

This document has been translated for knowledge, but for legal purposes the Arabic version is adopted.

Central bank of Jordan

Ref: 10/4/8554

Date:12 /10 /1439 Hijri

Corresponding to 26 / 6 / 2018

Anti Money Laundering and Counter Terrorist Financing Instructions No. (14/2018)

Issued pursuant to the provisions of article (99/b) of the Banking Law No. (28) of 2000 and its amendments, and to the provisions of article (14/a/4) and Article (18/b) of the Anti Money Laundering and Counter Terrorist Financing Law No. (46) of 2007 in force

Article 1: Definitions

First: The terms and expressions mentioned in these instructions shall have the meanings assigned thereto in the Anti Money Laundering and Counter Terrorist Financing Law and the Banking Law in force, unless the context indicates otherwise.

Second: The following terms and expressions, wherever mentioned in these instructions, shall have the meanings assigned thereto hereunder, unless the context indicates otherwise:

The Law : Anti Money Laundering and Counter Terrorist Financing Law in force.

Banking Relationship : The relation commenced between the bank and the customer, which is related to the activities, products, and services provided by the bank to its customers.

Occasional Customer : The customer who doesn't have a bank account with the bank and who is not involved in an ongoing relation with the bank.

Beneficiary of the transfer : The natural or legal person or the legal arrangement specified by the originator of the transfer as the recipient of the requested financial transfer.

Non-Profit Organization : Any legal person or legal arrangement established pursuant to the provisions of relevant laws who engages in raising or disbursing funds for charitable, religious, cultural, educational, social, or other similar purposes without the aim to profit making or sharing thereof or to accomplish personal benefit, including foreign branches of international Nonprofit organizations and agencies.

Control : The direct or indirect capacity to influence effectively the actions or decisions of another person.

Beneficial owner : The natural person with the real interest for whom or on whose behalf the business relationship is conducted or who has full or effective control over a legal person or a legal arrangement or has the right to conduct a legal act on behalf of either of them.

Foreign Politically Exposed Persons : Persons who hold or have held a senior public office in a foreign country such as heads of state or government, judicial or military officials, a senior government official, a prominent politician, a prominent figure in a political party, or senior executives at enterprises owned by a foreign state, including relatives of such persons of the first degree as a minimum, their business partners or any persons acting on their behalf or having an authorization issued by them.

Local Politically Exposed Persons : Persons who hold or have held a senior public office in the Kingdom, such as

heads of government or ministers, judicial or military officials, a senior government official, a prominent politician, prominent figure in a political party, or senior executives of state-owned enterprises, including relatives of such persons of the first degree as a minimum, their business partners or any persons acting on their behalf or having an authorization issued by them.

Persons (foreigners or locals) who held a prominent position in an international organization

members of senior management, i.e. directors, deputy directors, members of the board or equivalent positions in an international organization, including relatives of such persons of the first degree as a minimum, their business partners or any persons acting on their behalf or having an authorization issued by them.

This definition does not apply to the individuals holding intermediate or lower positions in the above- mentioned categories.

Shell Bank : The bank that :

- 1- Does not have physical presence/ permanent place of business in the country in which it was established and licensed, and the physical presence means the existence of a real mind and management in a country, while the mere presence of a local agent or few number of employees does not constitute a physical presence.
- 2- Does not keep records of its transactions.
- 3- Is not subject to inspection by a competent supervisory entity, whether in the country of

incorporation or any other country.

This definition shall not apply to a bank with no permanent place of business if it is a subsidiary to another licensed bank with physical existence and subject to effective supervision.

Shell company A company that is used as a means through which transactions are passed without holding any assets or conducting transactions related to its activity, even if it is registered.

Non-Resident : Natural or legal person who usually resides or his residence is outside the Kingdom or who has not completed a full year stay in the Kingdom, regardless of his/ her nationality, except for families and individuals who have status or economic interest and have permanent commercial activity and residence in the Kingdom, even if they reside intermittently

The Unit : The Anti Money Laundering and Counter Terrorist Financing Unit established pursuant to the provisions of the Law.

Money Laundering Reporting Officer : A member of senior management of the bank (who could be the compliance officer), appointed basically for the purpose of reporting transactions suspected to be related to money laundering or terrorist financing.

Senior Executive Management : Includes the general manager (Chief Executive Officer, "CEO") or regional

manager, deputy general manager or deputy regional manager, assistant general manager or assistant regional manager, Chief Financial Officer “CFO”, Chief Operations Officer “COO”, Chief Risk Officer “CRO”, Internal audit manager, Chief Treasury Officer (and investment), Chief Compliance Officer “CCO” and any other employee in the bank who has executive power parallel to the powers of the aforementioned and is directly reporting to the general manager.

- :
Wire Transfer : Any transfer made through a bank using electronic means of transferring funds on behalf of the sender, by which funds are sent to another bank or any other financial company where the beneficiary can receive, regardless of whether or not the sender and the beneficiary of the transfer are the same person.
- Batch transfer** : Is a transfer composed of a number of individual wire transfers that are being sent to the same financial institution, but may/may not be ultimately intended for different persons.
- Financial group** : Means a group that consists of a parent company or of any other type of legal person who owns control shares and who coordinates functions with other members of the group to implement or execute supervision over the group in accordance with the basic principles of effective supervision issued by Basel Committee for Banking Supervision along with the branches and / or subsidiaries

that are subject to Anti-money laundering and terrorist financing policies and procedures at the group level.

Financial institution : A legal person who, by virtue of the Articles of Establishment, conducts one or more of the financial activities stipulated in the Banking Law, including insurance companies, for the purposes of these instructions.

Subsidiary Company : A company in which one or more persons with a joint interest own at least 50 percent of its capital or hold an effective interest that allows the said person or persons to control its management or general policies.

Straight through processing (STP) : Payment transactions that are conducted electronically without the need for manual intervention

Legal arrangements : It is the relationship that arises under a contract between two or more parties and that does not result into establishment of a legal person such as direct trust funds or similar legal arrangements.

Express trust : The legal relationship created, between living persons or upon death, by a person or a trustee in which the assets are placed under the control of the person or the trustee for the benefit of a

beneficiary or for a particular purpose so that the assets are independent funds and not part of the trustee's property, and the right to the trustee's assets remains in the name of the testator or in the name of another person on behalf of the testator.

Article 2: Scope of Application

The provisions of these instructions shall apply to the following:

First: Banks operating in the Kingdom.

Second: Branches of Jordanian banks and their subsidiaries operating abroad to the extent permitted by laws and regulations in force in these countries, taking into consideration the implementation of the most stringent standards in the event the AML / CFT requirements in the host country are different from those in home country. The bank shall notify the Central Bank of Jordan of any restrictions or constraints that may prevent or limit the implementation of these instructions.

Third: Companies that are subsidiaries to Jordanian banks operating in the Kingdom unless such companies are subject to another supervisory entity in the Kingdom- and such entity issued instructions specific to Anti Money Laundering and Counter Terrorist Financing.

Article (3): Risk Based Approach

First: Risk Management:

1. Within the framework of the risk-based approach, the scope and intensity of the risk management function shall be commensurate with the nature, size and complexity of the bank's transactions and activities and the level of risk of money laundering and terrorist financing.

2. The bank's money laundering and terrorist financing risk management function shall be consistent and integrated with the overall risk management framework

Second: Risk Assessment:

1. The bank shall conduct a comprehensive assessment for the risks of money laundering and terrorist financing, at least on an annual basis, or if the need arises for such assessment as a result of a material change in the nature of the risks to which the bank is exposed and through which the risks of money laundering and terrorist financing are identified, assessed and understood in relation to customers, countries, geographical areas, products, services, operations and service delivery channels in accordance with a methodology approved by its board of directors or the regional management of the foreign bank. The assessment shall include the branches of the Jordanian bank and its subsidiaries abroad. Assessment processes shall be documented.

2. The assessment shall include at least the following: -

2.1 Results of monitoring the bank's activities such as the level of bank's exposure to money laundering and terrorist financing risks, details of the risks in terms of key activities and customers categories, trends of suspicious transaction reports (STRs) and cash transactions limit reports, and trends of the requests received by the bank from law enforcement authorities

2.2 Details of the material risk events that occurred internally or externally and their impact on the bank.

2.3 Any changes that occurred recently to the instructions or circulars regulating the AML / CFT and their impact on the bank.

3. The bank shall provide the Central Bank before the end of April of each year with the following:

3.1 The approved assessment methodology and any amendments thereto.

3.2 The assessment results submitted to senior management and board of directors

3.3 A report by the internal auditor of the bank or the competent committee of its board of directors clarifying the recommendations and actions to be taken to reduce the high risks that have emerged as a result of assessment.

Third: Risk Control and Mitigations:

The bank shall have the following:

1. Policies, controls and procedures to manage and reduce the identified money laundering and terrorist financing risks, approved by the bank's senior management, each according to its competence.
2. Monitoring the implementation of these policies, controls and procedures, and enhancing them when necessary.
3. Taking enhanced due diligence measures to manage and reduce the risks identified as "**high**" risks.
4. Verifying the implementation of these policies, controls and procedures in reality should be done by the internal audit as an independent authority

Fourth: Customers Classification:

1. The bank shall classify its customers according to the nature of their money laundering and terrorist financing risks. This classification shall be periodically updated in accordance with the nature and level of these risks for each customer, taking into account the following factors:

- Type of customer (natural or legal person, non-profit organization, etc.)
 - Occasional customer
 - The ownership structure of the legal person
 - Types of politically exposed persons
 - Types of occupations
 - Geographical location
 - The customer's country of origin
 - Products, services, transactions or service delivery channels (e.g. cash transactions, direct or indirect transactions, cross-border transactions)
 - Any other information indicating the customer's level of risk.
2. Risk mitigation measures applied by the bank shall be commensurate with the nature of the customer's risk.

Fifth: Higher risk: Represents the cases where the bank's assessment of the money laundering and terrorist financing risks is high, taking into consideration the factors below, as a minimum:

1. Factors related to customer risks

- The practice of business in extraordinary circumstances (for example, a large unjustified geographical distance between the bank and the customer)
- Non-resident customers
- Cases in which a legal customer or legal arrangement is a special purpose facility.
 - Businesses that heavily rely on cash
- Unjustified complexity in the ownership structure compared to the nature of the company's business
- High Net Worth Customers
- Customers who belong to regions known to have a high rate of crime (for example, countries known for drug production, transfer or trafficking).
- Customers who belong to, or reside in, countries that do not implement FATF recommendations or do not adequately implement them.
- Businesses classified by the FATF as "high risk" businesses in money laundering and terrorist financing.
 - Customers who meet the risk indicators defined by the bank.

1. Factors related to the risk of countries and geographical regions:

- Countries that lack adequate regulations in combating money laundering and terrorist financing or do not adequately implement FATF recommendations.

- Countries subject to sanctions, embargos or any other measures issued by the United Nations
- Countries with high levels of corruption or other criminal activities
- Geographic areas considered to be financing terrorism or supporting terrorist activities
- Countries where terrorist organizations are present
 - Countries with policy or security conditions hindering the commitment to FATF recommendations.

When determining risk factors for countries and geographical regions, the bank can refer to credible sources such as mutual evaluation reports, follow-up reports and any other relevant reports published by international organizations such as the United Nations and the FATF.

3. Factors related to the risks of products, services, transactions or distribution channels:

- Transactions carried out by anonymous persons (in which cash may be used)
- Non face-to-face business relationships or transactions
- Amounts received by the customer from several persons or from countries that are not consistent with the nature of his business and his risks
- Amounts received by the customer from unknown sources or from a third party that has no clear relationship with the customer

High-risk countries: The countries classified in the FATF lists as high-risk countries with respect to money laundering and terrorist financing or having deficiencies in AML / CFT procedures, which poses a threat to the global financial system, or for which the Kingdom has information that they are high-risk countries in money laundering and terrorist financing.

Sixth: The bank shall identify and assess the risks of money laundering and terrorist financing that may arise in relation to the development of products within new business lines, including new means of service delivery and those

that may arise from the use of new technologies within new or under-development business lines for both new and existing products. The bank shall take appropriate measures to manage and reduce those risks, and shall report the results to the Central Bank of Jordan.

Seventh: All risk related factors shall be considered before determining the overall level of risk and the appropriate level of risk mitigation measures that will be implemented.

Eighth: the appropriate mechanisms to provide the competent authorities, upon their request, with the risks identified shall be made available.

Article (4): Due Diligence Requirements

First: General Provisions

- 1-** Due diligence with relation to customers that needs to be conducted by banks shall mean:
 - 1.1** Identifying the identity of the customers (the permanent or occasional, whether they were natural persons, legal persons or legal arrangements) and their legal status, and verifying such by using documents or data or original information from a reliable and independent source.
 - 2.1** Comparing the name of the customer with the names of individuals and entities listed on debarment lists issued under the UN Security Council resolutions
 - 3.1** Verifying the customer's activity; understanding the purpose of the business relationship with the bank and its nature; and obtaining the relevant information.
 - 4.1** If a person acts on behalf of the customer, it shall be confirmed that he is authorized to do so by verifying his identity.
 - 5.1** Identifying the identity of the beneficial owner and verifying his identity using a government-issued identification document through reasonable measures so that the bank is satisfied that he is the beneficial owner.
 - 6.1** Verifying the sources of funds and supporting documents for operations (transactions) operated in the context of the ongoing banking relationship.

7.1 Exerting continuous due diligence on business relationships and auditing the transactions that are conducted within the framework of an ongoing relation to ensure consistency of these transactions with the bank's information about the customer, the type of his/ her activity and the nature of his/ her risks including the source of funds, when necessary; comparing the customer activity with his peers in the same activity or with those who has the same risk; and recording and keeping all relevant data in accordance with the provisions of these Instructions.

8.1 Ensuring that the documents, data or information obtained under due diligence measures are continuously updated and appropriate by auditing the existing records, particularly regarding high-risk customer categories.

9.1 Obtaining any other information related to Customer Risk Assessment Indicators.

2- The bank shall apply all due diligence measures on customers as set forth in paragraph (1) of item (First) above of this Article, while specifying the scope of such measures using the risk-based approach referred to in Article (3) of these instructions.

3- The bank shall exert due diligence procedures with relation to customers in the following cases (SITUATIONS):

3.1 Before or during the commencement of banking relationship.

3.2 When the bank has doubt about the accuracy or adequacy of previously obtained customer identification data.

3.3 Upon the performance of transactions for occasional customers if the value of a transaction or a number of transactions that seem to be related exceeds (JD10000) or the equivalent thereof in foreign currency.

3.4 If the bank has doubt that the occasional transaction is suspected to be related to money laundering or terrorist financing regardless of its value, or whether the simplified due diligence measures apply to it.

3.5 Any wire transfer transaction performed by an occasional customer regardless of the value thereof.

4- In the event that the bank is unable to complete customer due diligence procedures, the bank should not open the account or engage in any banking relationship with the customer or perform any transaction to his/ her account, and notify the Unit immediately if there is suspicion related to money laundering or terrorist financing pursuant to the form or means adopted by the Unit for this purpose.

5- The timing of verification of the identity of customer and the beneficial owner:

5.1 The bank shall verify the identity of the customer and the beneficial owner prior to, or during, the banking relationship or performing the transactions of occasional customers from reliable and neutral sources.

5.2 The bank may postpone certain procedures for verifying the identity of the customer and the beneficial owner until after the establishment of the constant business relationship, provided that these procedures are completed within a period of not more than 10 working days from the date of establishing the relationship. Otherwise, the relationship shall be terminated, the Unit shall immediately be notified in the case of suspected involvement in money laundering or terrorist financing according to the form or means approved by the Unit for this purpose, and the customer shall not be allowed to withdraw cash upon termination of the relationship but to use one of the other means of payment to enable tracking of movements (audit trail), provided that the postponement is made according to the following

5.2.1 Postponing the verification procedures is necessary to maintain the completion of normal business, so that there is no risk of money laundering or terrorist financing.

5.2.2 The bank has taken the necessary measures to effectively control the risks of money laundering or terrorist financing in relation to the situation in which the postponement has been made. This includes setting

threshold for the number, type and amount of transactions that may be performed prior to the completion of the verification procedures and stating this in the business procedures approved by the bank

6- In case the bank entered into an ongoing relation with the customer, and indicators of suspicious transaction related to money laundering or terrorist financing appeared, the bank shall:

6.1 Complete /re-perform due diligence procedures for the suspected transactions.

6.2 In the event that the bank is not satisfied with the adequacy of the due diligence procedures, and if the continuation of due diligence procedures may alert the customer (Tipping off), the bank shall, in such cases, stop such procedures and notify the Unit immediately pursuant to the form or the means approved by the unit for this purpose along with not allowing the customer to cash withdrawals and using another payment method in relation with Audit trail.

7- The bank shall exercise due diligence towards existing customers based on relative importance and risk and shall exert due diligence measures with respect to its current relationships with them in the cases set out below, provided that the bank is aware of whether due diligence measures have already been taken, the date they have been taken and adequacy of the data obtained:

7.1 When performing transactions in large amounts or using bank instruments in an unusual manner.

7.2 When there is a fundamental change in the customer information authentication mechanism.

7.3 When there is a material change in the way of managing the account.

7.4 When the bank realizes that there is not sufficient information about an existing customer.

8- Updating the customer identification data:

The bank shall exert due diligence measures on an ongoing basis for businesses relationships, which include:

8.1 Auditing the transactions carried out throughout the relationship to ensure consistency of the transactions with what the bank knows about the customers, their type of activity and the risks they pose, including the source of funds, if necessary.

8.2 Ensuring that documents, data or information obtained under due diligence measures are constantly updated and are appropriate by reviewing the existing records, particularly for high-risk customer categories.

8.3 The bank may rely on the identification and verification procedures that have already been carried out, unless it has doubts as to the validity of such information or in case of suspicion of money laundering or terrorist financing or when there is a material change in the way the customer's account is operated which is not consistent with customer activity.

8.4 In the event the customer does not respond to the bank's request to update its data as deemed appropriate by the bank, the bank may gradually suspend some financial transactions and services provided to the non-responsive customer until the customer duly updates his data, subject to activating tools and awareness campaigns for customers on the consequences of failure to update their data and urging them to conduct the update whenever necessary.

Second: Procedures for Identifying and Verifying the Identity of the Customer

- 1- The bank shall set the proper systems to ensure the identification and verification of the customer's identity in accordance with the requirements stated in item (First) of this article.
- 2- The bank shall preview the original and official identification documents of the customer and shall obtain a copy of the same documents signed by the competent employee declaring that it is an original copy.
- 3- Procedures for identifying the identity of a **natural person** shall take into consideration the following:

3.1 The data of identification shall include the full name of the customer, date and place of birth, national number , full information related to the Jordanian identity card, passport number and the personal number for non-Jordanians and his/ her nationality, annual residence permission issued by the Ministry of the Interior or a valid work permit issued by the competent authority if the customer is a

Foreign worker, nature of work, permanent residence address, telephone numbers, the purpose of the business relationship and its intended nature, and any other information the bank deems necessary to complete the process of identifying the customer.

3.2 For persons who are underqualified such as minors, the documents relating to their legal representative in dealing with these accounts shall be obtained in accordance with paragraph (2) above.

3.3 In case a person deals with the bank on behalf of the customer, it shall be verified that there is a valid power of attorney or an authorization approved by the bank. The power of attorney, a certified copy thereof or the authorization shall be maintained, and the attorney identity shall be verified according to the customer identification procedures stipulated in clause (3.1) of this article.

4- Procedures for identifying the identity of a legal person and legal arrangement shall include the following:

4.1 Identification data shall include name of legal person or legal arrangement, legal form, owners' names and addresses, ownership shares, headquarters address, nature of work and type of activity, amount of capital, date and number of registration, tax number, national number of the facility, names of authorized signatories, purpose and nature of the business relationship, names of the persons concerned who occupy the senior management positions with the legal person or legal arrangement, and any other information deemed necessary by the bank to complete the identification process and maintain it up-to-date.

4.2 Obtain the documents indicating the existence of an authorization by the legal person or legal arrangement to the natural persons authorized to act on the account, in addition to the need to verify the identity of the authorized person in accordance with the natural persons' identification procedures stipulated in clause (3.1) of this article and to verify that there is no legal impediment to deal with them and obtain their signatures.

4.3 Obtain information about the provisions regulating the work of the legal person or legal arrangement, including the ownership structure, the controlling management and the provisions governing the powers of making decisions deemed binding to

legal person or legal arrangement. Public Shareholding Companies shall be exempted from providing data relating to Owners' Names, their addresses and ownership shares of the shareholders whose share is less than 10% of the Company's capital, while obtaining a commitment from the authorized signatories to provide the bank with data of any shareholder whose ownership interest reaches this ratio.

4.4 Procedures for identifying the identity of a legal arrangements shall include the following:

4.4.1 The bank shall be aware of the nature of the client, the ownership structure and the board of trustees.

4.4.2 The authorized signatories and controlling persons [taking into account the procedures for identification of natural persons stipulated in item (1.3) of this article] shall be identified.

5- Procedures for identifying the identity of a non-profit organization shall take into consideration the following:

5.1 The identification data shall include the name of the non-profit organization, the legal form, the national ID number of the organization, if any, the address of the headquarters, the type of activity, the date of incorporation, the names of the persons authorized to act on the account, as well as their nationalities, phone numbers, purpose of dealing , sources of income or financing, names of concerned persons who occupy senior management positions with the non-profit organization and any other information deemed necessary by the bank.

5.2 Obtaining the documents indicating the existence of an authorization by the non-profit organization to the natural persons authorized to act on the account, in addition to the need to verify the identity of the authorized person in accordance with the customer identification procedures stipulated in clause (3.1) of this article.

Annex (A) form represents the minimum customer identification data to be collected.

Third: Procedures for verifying customer identification data

The bank shall take the necessary procedures to verify the validity of data and information obtained from the customer through neutral and reliable sources, including communication with the competent authorities that have issued the official documents proving these data, as follows:

1- Verification of the identity of the natural person:

This shall be done by referring to the website of the Civil Status and Passport Department for Jordanian citizens and obtaining a photocopy of the valid passport and any of the identification documents set out in item (Second), clause (3.1) of this article for non-Jordanians, signed by the competent employee as being original duplicates. The customer shall sign an acknowledgement to provide the bank with a copy of the passport upon renewal for non-Jordanians and the bank is entitled to gradually suspend some of the financial transactions and services provided to the customer in the event of failure to do so. Information about the employer and the customer's sources of income, such as an original copy of the contract or salary certificate, shall also be provided

2- Verification of the identity of the legal person or legal arrangement:

This shall be done by verifying the items mentioned in Article 4 / Second / 4 by means of the necessary documents and the information contained therein and by referring to the website of the Companies Control Department and the Ministry of Industry, Trade and Supply, such as the Memorandum of Association and Articles of Association of the legal person and the certificates issued by the Ministry of Industry, Trade and Supply and the industrial and commercial chambers, provided that they are up-to-date. A duly certified official certificate issued by the competent authorities shall also be obtained if the legal person or legal arrangement is registered abroad, in addition to any other information deemed necessary by the bank.

3- In case of legal persons being a foreign company unregistered, and not licensed to operate in the Kingdom: It shall be verified that the opening of accounts or practicing of any transactions by such companies in the Kingdom

comply with the laws and legislations in force, taking into account the nature of the transactions executed over these accounts.

- 4- Verifying the identity of the non-profit organization and its legal entity:**
This shall be done by referring to official documents and the information contained therein, such as the certificates issued by the Ministry of Social Development, or any other competent authority, and whether it is authorized to work in the Kingdom and / or to accept donations and grants from local or external sources and by referring to the website of the Register of Associations.
- 5- Verifying the address of the natural and legal person, legal arrangement and non-profit organization:** This shall be done by obtaining a copy of the lease contract, public utility bills, a visit to the customer's premises, and professions license.
- 6- In the case of opening accounts by correspondence:** The information and documents required in accordance with the customer identification requirements mentioned in Article (4) of these instructions shall be obtained and shall be duly certified either by a financial institution affiliated with the same group, or by official authorities, such as embassies and consulates of Jordan and foreign countries, or by obtaining a recommendation or a fundamental endorsement of the signature from well - known banks or financial institutions.

Fourth: Beneficial owner:

- 1-** The bank shall require each customer to provide a written statement specifying the identity of the beneficial owner of the transaction to be performed (in cases where this is required) so that the statement includes at least the customer identification information.
- 2-** The bank shall recognize the beneficial owner's identity and take reasonable measures to verify this identity according to the nature of the customer's risk (Risk Profile), based on data or information obtained from official documents and data so that the bank is satisfied with the identity of the beneficial owner.
- 3-** The identification of the beneficial owner in case of a legal person shall be considered as follows:
 - 3.1** Identification of the natural person (s), if any, who has / have an effective controlling interest on the customer within the legal person.
 - 3.2** In the event of suspicion about the identity of the natural person or inability to identify him in accordance with clause 3.1 above, the bank shall identify the natural person who has control within the legal person through other means.

3.3 In the event that no natural person is identified under clause 3.1 and clause 3.2 above, the bank shall identify and take the reasonable measures to verify the identity of the relevant natural person who occupies the position of senior administrative officer within the legal person

- 4- The identification of the beneficial owner if the customer is from the legal arrangements shall be considered as follows:
 - 4.1 Express trusts: Identification of the testator or the trustee, as appropriate, as well as the beneficiaries / the beneficiary's category for each other natural person exercising active and actual control over the trust
 - 4.2 Other types of legal arrangements: Identification of persons holding positions equivalent or similar to the abovementioned.

Article (5): The bank shall not maintain or deal with anonymous accounts or accounts with fictitious or digital names, including dealing with or entering into banking relationships with anonymous persons or those with fictitious or fake names or with shell companies or shell banks

Article (6): Simplified Due diligence measures:

First: the Central Bank shall decide, by virtue of orders issued, on the cases or transactions required to be performed or the customers for whom it is necessary to take due diligence measures in a simplified manner when identifying and verifying the identity of the customer and the beneficial owner, which provide examples of low-risk customers or transactions and any international controls or local requirements in this regard.

Second: It shall not be permissible to take simplified due diligence measures in case of suspicion of money laundering or terrorist financing or in circumstances involving high risk.

Article (7) Due diligence measures within the financial group or a third party other than the financial group:

First: The bank may rely on the member financial institutions within its financial group or a third party other than the financial group in accordance with the

provisions of these instructions in the application of due diligence measures and enhanced due diligence measures on the politically exposed customers, provided that the third party is subject to regulation and control by competent authorities and has procedures to comply with the customer due diligence requirements and maintain AML/ CFT records and programs contained in these instructions.

Second: The bank shall consider the degree of risk assessment for the country in which the member financial institution or the third party other than the financial group exists, by taking enhanced due diligence measures in the event the country is of high risk and by adequately reducing any high risks to countries by the financial group policies related to AML/ CFT.

Third: The ultimate responsibility in the application of customer due diligence measures rests with the bank so that it shall comply with the following:

1. Immediately obtain information on:

1.1 Establishing business relationships.

1.2 Performing transactions for occasional customers in which the value of one transaction or several transactions that appear to be linked is more than JD10,000 or its equivalent in foreign currency.

1.3 Performing occasional transactions in the form of wire transfers.

2. Take the necessary measures so that the bank is satisfied that copies of customer identification data and documents as well as other documents related to the customer due diligence requirements will be provided by member financial institution or the third party other than the financial group, upon request by them and without delay.

Article (8): Cases that require enhanced due diligence (i.e. additional measures to exert due diligence and obtain additional, more detailed information on these customers) in addition to the due diligence requirements mentioned in Article (4) of these Instructions:

First: The bank shall take enhanced due diligence measures when the classification of the customer's risks in money laundering and terrorist financing is "**high**", as follows:

1. Obtain the approval of the bank's general director / regional director or their designee from the senior executive management before establishing or continuing

the relationship with these customers. Such approval shall also be obtained upon discovering that the risks of one of the customers or the beneficial owners have fallen within this category.

2. Take sufficient measures to determine the sources of the wealth of the customers and the beneficial owners who have been classified within this risk category.

3. Pursue the transactions of these customers with the bank in a constant and accurate manner; exert enhanced due diligence to work relations and the transactions carried out with any of them; and continue to take enhanced due diligence measures and control of those relationships.

4. Take the necessary measures to determine the background of the circumstances surrounding any of business relationships and the transactions carried out with any of the customers classified within this category and their purposes in case the bank finds that any of them is based on no clear economic justification and take a decision on them while keeping the results in its records.

Second: Dealing with external banks:

1. The bank shall apply the customers due diligence requirements mentioned in Article (4) above when establishing a banking relationship with an external bank.

2. The bank shall be aware of the nature of the external bank's activity and its reputation in the field of anti-money laundering and combating the financing of terrorism through the information available to the public and whether it has been subjected to investigation on money laundering or terrorist financing or to regulatory action by supervisory bodies.

3. The approval of the bank's general director / regional director shall be obtained prior to the establishment or continuation of a relationship with the external bank.

4. The bank shall ensure that the external bank is subject to effective regulatory supervision by the regulatory authority in the parent country and / or the country in which it resides.

5. The bank shall verify the availability of adequate AML/ CFT programs with the external bank.

6. The bank shall assess the AML/ CFT policies, procedures, regulations and controls at the external bank and shall be satisfied that the external bank does not allow the use of its accounts by shell banks or for the execution of AML/ CFT related

transactions, so that the relationship with the external bank is built on the understanding of each bank of its responsibilities in the field of combating money laundering and terrorist financing in a clear manner.

7. The bank shall not commence or continue the banking relationship if the external bank has transactions with shell banks.

8. The bank shall ensure that the external bank has implemented due diligence measures relating to the customers who have the authority to use the Intermediate Payment Accounts, which are directly used by third parties for the conduct of their business, such as (Payable-Through Accounts) / (Downstream / Upstream Clearing / (Nested Accounts), and that the external bank has the capacity to provide information on the due diligence of such customers and the transactions performed on those accounts when necessary.

Third: Indirect dealings with customers:

The bank shall develop policies and procedures to mitigate the risks associated with the misuse of indirect, non-face-to-face transactions and to effectively apply them, particularly those made using modern technology such as ATM, telephone and Internet banking services, electronic points of sale (EPOS), prepaid or refillable cards, taking into consideration the instructions in force issued by the Central Bank of Jordan in this regard.

Fourth: Foreign politically exposed persons:

1. The bank shall establish a risk management system to determine whether the customer or beneficial owner falls within this category.
2. If any of the bank customers or beneficial owners are identified within this category, the bank shall take the enhanced due diligence measures as stated in item (First) of this article.

Fifth: Local politically exposed persons:

1. The bank shall take reasonable measures to determine whether the customer or beneficial owner falls within this category.
2. If any of the bank customers or beneficial owners are identified within this category, the bank shall assess the level of risks of money laundering and terrorist financing involved in the business relationship with this customer

3. If the bank assesses the risk to the bank as a "high risk", the bank shall exert enhanced due diligence measures as described in item (First) of this article and the bank can be satisfied with due diligence measures in the event that the customer risk assessment is below that

Sixth: Unusual transactions:

1. Unusual transactions are:

1.1 Transactions that are unusually large or complex in relation to the customer transactions and the movement of his account, or several interconnected transactions that collectively constitute a single transaction.

1.2 Any other transaction of an unusual form that does not appear to have a clear economic justification or does not comply with the nature of the customer risk and activity.

2. The bank shall exert enhanced due diligence on unusual transactions, as well as when there is suspicion of the validity or accuracy of the customer identification data after the establishment of the banking relationship, by carrying out the necessary analyses and studies in addition to any other procedures necessary to verify the source of funds and the nature of transaction, with the need to keep records thereof regardless of the decision taken and to include the bank's compliance policy and / or the applicable procedures of examples of the additional requirements necessary to exert enhanced due diligence on such transactions.

Seventh: Other cases:

The bank shall exert enhanced due diligence in the following cases in line with the level of risk:

1. When opening correspondent account.

2. When requesting deposit facilities.

3 - When renting a safe deposit box.

4. When depositing cash or checks in an existing account by a person / persons who do not represent the account holder under a power of attorney or approved authorization by the bank.

Article (9) The financial group and the external branches:

1. If the bank falls within a financial group, the group shall be required to apply AML / CFT programs at the group level, which shall apply, as appropriate, to all branches and subsidiaries in which the group owns a majority, taking into account the risks of money laundering and terrorist financing and the size of business. These programs shall include the following measures:

First: Prepare policies, procedures, internal controls and appropriate arrangements in relation to the following:

(1) Compliance management (including the appointment of the compliance officer at the management level).

(2) Appropriate test procedures to ensure high standards of efficiency when recruiting staff.

Second: Develop an ongoing training program for employees.

Third: Establish an auditing unit to test the system.

Fourth: Develop policies and procedures to exchange the information required for customer due diligence and manage the money laundering and terrorist financing risks.

Fifth: Provide information about customers, accounts and transactions by branches and subsidiaries to the compliance, auditing and / or AML / CFT functions at the group level, which may include analysis information of unusual transactions or activities and may also include notification to the Unit about the transaction, when necessary, for AML / CFT purposes, in line with risk management.

Sixth: Provide adequate guarantees on the confidentiality and use of exchanged information including non-notice guarantees.

2. If the host country does not allow the appropriate implementation of AML / CFT measures that are consistent with the Kingdom's measures, the financial group shall implement appropriate additional measures to manage the AML / CFT risks and inform the Central Bank of Jordan about that.

Article (10): Transfers: -

First: Scope of application:

1. The provisions of this article shall apply to incoming and outgoing transfers, including wire transfers worth more than JD 700 or its equivalent in foreign currencies, taking into account the obligations imposed by the UN Security Council resolutions regarding the prohibition of dealing with listed individuals and entities and freezing of any funds that belong thereto in accordance with the provisions of the instructions issued in this regard.

2. Notwithstanding the provisions of paragraph (1) of this article, the bank shall ensure that all the transfers below JD 700, or its equivalent in foreign currencies, contain all the information of the originator and the beneficiary of the wire transfer as stated in this article, bearing in mind that it is not necessary to verify the accuracy of such information unless there is suspicion of money laundering or terrorist financing.

Second: Obligations of the bank issuing the transfer:

1. The bank shall have full information about the originator and the beneficiary of the transfer, as follows:

1.1 If the originator is a customer with whom the bank has a banking relationship, the following transfer information shall be taken from the banking system (automatic linking) within locked fields:

1.1.1 Full name of the originator of the transfer.

1.1.2 International Bank Account Number (IBAN)

1.1.3 Address of the originator or statement from the customer that his/her address in the bank records has not changed.

In addition to the following data:

1.1.4 Purpose of the transfer

1.1.5 The relationship between the originator and the beneficiary of the transfer

1.1.6 A confirmation by the originator of the transfer about the beneficial owner of the transfer according to available information

1.2 If the beneficiary of the transfer is a customer with whom the bank has a banking relationship:

1.2.1 Full name of the beneficiary of the transfer

1.2.2 International Bank Account Number (IBAN)

1.2.3 Address of the beneficiary

1.2.4 Purpose of the transfer

1.2.5 The relationship between the originator and the beneficiary of the transfer

1.2.6 A statement from the beneficiary of the transfer that he/ she is the beneficial owner of the transfer.

2. If the originator of the transfer does not have an account with the bank (occasional customer):

2.1 The bank shall establish a system whereby a unique reference number is given to the transaction to allow its tracking

2.2 Customer due diligence measures shall be taken as provided for in Article (4) of these Instructions.

3. Procedures for verifying all information shall be taken in accordance with the standards and procedures stipulated in Article (4) of these instructions before sending the transfer.

4. The bank shall attach all the data stated in paragraph (1) and paragraph (2) of this article to the transfer, as follows:

4.1 The bank shall be able to provide the respondent bank or the competent official authorities with all the requested information within three working days from the date of receiving the request.

4.2 The bank shall be able to immediately respond to any order issued by the competent official authorities requiring the disclosure of such information.

5. For the batch transfer, the issuing bank shall attach the account number of the originator of the transfer or the unique reference number in the absence of an account, provided that:

5.1 The bank keeps full information on the originator and the beneficiary of the transfer as provided for in paragraphs (1) and (2) of this item.

5.2 The bank is able to provide the respondent bank or the competent official authorities with all the requested information within three working days from the date of receiving the request.

5.3 The bank is able to immediately respond to any order issued by the competent official authorities requiring the disclosure of such information.

6. The bank shall ensure that non-routine transfers are not sent within single batch transfers in cases that would increase the risk of money laundering and terrorist financing.

7. If the bank is unable to meet the requirements specified in clause (Second) of this article, the bank shall not execute / issue the transfer.

Third: Obligations of the respondent bank:

1. The bank shall establish effective regulations to detect any lack of information concerning the originator or the beneficiary of the transfer as stated in paragraphs

(1) and (2) of clause (Second) above.

2. The bank shall rely on the risk-based approach in the procedures for verifying the information relating to the transfers received into the accounts

of its customers, as well as when the transaction is suspected to be linked to money laundering or terrorist financing.

3. The bank shall adopt effective procedures based on the assessment of the degree of risk in dealing with transfers in which the information about the originator or the beneficiary of the transfer has not been completed. Such procedures include request for the information that has not been received by the bank issuing the transfer. In the event of failure to obtain such information, the bank shall take measures based on the assessment of the degree of risk, including the execution, suspension or rejection of the transfer, provided that this is a valid indication of the bank's assessment of the existence of suspicion of that transaction.

4. In case of cross-border wire transfers amounting to 700 dinars or more, the respondent bank shall verify the identity of the beneficiary, if not previously verified, and keep the data and records as specified in Article (10) of these Instructions.

5. In the event of receipt of a batch transfer, the respondent bank shall obtain all the information and requirements referred to in Article (10 / Second / 5) above. In case of failure to complete such data within three working days, the respondent bank shall refuse to execute the transfer.

6. The bank shall verify the identity of the beneficiary and keep this information for at least five years.

Fourth: Obligations of the intermediary bank:

1. If a bank participates in the execution of the transfer without being the issuing or respondent bank, it shall ensure that all the information specified in item (Second) of this article is attached to the transfer when the transfer is executed and shall take reasonable measures consistent with the straight through processing, in order to identify the transfers that lack information about the originator or the beneficiary.

2. If the bank is unable to keep the information attached to the transfer for technical reasons, it shall keep all the attached information as received for at least five years, irrespective of the completeness or shortage of such information, so as to be able to provide the available information to the respondent bank within three days from the date of request.

3. If the bank decides to execute the transfer in accordance with its internal policy and procedures, it shall report the respondent bank on incomplete information upon conducting the transfer process and shall keep all the attached information as received for at least five years, irrespective of completeness or shortage of such information.

Fifth: The following are excluded from the attachment provisions stipulated in paragraph (4) of item (Second) and item (Fourth) of this article:

1. The wire transfers arising from transactions made using payment or credit cards, provided that the transfer is accompanied by the card number.
2. The wire transfers in which each of the ordering and the respondent banks is acting for its own account

Sixth: General provisions relating to transfers:

The bank shall establish effective policies and procedures based on the assessment of the degree of risk in dealing with transfers, in which the bank specifies when to execute, reject, or request additional data about the transfers that did not fulfil all the information about the originator or the beneficiary and the appropriate follow-up procedures in such cases including immediate reporting to the Unit.

Article (11): Record-keeping:

First: The bank shall keep records and documents to record its local and international financial transactions. Such records shall include the data relating to due diligence and enhanced due diligence as set out in these instructions, including risk assessment procedures, for at least five years from the date of completion of transaction or termination of the relationship, as appropriate.

Second: The bank shall keep the records and documents supporting the banking relationships and transactions, commercial correspondence, and results of any analysis carried out, which are obtained as a fulfillment of the obligations stipulated in these instructions so that they include the original documents or copies thereof that are acceptable to the courts in accordance with the legislation in force in the Kingdom for at least five years from the date of completion of the transaction or termination of the relationship, as appropriate, including the date of termination of the occasional transaction.

Third: The bank shall develop an integrated information system for keeping the records, documents and information referred to in items (First) and (Second) of this article, so as to be able to respond to the request by the Unit and competent official authorities for any data or information in an integrated and fast manner within the specified period, and to ensure that the transaction records are sufficient to allow the re-establishment of individual transactions.

Article (12): Reporting of transactions suspected to be related to money laundering and terrorist financing:

First: If any employee in the bank has any doubt of a transaction suspected of being linked to money laundering or terrorist financing, he/ she shall immediately report to the money laundering reporting officer (MLRO).

Second: Duties of the MLRO:

1. The MLRO shall immediately report to the Unit all the transactions he/ she suspects or has reasonable grounds of being linked to money laundering or terrorist financing, whether or not such transactions are carried out and regardless of their value, by the means or the form approved by the Unit.
2. In the event that the suspected customer requests to close his/ her account(s), the MLRO shall not allow customer to withdraw the amounts in cash, but to use one of the other means of payment so as to enable tracking of the movements (audit trail) and shall immediately report to the Unit.
3. The MLRO shall provide the Unit and competent authorities with data concerning the transactions suspected of being linked to money laundering or terrorist financing as well as any other information or data required in accordance with the means approved by these authorities and shall facilitate their access to relevant records and information for the purpose of carrying out their tasks.
4. All employees shall be banned from the disclosure, directly or indirectly, or in any means whatsoever, of the Unit reporting or any of the reporting procedures on the transactions suspected of being linked to money laundering or terrorist financing or any information related thereto.

5. Anyone who have access or knowledge, directly or indirectly or by virtue of his or her job or work, shall be prohibited from disclosing any information provided or exchanged in accordance with the provisions of law and the regulations and instructions issued pursuant thereto, including these instructions.

6. The bank shall prepare files for the transactions suspected of being linked to money laundering or terrorist financing, in which the copies of reporting of such transactions and the relevant data and documents shall be filed. Such files shall be kept for at least five years from the reporting date or pending a final judgment on such instructions, whichever is longer.

Article (13): Internal regulations:

The bank shall establish appropriate internal regulations which include internal policies and controls and adequate and effective procedures, based on the bank's understanding of the money laundering and terrorist financing risks. These regulations shall include the following:

First: A clear AML / CFT policy approved by the board of directors or the regional director of the branches of foreign banks. This policy shall constantly be updated to include at the minimum all the requirements contained in these instructions.

Second: Detailed written AML / CFT procedures, taking into account the precise definition of duties and responsibilities in accordance with the policy approved and the instructions issued by the Central Bank in this regard.

Third: Designating independent and qualified staff within the internal audit department provided with sufficient resources to check compliance with the AML / CFT policies, controls and procedures.

Fourth: An appropriate mechanism to verify compliance with the instructions, policies and procedures established to combat money laundering and terrorist financing, carried out by both the audit employees

mentioned in item (Third) of this article and the compliance officer, taking into account the coordination in defining the powers and responsibilities among them.

Fifth: Developing the systems and procedures to ensure that the internal audit bodies have the role of examining the internal control systems to verify their effectiveness in combating money laundering and terrorist financing, with the need to be periodically reviewed to complete any deficiency or to be updated and developed to increase their efficiency and effectiveness.

Sixth: Identifying the name of the MLRO and his/ her deputy and informing the Unit and the Central Bank in case of changing either of them, provided that both of them have the appropriate qualifications and obtaining the non-objection of the Central Bank for the appointment or termination of their services.

Seventh: Defining the powers of the MLRO to include at least the following:

1. Receiving information and notifications on the unusual transactions or those suspected of being linked to money laundering or terrorist financing, as well as examining them and taking the appropriate decision whether to immediately report to the Unit or to keep them, provided that the decision to keep them is justified and the documents required for reporting are kept for at least five years.
2. Preparing periodic statistical reports to the board of directors on the transactions suspected of being linked to money laundering or terrorist financing.

Eighth: Determining the powers of the MLRO so as to include at least what enables him/ her to exercise his/ her powers independently, in order to ensure the confidentiality of the information he/ she receives and the measures he/ she undertakes, and thus to have access to the records and data required for doing his/ her business.

Ninth: Training and qualifying:

1. The bank shall develop continuous training plans and programs in the field of combating money laundering and the financing of terrorism for the bank

employees, provided that such programs include means of money laundering and terrorist financing, how to detect and report them, and how to deal with suspicious customers, while keeping records of all training programs carried out for a period of not less than five years, so as they include the names of the trainees, their job titles, and the training entity, both inside and outside the Kingdom. All new employees shall be subjected to training courses in the field of AML / CFT during the first year of their appointment.

2. The bank shall adopt policies, procedures and controls to ensure the highest standards in the recruitment of employees in order to verify the appropriateness of senior executive management, MLROs and other employees involved in the AML / CFT process.

3. Allocating an annual independent budget approved by the board of directors of the bank or the regional board of directors of the foreign bank to finance the bank employees' training, qualifying and attending of the AML / CFT seminars and workshops and to provide systems to assist the compliance department to carry out its duties, while providing the Central Bank at the end of each year with statistics showing the training courses and workshops attended by the employees during the year and their costs.

4. Qualifying the officers and assistants of branch managers at the bank in addition to the front desk staff in order to support and ease the burden of compliance departments.

5. The bank shall provide the employees with the necessary information on:

5.1 Applicable AML / CFT law and the regulations, instructions and decisions issued pursuant to any of them.

5.2 Patterns suspected of being involved in money laundering and terrorist financing as contained in Annexes 2 (a) and 2 (b) of suspicion indicators. These indicators shall be used as a tool for educating the bank employees and shall be taken into account in suspicious cases.

5.3 Procedures to notify the MLRO of the transaction suspected by the employee of being linked to money laundering or terrorist financing.

5.4 Policies, internal controls and procedures adopted by the bank to combat money laundering and terrorist financing according to the degree of risk.

6. The board of directors and executive directors shall support the compliance department staff with qualified and experienced personnel in the field of combating money laundering and terrorist financing and make sure they have personal and professional qualities that enable them to perform their duties effectively.

7. The topic of employees' dealing with unusual transactions shall be given the necessary training and qualifying.

Article 14: Security Council Resolutions:

Subject to the provisions of the instructions issued pursuant to the provisions of law, the bank shall implement the obligations contained in the relevant enforceable international resolutions, including all resolutions issued under Chapter VII of the UN Charter, which are communicated by the Central Bank of Jordan or the competent authorities.

Article 15: Closing Provisions

First: Any administrator shall be prohibited from managing any account on behalf of any customer, except for the spouse and first-degree relatives after obtaining the approval of the general manager or the regional manager of branches of foreign banks.

Second: The bank may not allow the business transactions on the accounts of natural persons (business-related financial transactions). If the bank verifies that its individual customers execute such transactions, the natural customer shall be notified of the need to discontinue business transactions on his account. If he fails to do so, his account shall be closed, and the Unit shall be notified in the event of suspicion of money laundering or terrorist financing in accordance with the form or means approved by the Unit for this purpose.

Third: The bank may not allow the transactions related to exchange and transfer to be executed through accounts of persons who are not authorized to do so. If the bank verifies that its customers execute such transactions, the Central Bank of Jordan shall be notified in accordance with the Exchange Act in force and the Unit shall be notified in the event of suspicion of money laundering or terrorist

financing in accordance with the form or means approved by the Unit for this purpose.

Fourth: Prepaid cards may not be issued to non-bank customers.

Fifth: If the bank violates any provision of these instructions, the bank shall be liable to the punishment or a measure or more of the sanctions and procedures established pursuant to the provisions of the Banking Law No. (28) for the year 2000, and amendments, and / or the Anti Money Laundering and Counter Terrorist Financing Law in force.

Sixth: Subject to the provisions and requirements of the Law and other instructions issued by the Central Bank of Jordan, banks operating in the Kingdom shall provide the Central Bank of Jordan with all reports issued by the internal and external control bodies if they include references to violations or observations related to procedures to combat money laundering or terrorist financing.

Seventh: Banks operating in the Kingdom shall provide anti- money laundering and counter terrorist financing unit within the specified period with any additional information, reports, or statistics required by the unit for the purpose of executing the provisions of the Law, regulations, and instructions issued thereof.

Eighth: The Bank should refer to the FATF methodology regarding the application of the methodology of assessment of the technical compliance with FATF recommendations and the effectiveness of AML / CFT systems and any matters not mentioned in these instructions.

Ninth: Anti Money Laundering and Counter Terrorist Financing Instructions No. (51/2010) dated 23/11/2010 are hereby repealed, as well as circular number (10/2/4/8874) dated 3/7/2016. These instructions shall be valid as of the date of their issuance.

Governor

Dr. Zeyad Fariz

Attachments

Annex 1 - Minimum customer identification data

Annex 2 - a: Suspicion indicators for transactions related to money laundering

Annex 2 - b: Suspicion indicators for transactions related to terrorist financing