examining the necessary documents i.e. Memorandum of Association, the Articles of

Association of the legal person and certificates issued by the Ministry of Industry and Trade and chambers of commerce and industry. If the corporation is registered abroad, an official certificate issued by the competent authorities shall be provided.

1.2.3 The bank shall obtain such documents that prove that the legal person has duly authorized the relevant natural persons to manage the account and shall verify the identification of the authorized person(s) in accordance with the KYC procedures.

1.2.4 Public shareholding companies shall be exempted from the condition of providing the names of owners and equities. The provision of data on the names of persons holding more than 10% of the company's shares shall be sufficient.

1.3 Procedures to Identify Non-Profit Organizations

1.3.1 The Know Your Customer information shall include the name of the non-profit organization, its legal structure, the address of the headquarters, the type of activity, date of establishment, the names of the authorized signers, their nationality, phone numbers, the purpose of the business relation, and any other information deemed necessary by the bank.

1.3.2 The existence and legal status of the non-profit organization need to be verified through examining the official documents such as certificates issued by the Ministry of Social Development or any other concerned entity.

1.3.3 Obtaining documents which shows that a delegation by the non-profit organization has been granted for normal persons authorizing them to... The authorized signer need to be identified in accordance with the Know Your Customer Procedures

1.3.4 The information and data obtained from the customer shall be verified through neutral and reliable sources including the official agencies that have issued the official documents. The database of the Civil Status Department that is available to banks and the Companies' Comptroller's Department website shall also be examined for the purpose stated above.

2- Customer Acceptance Policies:

2.1 It is vital that the name of clients are checked on the government/international lists prior to the opening their accounts If similar or identical names are found in the lists, the respective branch shall notify the AML-CTF Unit/Compliance and Risk Department to take necessary action and cease and desist from the relevant banking relation.

2.2 The customer shall fill in all data and information requested in the account opening form based on the supporting original official documents. Copies of

those documents shall be retained and with a notation stating that the originals have been perused.

2.3 The branch shall take all necessary actions to verify that data and information obtained from the customer are correct through neutral and reliable sources. Such verification sources include without limitation the Civil Status Department database to verify the accuracy of ID information and a water or electricity bill to ensure that the correct address has been provided.

2.4 The bank shall obtain all supportive documents on the nature of the customer's activity copies of which shall be retained with a notation stating that the originals have been perused.

2. 5 Customer identification data shall be updated once every two years, or whenever deemed necessary such as when suspicions arise on the accuracy or appropriateness of information obtained earlier.

2.6 When an account is opened by correspondence, the bank shall obtain a duly issued recommendation or certification verifying the signature of the customer by well-known banks or financial institutions in addition to a copy of the customer's ID. (No account may be opened for persons residing in the same country where a branch is already operating).

2.7 The bank shall ensure that the customer has no reservations on the deposits into his account made by any other person. Otherwise, the customer shall disclose to the bank the names of persons authorized to make such deposits.

2.8 The bank shall not deal with digital accounts or establish banking relations with unknown persons or customers using fake names or with listed persons or entities.

2.9 No accounts shall be opened through electronic portals. Customers subscribed to the electronic services of the Bank of Jordan may open additional accounts provided that the original account that is already open is complete in terms of information requested at the time of subscription to the electronic services.

2.10 Safe deposit boxes may not be rented for other than Bank of Jordan customers and data on old customers shall be updated when they request to rent a safe box and the purpose shall be stated.

2.11 Frozen accounts shall be transferred to the Banking Operations Department after the lapse of 365 days of their classification as frozen accounts. When the owner of the frozen account checks with the branch, the branch shall send a request to the Banking Operations Department asking for the account to be re-transferred to the branch (changing the administration-frozen code into branch-frozen code)

2.12 The bank shall peruse a copy of the identification document for such cash deposits made by persons who are not authorized to deposit in the respective account.

2.13 The Bank shall verify the real beneficiary through filling in the respective field in the account opening form in addition to a written declaration from the customer in which he specifies the real beneficiary of each and every transaction he intends to carry out through the bank. The bank shall do the due diligence on the real beneficiary as is the case with the original customer.

2.14 In the case of legal persons, the verification of the real beneficiary shall be subject to the implementation of reasonable procedures to capture the ownership structure and the controlling management of the legal person. This shall entail reliance on data or information obtained from official documents sufficient enough to generate for us the conviction that we are ascertained of the identity of the real beneficiary.

2- Risk Based Classification

The goal behind adopting a risk-based approach to classifying customers when they commence dealing with the bank is to organize and enhance the effectiveness and efficiency of the AML-CTF mechanisms through identifying the level of due diligence before and during the establishment of the banking relationship.

Consequently, the Bank has adopted the following criteria for classifying customers:

1- Classification level

High Risk
Medium Risk
low risk

2- Basis of Classification

The customer classification process based on risk is a helping tool in envisaging the future relationship with the customer and the basis that needs to be embraced for following up and monitoring his movements in accordance with the requirements of the supervisory authorities. To that effect, the Bank can rely on assessing to which extent the banking operation carried out by the customer matches the nature of the disclosed activity, and the other accounts the customer has opened at the bank, inter transactional behaviors and average movements. However, it is difficult to identify unified basis that apply to all customers.

Based on that, the following indicators have been identified as a basis for customer classification provided that they are frequently reviewed and amended so that they cope with developments and most recent data available and which could warrant such amendments.

2.1 High Risk Customers (High Risk level)

High Risk customers are those to which the following indicators apply:

* A natural person, which includes

2.1.1 Politically Exposed Persons (PEPs)

* Judges
*Senior military officers/employed in the army, public security department, air force, etc.
* Ex-cabinet members/parliamentarians/ministers/senators/governors, etc.
* Current and former members of political parties.
*Employees of non-profit organizations (associations/UN/Red Cross, etc.)
*Embassy employees in general regardless of their managerial echelons.

2.1.2 Persons operating in the following fields:

* Goldsmiths
* Insurance agents
* Travel agents and tour operators

2.1.3 Non-Residents regardless of the activities the exercised locally or internationally.

2.1.4 Customers of or residing in Non Cooperative Countries As defined by FATF .

* Legal Person which includes:

1. Economic Activity
    * Travel agencies and tour operators
    * Insurance firms
    * Import and export companies
    * Goldsmithery companies
    * Fast food companies (mainly those with international brands)
    * Hotels, cafes, night clubs, liquor companies
    * Associations, organizations and institutions that do not seek profit
    * Currency exchange agencies
    * Investment companies (real estate, etc.)
    * Real Estate agencies

2. Nationality

All non-Jordanian companies and institutions or organizations, regardless of the nature of economic activity they undertake

3. The work of the (Main owner, board member/shareholders with more than 10% holdings/general manager) of companies, institutions or businesses used to be:

- Judges
- Politicians
- Members of Political Parties
- Military servicemen
- Senior government officials (Parliamentarian, ministers, senates, governors, etc.)
- Embassy staff

4.Charities/non-profit organizations

2.2 Medium Risk Customers (Medium Risk Level)

* Every Customer (natural/legal person) who has a commercial activity and to whom none of the indicators mentioned in article (2.1) above apply is classified as medium-risk warranting the bank to follow simplified due diligence procedures regarding the identification of customer, the real beneficiary, and verification in accordance with the permissible limit as stipulated in the customer acceptance article.

*The simplified due diligence procedure shall not be used in case of ML/TF suspicion or the emergence of high-risk situations.

2.3 Low Risk Customers (Low Risk Level)

Each and every natural customer who does not hold a usual trade activity shall be classified as low risk customer provided that none of the indicators mentioned in article (2.1) above apply warranting the bank to follow simplified due diligence procedures regarding the identification of customer and the real beneficiary and verification thereof in accordance with the permissible limits provided in the customer acceptance article.

*The simplified due diligence procedure shall not be used in case of ML/TF suspicion or the emergence of high-risk situations

3- Customer Identification

The process whereby the banks identify analyzes and gets to know the work of the customer takes time. It is however necessity to observe the following:

1- In general terms, enhance due diligence and utmost care must be given to high-risk customers.

2- Establishing a relationship with a high-risk customer shall be subject to the approval of the Bank's general manager, regional manager or the one it authorizes for such a purpose. Such an approval shall be also required when discovering that a customer or a real beneficiary has been listed under any of such categories.

3- Adequate measures shall be applied to be assured of the sources of wealth of customers and real beneficiaries listed under any of such categories.

4- All transactions made by such customers with the bank shall be constantly under the watchful eyes of the bank. Special attention shall be paid to business relations and transactions made by any of them.

5- Necessary measures shall be taken to uncover any conditions harboring any of the business relations and transactions made by any customer of such categories as well as the purpose of such relations and transactions if we are ascertained that none of these have economically justifiable reasons. Relevant notes shall be entered into our records.

6- The bank shall update those accounts related to their holders and authorized signatories on an on-going basis to ensure that all of the bank's records are updated. Such an updating exercise shall be expedited in any of the following cases:

   a. Large amounts of money transactions are made or banking instruments are used in an unusual way.
   b. A substantial change in the process of documenting customer's data has been made.
   c. A significant change has been noticed in the account's management method.
   d. The bank has realized that it does not have sufficient information about any such customer.

7- The bank shall be aware of the sources from which the account is fed, the customer's nature of business, the expected size of account as compared

to other accounts of similar activities in the same region and any other available elements.

8- The bank shall verify all information that it gets about the customers, nature of their businesses, size of activities, work place, authorized signatories and other such information deemed necessary by the bank.

9- A special part in the customer's file shall be allocated for such documents and instruments necessary for the verification of the customer's identity and any other documents related to AML/CTF controlling procedures.

10- If the bank could not manage to fulfill the due diligence procedures on customers, it shall refrain from opening the account, entering into any banking transaction with the customer or carrying out any transaction for the customer's account. It shall also notify the AML/CTF Unit of any ML/TF activity in the forms prepared by the AML/CTF Unit for such a purpose.

11- The bank shall pay due diligence in relation to walk-in customers in the following circumstances:

a. If the value of a transaction or a number of seemingly interrelated transactions are higher than JD10,000 or equivalent in foreign currencies.
b. If the bank has suspicions that the incidental transaction is linked to ML/TF regardless of its value.
c. Any electronic transfer transaction made by a walk-in customer regardless of its value.

12- The procedures for verification of customer's identify may be postponed until after the establishment of continuous relation subject to the following conditions:

a. If the postponement of verification is deemed necessary for maintaining ordinary works and that such postponement does not lead to ML/TF risks.
b. The bank will implement the verification procedures at the earliest possible time.
c. The bank should have taken all procedures necessary for the wise management of ML/TF risks in relation to the case in which verification was postponed. This includes the limitation of numbers, quality and amounts of transactions that are permissible before completion of the verification procedures.
d. If the bank entered into a continuous relation with the customer before completion of the verification procedures in Article 12 above and if the bank failed to fulfill such procedures at a later stage, the bank shall end this relation and notify the AML/CTF Unit in case of any suspicious ML/TF transaction.

4- Continuous Monitoring on Accounts and their Operational Transactions (Particularly High-Risk Ones)

- Pay attention to account movements and transactions incompatible with the nature of the account or the type of activity in light of the suspicious transaction indicators mentioned earlier (conformity of transactions to the customer's professional activity, habits or personality).
- Relate the customer's nationality to sources of internal and external funds and to customer's expertise in its business.
- Relate the type and nature of relationship between the account holder to those of the agent or the person authorized to run the account.
- Pay attention to customers who receive transfers in currencies different from that in which their account is opened and receive the value of such transfers in cash or by transferring such remittances instead of executing them in their accounts. The bank shall document such acts, monitor their size and reach an explanation why the customer acts in this way.

6. "Know Your Employee"(KYE) Policy

- "Know Your Employee" (KYE) is an important principle given the decisive role
- of employees in countering or otherwise facilitating ML/TF in day-to-day banking transactions. Banking is based on particular traditions and cultures that are in turn part and parcel of the broader texture of public tradition and morals. Employees are always required to set the example in morals and trustworthiness their being members of the wider society and shall reflect such traits in their own behaviors. Employees shall distance themselves from suspicious situations, financial confusion and work abuse, and shall do all they can to render an excellent banking service.
- Employees shall be well selected and their resumes shall undergo close scrutiny particularly when such employees are in direct contact with customers. Smart, agile and vigilant should be among their traits as they are in the first lines of detecting suspicious transactions. They should be kept under watchful eyes especially if they are new to banking. Therefore, policies and procedures, job descriptions, internal controls, defined powers, compliance with laws, codes of conduct and dual monitoring among other deterring systems shall be the benchmark for all employees in the exercise of their work.
- Getting to know employees is a continuous process that does not last by their selection. Employees of different positions shall be constantly monitored in terms of their abidance by AML/CTF instructions with eyes open on any suspicious movements on their personal accounts if such transactions are not commensurate with their incomes.
- Implication of an employee in ML/TF can take several forms and can be sensed by some indicators. He may help in receiving deposits and transferring them to third parties or showing leniency throughout the verification of customer's good faith and integrity of data when opening up their accounts. Here are some examples of those indicators:
- Increase in an employee's standards of living and dressing style in a noticeable manner that is not commensurate with his monthly income.
- Refrain from taking leaves
- Frequently Bypass controlling procedures and resort to deception throughout the course of his work.
- Assist in the implementation of some transactions marked mainly by the anonymity of beneficiary.
- Exaggerate in the credibility, ethics, solvency and financial resources of the customer in his reports sent to the bank administration.

7. Patterns and Indicators of Suspicious ML/TF Transactions and Dealings

While it can be very difficult to expose transactions suspected of being related to ML/TF, there are some useful patterns and indicators that can be used. Here are some examples -but without limitation- of such patterns and indicators on the transactional level:

1. Cash Transactions:

1. Suspicious large amounts of cash are deposited by a natural or legal person whose outward commercial activity is usually pursued through checks and other payment instruments.
2. There is a big increase in cash deposits for any person without a clear justification. This applies particularly when such deposits are transferred within a short period of time from the account to another party that does not seem to have a clear connection with that person.
3. Cash amounts are deposited on several stages in a manner whereby the value of each deposit is less than the threshhold set in the regulations thought they are far above the threshhold in totality.
4. Cash amounts are deposited on several stages totaling overall a large amount.
5. Concentration is made almost solely on withdrawal and deposits rather than by using bank transfers and other negotiable instruments without a clear justification.
6. Large numbers of banknotes of small denominations are replaced by those with large denominations without showing clear reasons.
7. Large and unusual amounts of money are deposited through automatic teller machines to avoid contact with the bank employee particularly if such deposits are not commensurate with the usual business and/or the income of the respective customer.
8. The customer carried out several large monetary transactions with several branches of the bank or had such transactions done with the help of other persons on behalf of that customer and on the same day.
9. Large amounts of money are deposited including banknote stacks stamped by other banks.
10. The customer retrieved a part of the amount that is required to be deposited once he learned that special due diligence procedures will apply with unusual transactions as stipulated by the regulations.
11. Cash deposits are made with counterfeit, worn out or old bank notes at high rates.
12. The customer made a quick and abrupt withdrawal of his balances without a justifiable reason.

2. Customers' Accounts:

1. The customer maintains several accounts and makes deposits in each of them to the effect that they form in total a large amount that is not commensurate with his business, with the exception of customers whose business require them to maintain several accounts.
2. There are several accounts and through those accounts some transactions were made but they were not commensurate with the business of the customer because he uses the account to receive and/or distribute huge amounts of money for an unclear object or for a purpose not relevant to the account holder and business.
3. The customer maintains several accounts with several banks located in the same geographical areas and is then transferring the balances of those accounts into one account before transferring the accumulated amount to abroad.
4. Checks of third parties are deposited with high amounts and are endorsed for the account holder though are not compatible with the account holder's business.
5. Large amount withdrawals are made through a formerly inactive account or the withdrawals made by him are either relatively small or are made from an account with which unexpected huge amounts of money were deposited.
6. A number of persons deposited amounts in one account without a justifiable reason.
7. The customer submitted financial statements about his commercial activity that are clearly different from those of similar companies in the same sector.
8. Companies that relatively have huge activity submitted financial statements that are not audited or endorsed by a chartered accountant.
9. A company that receives checks from its customers does not make large withdrawals from its accounts in return for the depositing of such checks, which indicates the possibility of such a company's having other sources of income.
10. A substantive change has happened in the management of the customer's account that is not compatible with his personal details.
11. A company or a corporation's account shows little or non-systematic activity.

1. **Transfers**:

1. Deposits in an account are transferred to abroad directly either in lump sum or in installments.
2. Similar amounts are transferred (daily/weekly) that accumulate large amounts in total.
3. Transfer orders for a person who does not maintain an account with the bank by using several payment instruments each of which is less in value than the threshhold prescribed in the regulations.
4. Inward transfers accompanied by instructions to transfer their values into checks and send them by post to a person who does not maintain an account with the bank.

5. Transfers are made with large amounts to countries known to harbor banking and tax confidentiality.
6. The beneficiary used the value of inward transfers to buy a variety of financial instruments upon receiving the money with intent to pay to a third party.
7. A given account receives transfer of big amounts of values not deposited before in that account in a manner not commensurate with the business of the customer.
8. The customer frequently makes outward transfers of money he claims are of an international origin.
9. The customer deposits instruments in the order of bearer in own accounts then transfers them to a third or fourth party.
10. An open account of a currency exchange company receives monetary deposits or transfers whose amounts are less than the threshholdprescribed in the regulations.
11. Ordering an unusual transfer within a pack of usual transfers that are usually ordered as one transfer.
12. Transfer of big amounts of money to abroad or receiving inward transfers from abroad accompanied by orders of payment in cash.

2. <u>Safe Deposit Boxes:</u>

1. The customer maintains a number of safe deposit boxes without a clear justifiable reason.
2. Safe deposit boxes are used very frequently to the extent that may imply that the customer has large amounts of cash in such safe deposit boxes.
3. The customer very frequently visits the safe deposit boxes before and after depositing cash amounts that are less in value that the threshholdprescribed in the regulations.

3. **<u>Investment related transactions</u>**:

1. Financial securities are purchased to maintain them in safe deposit boxes with the bank and that such amounts are not commensurate with the customer's business and financial status.
2. The customer is heedless of the ordinary decisions applicable on investment accounts such as fees and investment tools.
3. The customer cleared a big financial position through a series of small monetary transactions.
4. The customer deposited monetary payments, payment orders, travellers' checks or over-the-counter checks with amounts less than the threshhold prescribed in the regulations for the financing of an investment account.
5. The customer used investment accounts as a tool to transfer money to foreign parties particularly offshore regions.
6. Entering from abroad huge financial amounts for investment in foreign currency or financial securities with the investment volume not commensurate with the financial position of the customer.

7. An attempt to show the financial transactions in a manner that is more complex than needed by using such impressive terms as: prime bank notes stand, hedging, by commitment, contracts, arbitrage.

4. Credit facilities

1. The customer submitted an application for credit facilities for foreign companies or for companies working in offshore regions or other facilities secured by external or offshore banks' commitments.
2. The customer repaid huge debts abruptly without a clear or reasonable clarification of the repayment source.
3. The customer purchased deposit certificates and used them at a later stage as a guarantee to repay the facilities.
4. Credit facilities are obtained as guaranteed by monetary deposits.
5. Credit facilities are obtained in return for a monetary guarantee abroad.
6. The customer transferred to abroad the value of those facilities that were abruptly obtained .
7. The customer repaid a debt classified as a non-operating debt before the expected repayment time and with amounts bigger than expected.
8. Facilities are obtained in return for setting on mortgage assets owned by a third party insofar as the source of such assets is not known to the bank or the volume of such assets are not commensurate with the customer's financial position.
9. The customer requests facilities or the arrangement of funding for him with third parties insofar as the source of the customer's or customers' financial contribution to that funding is unknown.
10. Credit facilities are obtained in return for seizing deposits belonging to a company or affiliated companies abroad particularly if such companies were located in countries known to be producers and/or promoters of drugs.
11. Some conditions surrounding the request for credit facilities lead to the bank's declining of granting such facilities because of doubts about the validity of those facilities' guarantees.
12. The customer submitted financial statements that do not agree with accounting standards.

5. Financing commercial transactions and documentary credits.

1. The customer requested a commercial funding whether for importing or exporting basic goods whose declared prices are substantially and clearly different from their prices in similar markets.
2. Documentary credits or letters of guarantee are issued upon the request of the customers in respect of bids despite the non-existence of contracts for current projects or for the benefit of an unusual beneficiary.
3. The customer changed the name of the first beneficiary from the documentary credit just a short time before the payment transaction.
4. The customer changed the place of payment in the documentary credit into an account in a country other than the country of the beneficiary.

5. The person benefiting from documentary credits is a number of companies owned by the customer or that the shipping companies are owned by the same customer.
6. The amounts mentioned in the documentary credit documents presented by the customer to the bank or the Customs Department are not compatible with the original documents.

6. **Financial and international banking transactions**:

1. A declaration is submitted to ascertain the identity of a person by external parties located in countries known to be producers and/or promoting drugs.
2. Huge balances are built up in a manner not commensurate with the volume of the natural business of the customer and frequent transfers to an account or to accounts open abroad.
3. A request is repeatedly made to issue traveller's checks in foreign currency or other negotiable instruments with a value exceeding the threshhold prescribed in the regulations.
4. The customer resorted to consecutive deposits of traveller's checks in foreign currencies with amounts higher in value than that of the threshhold prescribed in the regulations.
5. Banking transactions are made in connection with external offshore banking units bearing names similar to those of other legitimate banking corporations that have a good reputation.

7. **Electronic banking transactions**:

1. The account receives several small financial transfers electronically after making big transfers in the same way to another country.
2. Large amounts are systematically deposited in a variety of ways including electronic depositing or receiving large amounts systematically from countries known to produce and/or market drugs.
3. The customer requested to open an account through the internet and declined to provide necessary information for completion of the opening of such an account or refused to provide information that usually enables him to have access to services and facilities considered by an ordinary customer as an extra advantage.
4. The customer used the banking service online by transferring between his accounts several times without clear reasons for that.

8. Rules that shall be observed in relation to cash deposits and transfers

1. Cash Deposits

1. When a customer appears and desires to deposit an amount that is higher in value than JD20,000 or equivalent in foreign currency, the cashier shall fill in the item related to the source of money in the deposit voucher before printing it out.
2. The customer shall be asked to produce supportive documents to prove the source of any cash deposit exceeding in value the sum of JD20,000 or equivalent and maintain a copy thereof.
3. Should the customer have no documents proving the source of the money, the cash payment shall be accepted but the customer shall be told that he shall provide the bank with the required documents. Follow up is necessary until the documents are obtained.
4. If the customer refused to disclose the source of the deposited money or refused to provide the bank with the required documents, the cash deposit shall be accepted but in this case the AML/CTF unit/Compliance Department by filling the necessary "Suspicious Case Report" form.
5. If the customer retracted from a cash deposit transaction after he is requested to disclose the source of money, the branch's officer shall fill in the Suspicious Case Report form and send it to the AML/CTF unit. If a deposit is made by persons unauthorized to deposit in the given account, a copy of their identify cards shall be obtained.

2. Transfers

1. Outward transfers:

a. Onward transfer services may not be rendered to other than the bank's customers with the exception of checks that are issued to the order of governmental corporations or authorities.
b. Due diligence shall be paid in respect of customers requesting for an outward transfer. All necessary information shall be completed by the customers before the onward transfer is made. Such information includes the name of issuer, account number, the national number for Jordanians or the number of identify document for non-Jordanians.
c. Punch of transfers may not be issued. Only individual transfers for bank's customers may be issued.
d. All onward transfers shall be automatically verified and checked regardless of the amount against the list of restricted parties (UN, OFAC, etc.)
e. Onward transfers issued upon the request of customers who maintain accounts with the bank shall be made through the customer's account. In the case of cash payment, the transfer shall also be made through the customer's account.

2. Inward Transfers:

a. Inward transfers may not be accepted unless are sent to bank's customers.
b. All onward transfers shall be automatically verified and checked regardless of the amount against the list of restricted parties (UN, OFAC, etc.)
c. Manually verify all details of inward transfers and check that all information required about the issuer are complete including name of issuer, account number, national number or number of identify document for non-Jordanians.
d. The transfer shall be sent to the respective branch once the information about the issuer are completed. Any missing information should be sought from the bank that sent the transfer. If the bank fails to send the required information, the transfer shall be rejected.
e. All inward transfers for the bank's customers who maintain accounts in the same currency of the transfer shall be deposited in their accounts and may not be paid out to them in cash.
f. If the inward transfer is issued in a currency different from that of the account and the customer requested to receive the transfer in the account's currency, the transfer shall be first deposited before it can be withdrawn by the customer.

3. Intermediary Bank's Obligations:

If the bank participated in carrying out the transfer without being the source or receiver thereof, the following points shall be considered:

a. The bank shall verify that all information in the transfer about the transfer issuer is complete including name of issuer, account number and national number or number of identify document. If any information is missing, the recipient bank shall be informed when making the transfer.
b. All information accompanying the transfer are kept with it during the transfer.
c. If the bank could not retain the information accompanying the transfer for technical reasons, the same information shall be retained as received for a period of five years regardless of whether or not such information were complete or otherwise missing for the purpose of meeting the request of the recipient bank in case an inquiry is set about this transfer.
d. Inward and outward electronic transfers higher in value than JD700 or equivalent in foreign currencies are subject to the same regulations of transfers.
e. If the account currency is different from that of the transfer and the customer wishes to pay or receive the transfer in cash in the same currency of the account, the customer, in case of such recurrent requests, shall be asked to open another account with which such inward/outward transactions are dealt with.

9. Requirements for Dealing with External Banks

- Fulfill the requirements for the identification of customer (external bank) and get documents necessary for proving the legal entity of the Bank, which has requested to open an account, the ownership of the bank (public or private) and the names of shareholders whose shares account for more than 5% of the bank's capital.
- Get details about the type of activities carried out by the external bank and its reputation in AML/CTF, its locations and the purpose for opening an account.
- Get information about the bank's management (names of senior managers, their qualifications, experience, etc.)
-Get the approval of the director general for the creation of a business relation with the external bank.
- Get information about the controlling and monitoring procedures applied on the bank in the country wherein it works. No account may be opened for any bank registered in a given country but does not have any physical presence or is not subject to the control of state authorities there (Shell Banks).
- Check if there are in place any procedures or policies for the bank that requested the opening of the account in AML.
- Verify that the external bank has implemented the required due diligence measures in respect of its clients (KYC) who do not have the authority to use accounts (Payable-through accounts) and that the external bank is capable of providing information on those customers and on the transactions performed thereon when necessary.
- Confirm in writing to the Compliance Department that those requirements are fulfilled when opening accounts for external banks.

***If an account is opened for a external bank with Jordan Bank and that the said external bank allowed so e customers to act through this account by any payment method, then in this case the Jordan Bank shall make sure that the external bank did implement the KYC due diligence measures in respect of such customers.**

10. How to Identify Suspicious Transactions:

- A good knowledge of the suspicious transaction patterns and the nature of business of the customers gives the employee a clue on whether or not there is something fishy in the customer's transactions. The clue is further fostered through scrutinizing significant banking transaction statements and comparing them with the customer's transactions.
- If the employee in charge has any doubts that are not based on solid grounds, then he can discuss the matter with the manager or the assistant. It is not unlikely that a customer may at sometimes perform unusual yet legitimate transactions.
- Getting to know the customer very well and accessibility to information and details about his work, volume of activity, income sources and his transaction history in addition to any other available information is the only thing that can be used to either further the doubts or clear them out.

The following is a checklist that shall be answered by the employee in charge:

1. Is the transaction compatible with the customer's professional or personal activity?
2. Is the volume of transaction the same as accustomed to from that customer?
3. Are there any new changes emerging to the nature, quality and quantity other customer's transactions?
4. Is the external transaction justifiable by the existence of relations associated with the customer's work or person? Is the country in question non-cooperative or one where money laundering and drug crimes are widespread?

If in light of the answers to those questions the employee became suspicious of ML/TF activity, he shall follow the procedure below:

1. Fill in the Suspicious Case Form indicating that the subject case is suspicious of being related to proceeds from money laundering or is used for financing terrorism.
2. Prepare sufficient data and information about the customer and the suspected transaction by referring to the customer's file and other inquiry methods available with the branch and attach such information to the form.
3. Refer the case with attachments to the Liaison Officer for studying and endorsing it.
4. Liaison Officers shall review the suspicious case and the companying documents and send it then to the AML/CTF Unit, which will take the relevant decision.
5. The AML/CTF officer shall receive the case with its attachments. Then, he shall study and analyze it before requesting any additional information if necessary. Then, he refers the case to the money laundry reporting Officer.

6. The money laundry reporting officer reviews the case and studies it thoroughly.
7. If the money laundry reporting officer is convinced of the suspicion, he shall send a Suspicious Activity Report (SAR) supported by documents and instruments to the competent authority (i.e. AML/CTF Unit) through the system made for that purpose.
8. If the money laundry reporting officer deems the suspicion grounds insufficient, the documents shall be retained and the case in question shall be monitored for six months. In light of the findings within that period, the manager shall have the option of submitting the SAR based on strong suspicion grounds or alternatively he may remove the client from the watch list.
9. All documents and instruments related to the SAR reported cases shall be retained for a period of five years as of the date of notification or until the issue of a court order on such cases whichever is longer.

11. Duties and Responsibility of Liaison Officers

Work should be organized and responsibility should be defined in AML/CTF. To this end, a Liaison Officer has been defined in every bank unit (branches, business development offices, relation management officers in corporate development departments, follow-up department, collection department and human resource department).

Liaison Officers are not responsible for inspecting and verifying the legality of transactions. Their sole responsibility is to exert reasonable efforts and report on suspicious transactions as per the facts made available to them and the information they have about the customer's activity.

Therefore, a Liaison Officer is appointed and is entrusted with the following tasks:

1. Access the AML/CTF electronic system on a daily basis and examine the alerts given on customers in terms of purpose and source of money and the compatibility of the movement with the nature and type of the customer's activity by reviewing the customer's history of transactions.
2. Enter the findings of inspection on the electronic system's alerts in accordance with Article (1) and send them automatically to the Compliance and Risk Department at the AML/CTF Unit.
3. Provide the AML/CTF Unit/Compliance and Risk Department with reports, documents and other necessary instruments on the customer sin question.
4. Prepare a detailed report on suspicious customers and accounts along with justifications for suspicious accompanied by all supportive documents and instruments.
5. Receive suspicious cases from employees in relation to customers' behaviors and justifications for suspicions and prepare a suspicious

case and send it to the Compliance and Risk Department at the AML/CTF Unit.

12. Duties and Responsibilities of AML/CTF Unit

1. Sort out alerts coming from branches and respective departments through the electronic system to combat money laundering.
2. Study incoming alerts and accompanying Liaison Officer's notes.
3. Assess the adequacy of information and other notes submitted by the Liaison Officers at branches and decide on measure their justifications given in view of the movement that triggered the alert then take necessary measures.
4. Request Liaison Officers to provide it with detailed reports on customer's activity along with documents supporting the type of activity.
5. Prepare detailed reports on suspicious movements and report then to the money laundry reporting officer to study them and take the necessary decision.
6. Verify suspicious movements and report them to competent authorities if necessary.
7. Check suspicious transactions and report them to competent authorities if necessary.
8. Answer any inquires coming from the AML/CTF Unit or the Central Bank of Jordan and provide them with necessary information and details.
9. Receive inquiries from branches on the opening of accounts for customers classified as high-risk customers (non-residents, PEPs), inward transfers from high-risk countries and the payment of checks with values exceeding JD100,000 or equivalent in foreign currencies, note such information on the query form, answer them and present them before the Money laundry Reporting Officer for endorsement.
10. Prepare reports on the findings of the analysis and study of all required data and documents as mentioned in KYC in respect of PEPs and non-residents and present such reports before the department's manager for approval and endorsement.
11. Hold training and awareness raising sessions for employees on ML/TF and AML/CTF as per the training schedule adopted by the training department.
12. Follow up with the electronic system and update lists regularly.
13. Follow up with the correspondent banks' unit to answer their inquiries about customers.
14. Answer questionnaires received from external banks to measure the bank's compliance with AML/CTF laws and regulations.
15. Keep abreast of latest developments in terms of ML/TF trends and methods of combating such crimes particularly those published by

FATF, IMF. WB, Basel Committee and other international organizations.

16. Prepare questionnaires to verify the compliance of correspondent banks with laws and regulations governing AML/CTF activities.
17. Create files especially for suspicious ML/TF transactions or names of persons and keep in those files all notifications on such transactions and relevant data.

13. Duties and Responsibilities of the Money laundering Reporting Officer

1. Receive information and reports on unusual or suspicious transactions or those that are suspected to be ML/TF related, examine such cases and take the appropriate decision to send a SAR to the competent authority, i.e. AML/CTF Unit or to close the case provided a justification is given in the latter case.
2. Retain all documents and reports that he receives for a period not less than five years.
3. Provide AML/CTF Unit and other competent authorities with data related to ML/TF suspicious transactions or any other information upon request. He shall also facilitate such authorities' perusal of all relevant records and information to allow them to carry out their duties.
4. Prepare periodical reports to be submitted to the board of directors on unusual or ML/TF suspicious transactions.
5. Provide the AML/CTF unit with information on obstacles and developments that may hinder the application of procedures with external branches and inform the AML/CTF Unit whether the requirements in the other country are more or less strict than those in Jordan.
6. Ensure that employees are fully aware of the work procedures and AML/CTF policies.
7. Ensure those means that guarantee the updating of the list of uncooperative states and the black list that includes the names of suspected persons in light of the list issued by the Central Bank of Jordan.
8. Allow for a sort of cooperation between local and external banks for the sake of exchanging information on the activities of a given customer or on specific transactions whether by requesting or providing information.
9. Keep abreast of latest developments on ML/TF operations and how to combat and control such crimes.
10. Discuss training plans for employees on AML/CTF.

14. Duties and Responsibilities of the Inspection and Internal Audit Department

1. Ensure that all employees and officers in charge are aware of ML/TF and the trends of suspicious transactions each according to own capacity.
2. Ensure that the branches and employees are carrying out the duties entrusted to them in relation to AML/CTF.
3. Ensure that the Liaison Officer is handling the AML/CTF electronic system.
4. The accounts controller in the branch to ensure that there is no delay in reporting to the Money laundry reporting Officer on suspicious transactions.
5. Conduct necessary controlling inspections to ensure that the movements of customers' accounts are commensurate with the nature with their activities and that if any suspicion is raised then the relevant translation is reported to the Compliance and Risk Department at AML/CTF Unit, which will in turn put the account under control.
6. Train employees at the inspection and internal audit department so that they handle their duties and responsibilities in implementing the procedures, policies and internal controls adopted in AML/CTF.

15. Employee Training and Education

A rudimental component in the AML/CTF process., training sensitizes them on the nature, type and ways of ML/TF and updates them on any development in the field on the local and world levels. Training also helps employees avert themselves from being trapped in as victims of ML/TF not to mention that their awareness and positive cooperation help in detecting ML/TF practices and stimulate them to undertake their respective duties in protecting the reputation of the bank and prevent it from being exploited by money launders. Along those lines, here is a list of what should be done:

- Prepare and implement a continuous training program for the training of all employees of different managerial echelons on money ML and TF and ways to combat those crimes.
- Hold specialized training workshops that match the levels of employees in accordance with the nature of their respective works.
- Keep abreast of training courses and local and international publications on the subject to keep updated of any development and adjust the training courses accordingly.
- Retain records for all training programs that have been held over a period of no less than five years. Such records shall maintain the names of trainers and their qualifications in addition to the party that held the training whether held inside or outside the country.

16. File and Records Keeping

1. All records and documents supporting the ongoing relations and banking transactions shall be retained for a minimum period of five years as of the date of execution of the transaction or termination of the relationship.
2. The customer's file shall spare a part allocated for retaining all documents and instruments required for the identification of the customer and any other documents that relate to AML/CTF operations.
3. A special file shall be created to file all ML/TF suspected transactions. This file shall keep copies of notifications of such transactions and other relevant data and instruments. Such files shall be retained for a period not less than five years as of the date of notification or until the issuance of a court decision on such transaction whichever is longer.

17. General Rules:

1. Employees of all levels shall study, understand and implemented these procedures. They shall also seek any clarification necessary to allow them to carry out their duties.
2. Every administrative officer in the bank shall comply with the policies and procedures adopted by the bank in addition to applicable AML/CTF laws, bylaws and regulation each in his own capacity.
3. No administrative officer may run any accounts by proxy on behalf of any client except the spouse or first degree relatives subject to a prior approval from the higher management.
4. Under no circumstances may the management of accounts, making transactional moves or conducting commercial business be accepted with any current or potential customer who is suspected to be implicated or from whose behavior it can be deduced he wants to be engaged in ML/TF activities whether or not such transactions have been performed.
5. All administrative officers are strictly prohibited from disclosing directly or indirectly and in any means that a notification is sent to the AML/CTF Unit on any procedures known to the competent authority that is bound to fulfill the notification obligation in accordance with the provisions of AML/CTF law No. 46 for the year 2007.
6. No customer me be interrogated with upon suspicion of a ML/TF transaction. The bank's sole obligation in this respect is to collect data and information relevant to the transaction then reports them to the competent authority.
7. The bank and its employees shall be released from all criminal, civil, administrative and disciplinary liability if any of them makes a notification in good faith about a ML/TF suspected transaction or provides relevant information or data thereof in accordance with the AML/CTF law No. 46 for the year 2007.
8. Officers at the bank should not hesitate at all to contact the compliance department at AML/CTF Unit to inquire about any suspicious cases.
9. On the strength of AML/CTF Instructions No. 51/2010, closing the accounts of suspected persons is strictly prohibited.

18. Definitions:

Money Laundering (ML)	Every conduct involving acquisition, possession, disposing of, moving, managing, keeping, exchanging, depositing, investing of funds or manipulating its value or movement and transferring, or any action that leads to conceal or disguise its source, origin, nature, place, disposition mean, ownership or related rights, with knowledge that the funds are proceeded of one of the crimes stipulated in article (4) of the law or any other article that may replace it.
Terrorism Financing (TF)	Providing, collecting or securing funds by any means, directly or indirectly with the intention of using them to carry out an act of terrorism as defined in effective legislation or in the knowledge that they are to be used, in full or in part, in order to carry out an act of terrorism regardless of whether or not such an act has materialized.
Suspicious Transaction	Any transaction thought for any justified reason to be related to proceeds of any crime of those stipulated in article (4) of the law or any other article that may replace it.
Banking Relationship	The relation that is created between the bank and the current in respect of those activities and services given by the bank to its customers.
On-Going Relationship	The banking relationship that when created is excepted to last for an unlimited period of time and to involve several transactions.
Walk-in Customer	The customer who is not related to the bank in an ongoing relationship.
Non-Profit Organization (NPO)	Any legal person established in accordance with the relevant laws with the main object of rendering social or volunteering services without seeking through its activities profit, profit sharing or a personal utility.
Controlling	The direct or indirect ability to exercise an effective influence on the works and decisions of another person.
Real Beneficiary	The natural person who has the real stake and for whose interest or on behalf of whom the business relationship is established, or the person that has full or effective control over a legal person or the right to carry out a legal action on behalf thereof.
Politically Exposed Persons (PEPs)	individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, prominent politicians, important party officials or senior executives of state owned corporations including the relatives of such persons up to the first degree as minimum or their partners.

Shell Bank	The bank that: 1- Does not have a physical presence wherein it may receive its customers 2- Does not employ any person to hold actual activity or management positions. 3- Does not maintain records for its transactions 4- Is not subject to inspection by a competent controlling authority whether in the country whether it was established or in any other country. The Shell Bank's definition does not apply to a bank that does not have fixed headquarters so long as it is affiliated with a bank that is licensed, that has a physical presence and that is subject to an active controlling.
Non-Resident	A natural or legal person that resides or whose headquarters are seated outside the Kingdom or that who has not competed one year of residence in the Kingdom regardless of the nationality of such a person with the exception of individuals who have a permanent economic activity and a permanent housing in the kingdom even if such individuals resided in the country in an intermittent manner.
The Unit	The Anti-Money Laundering and Counter-Terrorism Financing Unit established in accordance with the law.
Money laundering Reporting Officer	The officer who assumes a position in the higher echelon of management in the bank and who is appointed to make notifications of any suspicious transactions or those that relate to the financing of terrorism or listed persons and entities.
Administrative Officer	A member of the bank's board of directors acting whether in own personal capacity or as a representative of a legal person, the director general of the bank or any employee therein.
Electronic Transfer	Any transfer transaction made via a bank using electronic means on behalf of the transfer issuer whereby money us sent to another bank where the receiver can receive it regardless of whether or not the issuer of the transfer is the same person as that as the receiver.
Unified List	The list prepared and adopted by the Sanctions Committee with respect to Al-Qa'ede Organization, Osama Ben Ladin, Talban Movement and all persons and entities linked with them
Named Person	The natural person named by the Sanctions Committee including the person linked with Al-Qa'eda Organization, Osama Ben Ladin and Talban Movement.
Named Entity	The legal person named by the Sanctions Committee including the corporate person owned, controlled or linked directly or indirectly by Al-Qa'eda Organization, Osama Ben Ladin and Talban Movement.