No.: 28/2/12496

Date: 28/9/2020

Instructions of Anti Money Laundering and Countering Terrorism Financing for Microfinance Companies No. (8) Of 2020

Issued pursuant to the provisions of Article (18/ B) of the Anti- Money Laundering & Countering Terrorism Financing Law No. (46) Of 2007 and its amendments, and Article (26/ G) of the Microfinance Companies Bylaw No. (5) Of 2015

Article (1): These instructions are cited as "Instructions of Anti Money Laundering and Countering Terrorism Financing for Microfinance Companies" and shall enter into force on the date of their issuance.

Article (2): Definitions

A) The words and phrases included herein shall have the meanings assigned to them in the Anti Money Laundering and Countering Terrorism Financing Law in force, unless the context indicates otherwise.

B) The following words and phrases shall have the meanings assigned to them hereunder wherever they are mentioned in these instructions, unless the context indicates otherwise:

The Central Bank: The Central Bank of Jordan

The Law: The Anti- Money Laundering and Countering Terrorism Financing Law in force

The Bylaw: The Microfinance Companies Bylaw No. (5) Of 2015 or any replacing legislation

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

The Company: The microfinance company licensed in accordance with the provisions of the Bylaw.

The Board: The board of directors or the management committee of the company

The business relationship: the relationship that emerges between the company and the customer in relation to the activities and services provided by the company to its customers.

The ongoing relationship: the business relationship that, upon establishment, is expected to extend to a non- defined period and to include several operations

The Customer: each person who receives or deals with any of the financial services with the company, whether a natural or a legal person, a legal arrangement, or a non- profit organization. Anyone who commences receiving or dealing with any of those services is also considered a customer.

The Occasional Customer: the customer who is not bound to the company by an ongoing relationship

Foreign Politically Exposed Persons: Persons 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; or who used to be a prominent politician or "VIP" figure of a political party; or senior executives at state- owned companies. These include, as well, first-degree relatives as a minimum, persons close to them, or any persons who act on their behalf or hold authorizations issued thereby.
This definition does not apply to individuals occupying middle rank positions or less in the aforementioned categories.

Domestic Politically Exposed Persons: Persons who are or have been entrusted with a senior public job in the kingdom such as a prime minister, a judge, a military official, or a senior governmental official; or used to be a prominent politician or a "VIP" figure at a political party; or the senior executives in state- owned companies. These include first degree relatives as a minimum, persons close to them, or any persons who act on their behalf or hold authorizations issued thereby.
This definition does not apply to individuals occupying middle rank positions or less in the aforementioned categories.

Persons (either foreigners or locals) assigned (previously or currently) with outstanding tasks by an international organization: These are members of the senior management; i.e. manager and their deputies and members of the Board of Directors (BOD) or equivalent positions in an international organization. These include their first-degree relatives as a minimum, persons close to them, or any persons acting on their behalf, or own delegations issued by them.
This definition does not apply to individuals occupying middle rank positions or less in the aforementioned categories.

Control: The direct or indirect capacity to exercise an effective impact on the actions and decisions of another person.

Influential Interest: controlling a minimum of (10%) of the capital of a legal person.

Beneficial Owner: The natural person who ultimately owns the real interest and the business relationship is taking place to his/ her interest or on his/ her behalf or has full or effective control of a legal person or a legal arrangement and has the right to do a legal act on behalf of either one.

Reporting officer: An official of the Senior Management of the company (could be the compliance oversight manager) who undertakes reporting operations suspected to be linked to money laundering or terrorism financing.

Senior Executive Management: Includes the general manager of the company or the regional manager, deputy general manager or deputy regional manager, assistant general manager or assistant regional manager, the financial manager, operations manager, risk management manager, internal audit manager, and compliance oversight manager, in addition to any employee in the company who has an executive authority parallel to any of the authorities of the aforementioned persons, and is functionally reporting directly to the general manager/ regional manager.

The Financial Group: A group consisting of a parent company or any other legal person, who own the controlling shares, and who coordinate the functions with the rest of group members to implement or execute supervision of the group alongside the branches and/ or subsidiaries subject to the policies and procedures of Anti Money Laundering and Countering Terrorism
Financing at the group level.

Shell Bank: A bank that is characterized by one of the following:

- has no physical presence in the country in which it is incorporated and licensed. Physical presence is construed as a meaningful mind and management located within a country. The existence simply of a local agent or low- level staff does not constitute a physical presence.
- does not keep records for its operations.
- is not subject to supervision by a competent supervisory authority, either in the country in which it was incorporated or in any other country.
- Unaffiliated with any financial services group that is subject to effective consolidated supervision.

The shell bank definition does not apply to a bank that does not have a permanent headquarters while being a subsidiary to a licensed bank that has a physical presence and is subject to an effective supervision.

Shell Company: A company that is used as a conduit for operations without keeping any assets and does not do operations related to its activity even if registered.

Subsidiary Company: A company in which one person or a group of persons united by a common interest own a minimum of (50%) of its capital, or in which this person or these persons own the controlling shares allowing to control its management or its general policy.

Non-Profit Organization: Any legal person or legal arrangement or institution established pursuant to the provisions of relevant laws for raising or spending funds for charitable, religious, cultural, educational, social or any other similar purposes and is not aimed at realizing or sharing profit from its activity or at achieving a personal interest. This includes the foreign branches of international non-profit organizations and entities.

Legal Arrangement: The relationship that is created pursuant to a contract between two or more parties, while not resulting in the establishment of a legal entity, such as direct Express trust or similar legal arrangements.

Express trust: These are the legal relationships formed– between living persons or at death– by a person or trustee, when assets have been put under control of the person or trustee to the account of a beneficiary or for a certain purpose. However, the assets must be independent assets and not part of the property of the trustee. The right to the assets of the trustee remain in the name of the testator or in the name of another person on behalf of the testator.

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 Risks: The risk of money laundering and/or terrorism financing.

High risk countries: countries listed by the Financial Action Task Force (FATF) as countries of high risks or that have an inefficiency in anti-money laundering and countering terrorism financing procedures, thus posing risk on the global financial system, or there is information available at the Kingdom on them as being high risk countries.

Article (3): Application Scope

The provisions herein will apply to the following:

A) Microfinance companies and their branches operating in the kingdom.
B) Branches of companies and their subsidiaries abroad, to the extent allowed by the laws and the by- laws in force in countries where they operate, while taking into consideration that the enhanced standards must be applied, though, to the extent possible in case the requirements of Anti- Money Laundering and Countering Terrorism Financing (AML/CFT) in the hosting country differ from the requirements in the parent country. However, the Central Bank must be informed of any impediments or restrictions that can limit or prevent the implementation of these instructions.
C) Subsidiaries of companies operating in the kingdom provided that these companies are not subject to oversight by another supervisory authority in the kingdom, while that authority has issued special instructions for anti- money laundering and countering terrorism financing.

Article (4): Risk- Based Approach

A) Risk Management

1. The scope and intensity of the risk management function must commensurate with the nature, size, and complication of the company's operations and activities, in addition to the level of money laundering and terrorism financing risks it has.
2. The money laundering and terrorism financing risk management function in the company must be compatible and integrated with the overall level of risk management it has.

B) Risk Assessment

1. The company must conduct a comprehensive assessment of the money laundering and terrorism financing risks at least once a year, or in case the need arises for conducting this assessment as a result of a substantial change in the nature of the risks that the company is exposed to. Through this assessment, money laundering and terrorism financing risks are identified, evaluated, and understood, with regards to the customers, countries, geographic areas, products, services, transactions, and channels of providing the service, according to a methodology approved by the company's board of directors or the regional management of the foreign company's branch. The assessment shall include company branches, and its subsidiaries inside and outside the kingdom, and the assessment operations should be documented, taking into consideration all related risk factors before identifying the overall level of risks and the appropriate level of the risk mitigating procedures that will be applied.
2. The assessment must include the following as a minimum:
   A) The results of oversight of the activities executed by the company such as the level of the company's exposure to money laundering and terrorism financing risks, the classification of the risks according to the main activities, and customers' categories.
   B) The details of the significant risks events that occurred internally or externally and their impact on the company.
   C) Any changes that recently occurred in the instructions or the circulars regulating AML/CFT and their impact on the company.
3. The company must provide the Central Bank at least on an annual basis with the following:
   A) The approved assessment methodology and any amendments thereto
   B) The results of the assessment reported to the Senior Executive Management and the board.
   C) The internal auditor's report of the company clarifying the recommendations and procedures that are intended to be taken to mitigate the high risks revealed as a result of the assessment.

Risk control and mitigation

1. The company must take all necessary procedures for effective oversight and detection of money laundering and terrorism financing risks, so that it has the following at a minimum:
   A) Policies, controls, and procedures approved by the senior executive management, and adoption of the necessary foundations for managing the risks that were identified, assessed, monitored, and mitigated.
   B) Internal control systems that would manage the risks.
   C) Checking the effectiveness of internal control systems that are placed for managing the identified risks.
   D) Monitoring the implementation of these policies, controls and procedures in reality by the company's internal audit and enhancing it if necessary.
2. The company must update scenarios for its own information technology systems on a regular basis, and adopt risk management information systems to detect suspected transactions based on the trends and methods of money laundering and terrorism financing.
3. The company must provide the appropriate mechanisms for providing the competent authorities, based on their request, with the identified risks.
4. The company must undertake enhanced due diligence procedures for managing high risks and mitigating them.

C) Customer classification

1. The company should classify its customers according to the nature of their risks related to money laundering and terrorism financing. This classification should be updated periodically and in accordance with the nature and level of those risks for each customer, taking into consideration the following factors:
   A) Resident or non-resident.
   B) Customer's type (natural person, legal person, legal arrangement, non-profit organization).
   C) The occasional customer.
   D) The structure of the legal person's ownership.
   E) Types of Politically Exposed Persons.
   F) Geographic location.
   G) The nature of activity.
   H) The customer's country of origin.
   I) Products, services, transactions, or channels of providing the service.
   J) Any other information indicating that s/he is a high- risk customer.
2. Risk mitigation procedures applied by the company have to be commensurate with the nature of the customer's risks.
3. The guidance manual [Annex (1)] includes the cases where the company's risk assessment is high at a minimum.

Article (5): Due Diligence Requirements

A) General Rules

1. Customer Due diligence (CDD) means identifying the customer, his/ her legal status and the purpose of the business relationship and its nature as well as the beneficial owner (if any). All of these issues must be verified, and the operations under the ongoing business relationship must be continuously followed up using any of the methods stipulated in relevant legislations. This is in addition to identifying the nature of future relationship between the company and the customer and its purpose. CDD procedures that should be implemented by the company include the following:
    a. Obtaining information regarding the customers' identity (permanent or occasional; either natural persons, legal persons, legal arrangements, or a non-profit organization) and their legal status, and verifying it using documents, data, or authentic information from a reliable and independent source.
    b. Comparing the name of the customer with the names of individual and entities listed on debarment lists issued under the UN security council resolutions
    c. Verifying the customer's activity and understanding the purpose of the business relationship with the company and its nature, in addition to obtaining the related information.
    d. In case of the existence of a person acting on behalf of the customer, it must be verified that he/ she is authorized to do so, by identifying and verifying his/ her identity.
    e. Identifying the beneficial owner and taking reasonable procedures in verifying his/ her identity using a government issued identification document, so that the company gains enough confidence that it is aware of the beneficial owner identity.
    f. Obtaining any other information related to the customer's risks assessment indicators.
    g. In case the customer is a legal person, a legal arrangement, or a non-profit organization, the company must verify the customer's nature and the control over it, as well as the ownership structure and the council of guardians.
    h. Verifying the sources of repayment within the framework of transactions implemented with the company.
2. The company must apply all CDD procedures stipulated in clause (1) of this Article, while identifying the scope of these procedures using the risk- based approach indicated in Article (4) of these instructions.

B) The company is banned from dealing with anonymous accounts, accounts under fictitious names, or digital ones, including dealing or entering into a business relationship with anonymous persons, or those with nicknames, or fake names, or with shell banks or companies.

C) The company is required to undertake due diligence measures for the customer and the beneficial owner (if any) in the following cases:

1. upon and during the establishment of the business relationship with the client.
2. If there are doubts about the veracity or adequacy of previously obtained customer identification data.
3. If there is a suspicion of a money laundering or terrorism financing transaction regardless of its value or the applicability of simplified due diligence.
4. Upon carrying out occasional customers' transactions if the value of one transaction or that of several transactions, which seem to be interconnected, exceeds JD (5,000).

D) In case the company is unable to comply with CDD procedures, it shall not engage in any business relation with the customer, and the Unit must be instantly informed in case of a suspected money laundering or terrorism financing act using the form or tool approved by the Unit for this purpose.

E) Timing of customer and beneficial owner identity verification

1. The company must verify the customer's and the beneficial owner's identity before and during the business relationship or the implementation of transactions for occasional customers from reliable impartial sources.
2. The company may postpone some identity verification procedures for the customer and the beneficial owner until after the establishment of a permanent business relationship, provided that it will be completed during a period of (10) working days as a maximum from the date of establishing the relationship. In other cases, the relationship shall be terminated and the unit should be informed in case of a suspected money laundering or terrorism financing act using the form or method approved by the Unit for this purpose, provided that the postponement is according to the following:
    a. The postponement of verification procedures is necessary to maintain the accomplishment of ordinary businesses, while not resulting in money laundering and terrorism financing risks.
    b. The company has undertaken the necessary procedures to effectively control the money laundering and terrorism financing risks for the case where the postponement takes place, including setting limits for the number and type of transactions that might be implemented before completing the verification procedures, and including that in the business procedures approved at the company.
    c. The company shall accomplish these procedures as soon as possible.

3. In case a money laundering or a terrorism financing operation is suspected and the company believes, for logical reasons, that resuming the due diligence process will alert the customer ((Tipping off), the company is allowed not to resume the due diligence procedures, provided that it instantly informs the Unit using the form or tool approved thereby for this purpose.
4. If the company enters into an ongoing relationship with the customer before fulfilling the CDD procedures, and the company could not fulfill them later, it must terminate this relation and inform the Unit in case of a suspected money laundering or terrorism financing transaction using the form or tool approved by the Unit for this purpose.
5. In case the company is unable to comply with CDD procedures, it shall not engage in any business relationship with the customers, and it should instantly report to the unit in case of a suspected link to money laundering or terrorism financing using the form or tool approved by the Unit for this purpose.

F) The company must implement the due diligence procedures with regard to the existing customers who are dealing with it, according to relative materiality and risks, in the following times:

1. When entering into business relationship of relatively large amounts, or when the customer uses new products.
2. When there is a substantial change in the customer's identification data or in case an insufficiency has been revealed in the data available on one of the existing customers.
3. When the customers' data updating date is due or the company realizes that there is no sufficient information available at it about one of those customers. This should be done every two years as a minimum in the cases of ongoing transactions.

G) Updating data

The company should undertake due diligence procedures on an ongoing basis regarding the business relationship, including:

1. Auditing the transactions that take place as long as the ongoing relation is existing, in order to ensure consistency of these transactions with what the company knows about the customer, his/ her pattern of activity, and the risks he/ she represents as well as the source of his/ her funds if necessary, and comparing that with his/ her peers in the same activity, or those within the same risk level, recording all related data and storing them according to the provisions of these instructions.
2. Ensuring that documents, data, or information obtained under the due diligence procedures is continuously updated and adequate. This can be done by reviewing the existing records especially for the high- risk segments of customers, as the updating should be implemented every two years as a maximum.
3. The company may rely on the identification and verification procedures that were previously implemented unless it has suspicions regarding the accuracy of this information or in case of suspicion of money laundering and terrorism financing or if there is a substantial change in the customer's method of managing his/ her account that does not match the customer's activity.

4. In case the customer does not respond to the company's request to update his/ her data, according to what the company believes appropriate, the company may gradually suspend some of the transactions and services provided for such a customer, until he/ she duly updates his/ her data, provided that awareness campaigns for customers are activated, with regard to the consequences of not committing to updating the data, in addition to encouraging them to update whenever necessary.

H) Reliance on a third party

1. The company may hire a third party for completing the implementation of due diligence procedures and enhanced due diligence towards customers in accordance with these instructions either through completing the necessary data or verifying the provided data, provided that the following requirements are fulfilled:
   a. The company must instantly obtain from the third party all necessary information and documents, related to CDD procedures mentioned in this Article.
   b. The company must make sure that the third party is subject to the oversight and supervision of a competent authority and that it has applied policies and procedures to commit to the due diligence requirements including the requirements regarding the customer identification, and keeping records and AML/ CFT programs stipulated herein.
   c. The company must take adequate steps to ensure that the copies of the documents to identify the identity of the customer and other documents required for due diligence towards customers will be presented by the third party once requested and without any delay.
   d. The relationship between the company and the third party should be governed pursuant to an agreement that identifies the duties and responsibilities of each party.
2. The final responsibility for meeting the CCD measures remains with the company not the third party.
3. The company can rely on third parties from the same financial group in order to implement the due diligence procedures towards customers either by completing the necessary data or verifying the provided data, on the condition that the financial group applies CDD procedures, including risk- exposed persons, and keeping records as well as AML/CFT programs in line with the relevant content herein. The implementation of these requirements should be supervised by competent supervisory authorities in the parent country as well as the host country.
4. The company must take into account the level of risk assessment for the country where the member financial institution or the third party outside the financial group is located, as enhanced due diligence procedures shall be implemented in case it was a high- risk country, in addition to sufficiently mitigating any high risks of countries through the financial group's policies related to AML/ CFT.

Article (6): Customer and beneficial owner identification and verification procedures

A) The company must put in place the necessary systems that identify and verify the customer's identity in accordance with the requirements stipulated in Article (5) of these instructions.

B) The company must review the original official documents to identify customer's identity and keep a copy of same documents signed by the company's competent person, stating that it is an exact copy of the original.

C) The company must take the necessary steps to verify the data obtained from the customer by referring to reliable and impartial sources. This includes– whenever possible– contacting the competent authorities that issued those official documents, and checking available electronic sources, such as the websites of the Companies Control Department, the Ministry of Industry, Trade and Supply as well as the websites of authorities issuing these documents and certificates. The following shall be taken into account in customer identification for natural persons procedures:

1. The identification data of the customer must include: the full name, date and place of birth, the national number and all information related to the identity document for Jordanians, the passport number and the personal number for non-Jordanians, the nationality, and the residence permit issued by the Ministry of Interior or a valid work permit issued by the competent authority in case the customer was an expatriate worker, the nature of his work, his permanent residence address, his phone numbers, purpose of the business relationship and its nature and any other information that the company deems necessary to complete the customer identification procedure.
2. Obtaining the original official documents or a duly certified copy that proves the authenticity of the delegation in case there was a person or entity dealing with the company on behalf of the customer with keeping a copy of these documents. It is also necessary to identify the customer and his delegate and verify their identities according to the customer identification and verification procedures.
3. Obtaining a pledge from the customer to update his data as soon as any changes occur or upon the company's request.
4. In case a person deals with the company on behalf of the customer, it must be ensured that there is a valid power of attorney or authorization approved by the company, with the necessity to keep the power of attorney or a certified copy or the authorization in accordance with Clause (B) of this article, in addition to the need to identify the delegate according to the customer identification procedures as stipulated in Clause (C) of this article.

D) The following shall be taken into account when identifying the legal person or arrangement:

1. The identification data shall include the name of the legal person or arrangement, the legal form, the purpose and nature of the business relationship and the type of the activity, the date of registration and its number, the national number of the facility and its tax number, the names of the owners and their addresses, ownership shares, names of the persons occupying senior management positions, head office address and phone number, names of authorized signatories, as well as their nationalities, phone numbers, and any other information or documents that the company deems necessary to complete the identification process. All of which shall be kept constantly updated.
2. Obtaining official documents or duly certified copies thereof that prove the establishment of the legal person or arrangement and its legal entity as well as the names of the owners and those authorized to sign. This can be done by verifying their registration at the competent authorities and the documents and information necessary to prove this, such as the memorandum of association, the articles of association and certificates issued by the Ministry of Industry, Trade and Supply, and the Companies Control Department and the certificates issued by the chambers of commerce and industry, in addition to the need to obtain an official certificate issued by the competent authorities in case the legal person or arrangement is registered abroad.
3. Obtaining documents indicating the existence of an authorization from the legal person or arrangement to the natural persons representing them and the nature of their relationship, in addition to the need of identification of the person authorized to deal according to the identification procedures for natural persons stipulated in these instructions and verifying that there is no legal impediment to dealing with them and obtaining samples of their signatures.
4. Obtaining information regarding the provisions that regulate the business of the legal person or arrangement, which includes the ownership structure, the controlling management, and the provisions that regulate the powers of making binding decisions on the legal person or arrangement. Public shareholding companies are excluded from the request for data related to the names and addresses of the owners and the equity shares of the shareholders whose contribution is less than 10% of the company's capital with obtaining a pledge from the authorized signatories to provide the company with the data of any shareholders whose contribution falls within this percentage.
5. The following shall be taken into account in the identification of the legal arrangement:
    a. The company must be aware of the customer’s nature, ownership structure and board of trustees.
    b. The necessity to identify the authorized signatories and the controlling persons according to the procedures of the customer identification as stipulated in these instructions.

E) The following shall be taken into account in the identification procedures of the non-profit organization:

1. The identification data shall include: the name of the non- profit organization, the legal form, the national number of the organization (if available), the address of the headquarters, type of activity, date of establishment, the names and nationalities of those authorized to use the account, the phone numbers, the purpose of the transaction, the sources of income or financing, the names of the concerned persons who occupy the senior management positions of the non-profit organization and any other information that the company deems necessary to obtain.
2. Obtaining documents that prove the existence of an authorization from the non-profit organization to the natural persons authorized to use the account, in addition to the need to identify the identity of the authorized customer's delegate in accordance with the identification procedures as stipulated in clause (C) of this Article.

F) The following shall be taken into account in the identification procedures of the beneficial owner:

1. The company must request from each customer a written declaration in which he/ she specifies the identity of the beneficial owner of the business transaction to be performed (in cases requiring that) so that the declaration includes at least the customer's identification information.
2. The company must identify the beneficial owner and take reasonable measures to verify this identity according to the customer's level of risk, and this includes relying on data or information obtained from official documents and data, so that the company is sure that it knows the identity of the beneficial owner.

G) The following shall be taken into account in the identification of the beneficial owner in the case of legal person:

1. The identity of the natural person(s) – if available – and who has (have) an equity share that actually controls the legal person.
2. In case there is any doubt about the identification of a natural person or in case of inability to identify him in accordance with Clause (1) above, the company must identify the natural person who has control within the legal person through other means.
3. In case that no natural person is identified within the framework of applying the Clauses (1) and (2) mentioned above, the company must identify and take reasonable measures to verify the identity of the relevant natural person who occupies the position of a high administrative official within the legal person.

H) The following shall be taken into account in the identification of the beneficial owner in case the customer is a legal arrangement:

1. Express trust: identifying the testator, the trustee, or custodian (as relevant) and the beneficiaries or category of beneficiaries for every other natural person who exercises effective and actual control over the fund.
2. Other types of legal arrangements: identification of the persons who occupy positions equivalent to the above- mentioned or similar.

Article (7): Simplified Due Diligence procedures:

A) The Central Bank, pursuant to the orders it issues, has the right to decide the cases, or the transactions whose implementation requires, or the customers requiring Simplified Due Diligence measures when determining and verifying the identity of the customer and the beneficial owner. These orders identify examples of low- risk customers or transactions, in addition to any international controls or domestic requirements in this regard.

B) Simplified Due Diligence measures must not be undertaken if money laundering or terrorism financing transactions are suspected or if there are high-risk circumstances.

Article (8): Enhanced Due Diligence procedures:

A) The company must undertake enhanced due diligence measures when the customer risk for money laundering and terrorism financing is categorized as 'high'. This must be done as follows:

1. Obtaining the approval of the general manager/ regional manager of the company or whomever he/ she delegates from the senior executive management before establishing or continuing the relationship with these customers. It is also necessary to obtain this approval when discovering that any of the customers or the beneficial owners fall into this risk category.
2. Taking adequate measures to ascertain the sources of funds for customers and beneficial owners who are classified under this risk category.
3. Following- up these customers' transactions with the company in an accurate and continuous manner, and implementing enhanced due diligence to the business relationships and transactions that take place with any of them, while continuing to take enhanced due diligence measures and monitoring those relationships.
4. Taking the necessary measures to identify the background of the circumstances surrounding any of the business relationships and transactions that take place with any of the customers classified within this category and their purposes in case that the company finds that any of them is not based on clear economic justifications. The company shall take a decision regarding them while keeping the results in its records.

B) Situations that require enhanced due diligence:

1. **Foreign Politically Exposed Persons**:
   a. The company must put in place an appropriate risk management system to identify whether any of its customers or beneficial owners fall into this category.
   b. In case that any of the customers or beneficial owners are identified within this category, the company must undertake the enhanced due diligence measures as described in Article (8/a) above.

2. **Domestic Politically Exposed Persons**:
   a. The company must take reasonable measures to identify whether the customer or the beneficial owner falls into this category.
   b. In case that any of the customers or beneficial owners are identified within this category, the company must assess the level of money laundering and terrorism financing risks involved in the business relationship with this customer.
   c. In case the company evaluates the customer's risks as being high, the company must undertake the enhanced due diligence measures as described in Article (8/a) above. It is sufficient for the company to undertake due diligence measures when the assessed risk level is below that.

The company must apply the requirements mentioned in Clauses (1) and (2) above on the family members of or persons close to the politically exposed persons.

3. **Non face-to-face financial transactions especially those that take place using new technological means such as the Internet or via electronic payment methods. In these cases, the company must do the following**:
   a. Identify money laundering and terrorism financing risks associated with developing new products and new business practices, including new means of providing services, and those arising from the use of new or under- development technologies in relation to all new and existing products.
   b. undertake the risk assessments prior to the launch or use of such products, practices and technologies
   c. take appropriate measures to manage and mitigate the risks

4. Unusual transactions:

   a. The following are considered an unusual transaction:

      1. Transactions that are large or complex to an unusual degree compared to the customer's transactions and activity, or several low-value transactions that appear interconnected with each other, so that in their entirety they form one transaction of an unusual pattern.

      2. Any other unusual transaction that does not seem to have a clear economic justification or is inconsistent with the nature of the customer's risk and his/ her activity.

   b. The company has to undertake enhanced due diligence with regard to unusual transactions, and when doubting the validity or accuracy of the customer identification data after establishing the business relationship by conducting the necessary analysis and studies and any other procedures necessary to verify the source of the funds and the nature of the transactions with the need to keep special records for that regardless of the decision taken in their regard. The company's policy for compliance and/ or work procedures must include examples on additional requirements needed to conduct enhanced due diligence in such transactions.

5. Other cases:

The company must also exert enhanced due diligence in the following cases, in proportion to the level of risks:

a. Having doubts about the correctness or accuracy of the identification data of the customer or the beneficial owner after establishing the business relationship.
b. When paying cash amounts or cheques in an existing loan/ financing account by a person(s) who does (do) not represent the account holder according to a legal power of attorney or authorization approved by the company.
c. When conducting transactions for non- resident customers.
d. Cases in which the company identifies the customer's risk as high, and as indicated in the guidance manual [Annex no.(1)]
e. Business relationship or transactions carried out by natural or legal persons from countries that are classified as high risk and/ or do not apply the recommendations of the Financial Action Task Force (FATF).

Article (9): The financial group, its branches and subsidiaries abroad

A) In the case that the company is part of a financial group, the group should be required to implement anti- money laundering and countering terrorism financing programs at the group level, which should apply as appropriate to all branches and subsidiary companies in which the group owns a majority, provided that these programs include the following measures:
   1. Preparing appropriate policies, procedures, internal controls and arrangements with respect to the following:
      a. Compliance oversight management (including the appointment of a compliance oversight manager at the managerial level).
      b. Appropriate screening procedures to ensure high standards when hiring employees
   2. Putting an ongoing employee training programme.
   3. Creating an independent audit unit to test the system
   4. Establishing policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management.
   5. Providing information related to customers and transactions from branches and subsidiaries to the group-wide compliance monitoring, auditing and/ or anti money laundering and countering terrorism financing, which might include information analyzing unusual transactions or activities. It may also include that a report has been sent to the Unit regarding the transactions when it is necessary for the purposes of anti- money laundering and countering terrorism financing and for risk management purposes.
   6. Adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

B) If the host country does not allow adequate implementation of special measures to Anti money laundering and terrorism financing in line with the kingdom's procedures, the financial group should apply appropriate additional measures to manage money laundering and terrorism financing risks and inform the Central Bank of that.

Article (10): Internal System

The company must establish an appropriate internal system that includes adequate and effective internal policies, controls and procedures based on the company's understanding of the risks of money laundering and terrorism financing, provided that the system includes the following:

A) A clear policy for AML/ CFT approved by the board of directors or the regional manager of branches of foreign companies, with constant updating, so that this policy includes all requirements mentioned in these instructions as a minimum.
B) Detailed written procedures for AML/ CFT, taking into account the precise definition of duties and responsibilities in accordance with the approved policy and instructions issued by the Central Bank in this regard.
C) Allocation of an independent qualified and resourced staff within the internal audit department to test compliance with policies, internal controls, and procedures for anti-money laundering and terrorism financing.
D) An appropriate mechanism to verify compliance with the instructions, policies and procedures established to anti-money laundering and terrorism financing by the internal audit and the reporting officer, taking into account the coordination in the area of determining powers and responsibilities between them.
E) Establishing procedures that ensure that the internal control unit performs its role of examining internal control and oversight systems to ensure consequently their effectiveness in AML/ CFT with the necessity of reviewing them periodically to complete any deficiency or updating and developing them to increase their efficiency and effectiveness.

Article (11): Training and Qualification

A) The company must set up continuous training plans and programs in the field of AML CFT for the company's workers, provided that these programs include methods of money laundering and terrorism financing, how to discover and report them, and how to deal with suspected customers. Records for all trainings that have taken place during a period of no less than five years shall be maintained and should include: the names of the trainees, their job titles, and the entity that conducted the training, whether inside or outside the Kingdom. All new employees shall be subjected to training courses in the field of AML/ CFT during the first year of their employment.
B) The company must adopt policies, procedures, and controls to ensure the highest standards when hiring employees, in order to verify the suitability of senior executive management and reporting officer and other employees involved in AML/ CFT.

C) Allocating an independent budget approved by the board of directors of the company or the regional management of the foreign company providing the funding necessary to train and qualify and attend seminars and workshops related to AML/ CFT for the company's workers, and to provide systems that help the compliance oversight department to carry out its tasks. The Central Bank shall be provided at the end of each year with a statistic showing training programs and workshops in which the employees have participated during the year.

D) Keeping records of training programs and all related data for at least (5) years from the date of training.

E) The company must provide its employees with the necessary information about:
   1. The law in force, the bylaws, and instructions as well as the decisions issued pursuant to any of them.
   2. The patterns that are suspected of falling within the money laundering and terrorism financing transactions mentioned in the Guideline for Indicators of Suspicion of Money laundering and Terrorism Financing transactions [Annex (2)], and the use of these indicators as a tool to educate the company's employees and take them into account in cases of suspicion.
   3. Procedures for informing the reporting officer about transactions that the employee suspects to be related to money laundering or terrorism financing.
   4. Policies, internal controls, and procedures followed by the company to anti money laundering and terrorism financing, according to the degree of risk.

Article (12): Reporting about transactions suspected of being related to money laundering or terrorism financing:

A) The company must specify the name of the reporting officer and his/ her deputy and inform the Unit and the Central Bank in the event that any of them is changed, provided that each of them has the appropriate qualifications.

B) The authorities of the reporting officer shall be determined to include at least what enables him/ her to independently carry out his/ her responsibilities and in a manner that ensures preservation of the confidentiality of the information received by him/ her and the procedures that he/ she performs. For this purpose, he/ she shall have access to the records and data required for him/ her to carry out his/ her work. These authorities shall include the following:
   1. Receiving information and reports on unusual transactions or those suspected of being related to money laundering or terrorism financing, examining them, and taking the appropriate decision regarding reporting to the Unit immediately or keeping them, provided that the decision to keep them is justified and that the necessary documents are kept for a period of no less than (5) years.
   2. Preparing periodic statistical reports to be submitted to the board of directors on transactions suspected of being linked to money laundering or terrorism financing.

C) If any of the company's employees suspects that a transaction in progress is related to money laundering and terrorism financing, he/ she must report to the reporting officer.

D) reporting officer must immediately report to the Unit all transactions that he/ she suspects or has a reasonable grounds to suspect as being related to money laundering or terrorism financing whether these transactions are executed or not and regardless of the value of this transaction, using the tool or form approved by the Unit.

E) The reporting officer shall provide the Unit and the competent authorities with data related to transactions suspected of being interconnected to money laundering or terrorism financing and with any other information or data requested from him/ her in accordance with the method approved by these authorities and facilitate their access to relevant records and information for the purposes of carrying out their duties.

F) It is prohibited for any employee to disclose directly or indirectly, or by any means whatsoever, about any reporting process to the Unit or to any other official authorities regarding transactions or any reporting procedures undertaken in regard to transactions suspected of being related to money laundering or terrorism financing or any information related to them.

G) It is prohibited for anyone who comes across or knows directly or indirectly, or by virtue of his/ her position or work, to divulge any information that has been presented, exchanged, or disclosed in any way, except for the purposes of implementing the law and these instructions.

Article (13): Keeping Records and Documents

Every company must develop an integrated information system to keep the records, documents and information referred to below, in order to make all records related to customers and transactions available upon request from the Unit and the competent official authorities in an integrated and fast manner within the specified period for that.. The transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

A) The system shall include the following:
   1. Records and documents related to business relationship and domestic and international transactions including those related to the due and enhanced diligence requirements stipulated in these instructions.
   2. Records of suspected transactions, provided that they include copies of reports of transactions sent to the Unit and the data and documents related to them.
   3. Reports of unusual transactions and the evidence of reviewing these reports.
   4. Records and documents supporting business relationships, transactions, correspondence, and results of any analysis performed.

B) The aforementioned records must include original documents, hard copies, scanned copies and stored copies, or any other form that is accepted by courts under the legislation in force in the Kingdom.

C) The company must keep records and documents in a secure manner and keep backup copies of them elsewhere.

D) The records and documents indicated above shall be kept for a period of at least five years from the date of the completion of the transaction or the termination of the relationship as necessary including the date of termination of the occasional operation.
E) The company must prepare special files for transactions suspected of being linked to money laundering and terrorism financing in which copies of reports, data and documents related to them are kept. These files shall be kept for a period of no less than 5 years from the date of reporting or until a final court decision is issued regarding these operations whichever is longer.

Article (14): Taking into consideration the provisions of the instructions issued pursuant to the provisions of the law, the company must implement the obligations contained in the relevant and enforceable international decisions, including all the decisions issued under chapter (7) of the United Nations Charter without delay.

Article (15): Concluding Provisions

A) The company must include in the agreement signed between it and the legal accountant what obliges them to ensure that the company applies the law and these instructions, to examine the adequacy of the company's policies and the related procedures, and to include the results in their report submitted to the management with the need to inform the Central Bank immediately upon discovering any violation of these instructions.
B) It is prohibited for any employee to manage any proxy accounts for any customer, except for the spouse or first- degree relatives, after obtaining the approval of the General Manager/ the Regional Manager.
C) Considering the provisions and requirements of the law and other instructions issued by the Central Bank, companies operating in the Kingdom must provide the Central Bank with all reports issued by internal and external supervisory authorities if they include references to violations or observations related to AML/ CFT measures.
D) Companies operating in the Kingdom must provide the AML/CFT Unit within the specified period with any additional information, reports or statistics that it requires for the purpose of implementing the provisions of the law and the regulations and instructions issued pursuant thereto.
E) The company should be guided by the methodology issued by the Financial Action Task Force (FATF) regarding the application of the methodology for evaluating technical compliance with the recommendations of the FATF and the effectiveness of AML/CFT systems, and any matters not mentioned in these instructions.
F) The company shall adopt the following policies to limit money laundering and terrorism financing transactions:
    1. Know Your Customer (KYC) policy
    2. Anti- money laundering and countering terrorism financing policies and procedures used to identify the true identity of the customer and the beneficial owner, and the acceptable type of activity and to detect the unusual activity of the customer.

Article (16): Anyone who violates the provisions of these instructions shall be punished by the sanctions stipulated in the law and/ or the by-law, while not breaching any more strict punishment stipulated herein.

Article (17): The attached guidance manuals shall be considered an integral part of these instructions.

Governor

Dr. Ziad Fariz

Annexes:

- Annex (1): The Guidance Manual for the cases where the company's assessment for Money Laundering and Terrorism financing Risks is high (as a minimum)
- Annex (2): Guideline for Indicators of Suspicion of Money Laundering and Terrorism Financing Transactions.

Annex (1) The Guidance Manual for the cases where the company's assessment for Money Laundering and Terrorism financing Risks is high (as a minimum)	
Factors	**Cases**
Factors related to customer risks	- Doing business in unusual circumstances (e.g. big and unjustified geographical distance between the company and the customer) - Non- resident customers - Cases where the legal customer or legal arrangement is a special purpose facility - An unjustified complexity in the ownership structure compared to the nature of the company's business - Customers from regions known to have a high crime rate (e.g. countries known for producing, transporting, or smuggling Narcotic Drugs) - Customers who belong to or are located in countries that do not apply the recommendations of the Financial Action Task Force (FATF) or do not adequately implement them. - Business classified by the Financial Action Task Force (FATF) as "high risk" in money laundering and terrorism financing - Customers who meet the risk indicators specified by the company
Factors related to country and geographic regions risks	- Countries that lack adequate systems in AML/ CFT or do not adequately implement the FATF recommendations. - Countries subject to sanctions, embargoes, or any other measures issued by the United Nations. - Countries with high levels of corruption or other criminal activity. - Geographical areas designated as financing terrorism or supporting terrorist activities. - Countries where terrorist organizations are located. - Countries experiencing political or security conditions that impede their compliance with FATF recommendations. - When identifying risk factors for countries and geographical regions, the company can refer to credible sources such as: mutual evaluation reports, follow-up reports, and any other related reports published by international organizations such as: the United Nations and the Financial Action Task Force (FATF).
Factors related to the risks of products, services, processes or distribution channels	- Transactions carried out by unidentified persons (in which cash may be used). - Non face-to-face business relationships or transactions - Payments made on the customer's account from unknown sources or from a third party with which the customer has no clear relationship.

Annex (2):

Guideline for Indicators of Suspicion of Money Laundering and Terrorism financing Transactions

First: Customer's Behavior

a. The customer whose mood is volatile and who refuses to provide the company with the necessary identification documents and to provide any detailed information about himself/ herself that are among the conditions for completing the transaction.

b. The customer who shows dissatisfaction and unwillingness to complete the procedures of the process to be performed when he/ she knows that it requires informing the concerned authorities of its details.

c. The customer who inquiries from the company about the company's records, systems and instructions, with the aim of obtaining sufficient information about money laundering transactions and avoiding legal violations regarding them.

d. The customer provided false or misleading information that is difficult for the company to verify, for example providing an unreachable telephone number.

e. The customer offers unjustified gifts or bribes to company employees and attempts to persuade the employee not to verify identity documents and other documents.

f. The suspected customer or his representative requests the cancellation of the transaction once the company employee tries to obtain the missing important information.

g. The customer is controlled by another person upon his/ her presence in the company, and the customer is unaware of what he/ she is doing or he/ she is old and is accompanied when a transaction is executed by another person who has no connection with him/ her.

h. The customer who presents suspicious or forged personal identification documents and refuses to provide the company with his personal information.

i. The customer who provides the company with a permanent address for him located outside the company's service area or outside the kingdom.

j. The customer whose home, work or mobile number is out of services or disconnected.

k. The customer who refuses to disclose the details of the activities related to his work.

l. The customer frequently changes his/ her residential address.

m. The beneficial owner belongs to a region known to have criminal activity or security disturbances.

n. The company employee knows that the customer has criminal precedents, or, from reliable sources such as (the media), that the customer is involved in illegal activities.

o. The customer or his representative shows signs of anxiety or confusion during the implementation of the transaction.

p. The customer attempts to cancel the transaction after being informed that the information provided by him/ her will be verified, or shows dissatisfaction with the procedures and systems used by the company.

q. The customer avoids (fears) to meet the company's employee face-to-face and resorting to the use of alternative methods.

r. The customer or his/ her representative unexpectedly provides an early settlement of debts before the specified time and without a reasonable explanation of the source of payment.

s. The customer's nationality and profession do not match his/ her name, appearance or beliefs.

t. The customer suddenly pays a large debt without a clear and reasonable explanation of the source of payment.

u. The level of customer's activity to be funded does not match the known level of the customer.

v. The loan is paid by another loan obtained by a bank, company, or any party that is not related to the customer.

Second: Employee's Behavior

a. Significant and sudden increase in the employee's standard of living and the level of his spending, which is not commensurate with his monthly salary and without a clear justification.

b. The employee' do not provide the company with a non-conviction certificate issued by the Ministry of Justice.

c. The employee' do not take his/ her annual leave or frequent visits to the company during his/ her leave.

d. The employee's assistance in carrying out transactions characterized by the fact that the beneficial owner or the counterparty is not fully known.

e. The employee frequently bypasses supervisory procedures and follows the evasive policy while performing his/ her work.

f. The employee assists in completing transactions where the customer is not fully known.

g. The employee exaggerates in the credibility and ethics of the customer and his/ her financial sources and solvency.

h. The employee involves in a large number of exceptions related to processing the transactions.

i. The employee exploits the authorities granted to him/ her or to his/ her position in order to carry out transactions that do not comply with the Code of Conduct.