Pursuant to provisions of Article 10, Fourth of the Anti-Money Laundering and Counter-Terrorism Financing Law No. 39 of 2015, the following Instructions no. (1) of 2016 on

Customer Due Diligence are issued:

Article 1:

Definitions and terms used in these instructions

First: Customer Due Diligence (CDD):

CDD includes identifying the customer, determining the legal status of the customer, the activity and the purpose and nature of their business relationship with the financial institution in addition to verifying such, pursuant to the obligations set out in the Law and these Instructions. It also includes identifying, and where required, verifying the beneficial owners of the business relationship. CDD further includes the ongoing monitoring of the customer's transactions carried out as part of an ongoing business relationship.

Second: The high- risks officials: shall include any natural person, whether as customer or beneficial owner, who is or was entrusted with a prominent public function in the State of Iraq or in a foreign country, such as Head of States or of governments, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials; or entrusted with a prominent function by an international organization, such as directors, deputy directors and members of the board. The term also includes immediate family members and close associates. Close associates includes widely and publicly known close business colleagues or personal advisors or any persons who are in position to benefit significantly from close business associations with the high-level officials, and their relatives of the second degree.

Third: Non-profit organization: any legal person established according to the law that has main purpose is to provide social and voluntary services without seeking to profit or personal interest and it includes the local and foreign organizations.

Fourth: Promptly/immediately: through hours without exceeding a one-working day.

Fifth: Reporting official: the head of department mentioned in the article (14) of the AML&CFT law 39 of the year 2015, and this official will be appointed by the main administration for the purpose of reporting on suspicious transactions that may be involved in money laundering and financing the terrorism activities.

Sixth: Financial group: it is a company, or any other kind of the natural or legal persons who own the controlling stakes and coordinate the tasks with other

members of the group in order to conduct and implement supervision on the group in accordance with the basic principles alongside the branches and subsidiary companies that subject to the policies and procedures of AML&CFT applied within same group.

Seventh: Intermediary institution: is the financial institution that proceeds or covers the payment through receiving and sending the funds of wire transfers on behalf of the originating financial institutions, and receiving financial institutions, or on behalf of another intermediary financial institution.

Eighth: Sending\ originating financial institutions: is the financial institution that sends funds of a wire transfer after receiving a request for conducting a wire transfer order.

Ninth: Receiving financial institution: is the financial institution that receives the funds of a wire transfer from an originating financial institutions, directly or via an intermediary financial institution, and providing that funds to the beneficially.

Article 2

The financial institutions shall implement the rules of CDD as the following:

First-

a- Financial institutions shall not open or maintain anonymous accounts or accounts under fictitious names, or numbered accounts, or provide any services for such accounts. Customer due diligence measures shall be applied to account-holders or beneficial owners of existing anonymous accounts or accounts under fictitious names, or numbered accounts as soon as possible and in any event before such an account may be used in any way.

b- Identify and verify the customer and beneficial owner using reliable, independent source documents, data or information in line with the stipulations of the present instructions for each category.

c- Understand the purpose and intended nature of the business relationship and request additional information in that regard, when necessary.

d- Monitor the business relationship on an ongoing basis using automatic systems to monitor the relationship with the customer and identify their transaction pattern and detect any transactions that are inconsistent with the institution's knowledge of the customer, commercial activities and risk profile, including identifying their source of funds for any customer classed as high-risk.

e- The institution shall carry out CDD procedures itself, and shall not rely on any third party to carry out these procedures.

Second: Financial institutions shall apply all CDD measures stipulated in paragraph 1 of this Article that provided they define the scope of such procedures according to the risk-based approach.

Third: Financial institutions shall implement the Customer Due Diligence (CDD) measures regarding the states mentioned in paragraph (1) of the article (10) of the AML&CFT Law.

Fourth: By exception, the verification procedures may be implemented later, but as soon as possible after the establishment of the business relationship in the following circumstances:

a. Postponing verification procedures is essential in order not to interrupt the normal conduct of business.
b. The institution completes due diligence procedures pursuant to the obligations of the AML&CFT Law and this Instruction as soon as possible after the establishment of the business relationship.
c. The institution has taken the necessary measures in assessing the ML/FT risk for the case in which the delay was applied, including a limit on the number, type and value of transactions that can be executed before the completion of the verification procedures.

Fifth: If the financial institution is unable to comply fully with the CDD obligations of the Law or this Instruction, it shall not open an account or establish any business relationship with the customer or perform any transaction to his/her account. It also must terminate the business relationship for existing relationships and report such customer to the Office.

Sixth: In cases where the financial institution forms a suspicion of money laundering or financing of terrorism, and it reasonably believes that carrying out CDD procedures may tip-off the customer, it is permitted not to pursue the CDD process, and instead file a suspicious transaction report with the Office.

Seventh: The financial institution shall apply, the basis of materiality and risk, CDD procedures to customer-relationships that existing before the entry into force of the AML Law, and shall conduct CDD on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

Eighth: Institutions must ensure that the customer is not designated on any barred persons lists pursuant to Article 12, Third of the Law before entering into an ongoing business relationship with such customer. They shall also refrain from carrying out any transaction with a customer with whom it is not in an established business relationship designated on such lists.

Ninth: Institutions shall rely on official identification documents to identify the customer (or customers for joint accounts), verify their veracity and validity and keep a copy of these documents signed by the competent employee stating that these are a true copy. If there is doubt regarding the validity of these documents, the financial institution shall verify the validity of the data and information obtained from the customer by

contacting competent authorities that issue such official documents evidencing the information.

Article 3.

Procedures are to be implemented by the financial institution to identify and verify the identity of a natural person:

First: The financial institution shall verify the identity of the natural person using valid official documents (national identity card, driver's license, residency papers, passport or travel document), ensuring that the identification data includes the full name of the customer, their nationality, date of birth, address of permanent residence, phone numbers, work address, type of activity, purpose of the business relationship, names of persons authorized or commissioned to deal with the account and their data, and any other information the financial institution deems necessary to obtain.

Second: In the case of persons with limited or no legal capacities such as minors, the financial institution shall obtain documents pertaining to them and their legal representatives dealing with such accounts.

Third: In case another person deals with the financial institution on behalf of the customer, it shall ensure the presence of a power of attorney allowing them to do so, and keep an original or authenticated copy of it. The institution shall also identify and verify the identity of such person according to procedures specified in the AML&CFT Law and these instructions.

Article 4.

Procedures to identify and verify the identity of a legal person:

First: Identification data of a legal person includes: the name of the legal person, the legal form, the headquarters address, type of activity, capital, the names of persons authorized or commissioned to manage the account and their nationalities and phone numbers, the purpose of the business relationship, and any other information the institution deems necessary to obtain. The institution shall verify the identity of the legal person and obtain official documents validating its existence.

Second:

a- For business relationships with legal persons, the institutions must verify the existence of the legal person of the company through the appropriate documents and the information contained therein as follow:

- Certificate of registration of the company at the Commercial Registrar and a certificate of business commencement for public shareholding companies.
- Memorandum and Articles of Association.
- The company's address and headquarters.
- The decision of the Director or Board of Directors to open an account at the institution.
- Company's accounts

- The decision of the Director or Board of Directors to appoint authorized persons to manage the company's accounts and limits of their powers.

b- Verifying the existence legal person of the Government units, and public establishments and institutions through implementing the mentioned below procedures:

- The approval of the competent authority to which the government unit is affiliated or of the Director General of the establishment or institution, as the case may be, to open the account.
- Mandate specifying the names of persons authorized to sign on the account and the limits of their powers signed by the head of the government unit or the Director General, as the case may be.

Third: Financial institutions shall obtain copies of documents proving the authorization from the legal person to a person representing them or of documents establishing the commissioning of natural persons to manage the account. In addition the financial institution shall identify such authorized persons in accordance with the customer identification procedures stipulated in the present Instructions.

Four: Mixed joint-stock companies shall be exempted from the requirement to provide information on names of owners and ownership shares. It is only required to obtain information on the names of shareholders whose share exceeds 10% of the company's capital.

Article 5.

Non-profit organizations and associations

The financial institutions will take the below- mentioned procedures to verify the identity of non-profit organizations and associations:

First: Identification data of a non- profit organization includes: the name of the organization, the legal form, the headquarters address, type of activity, capital, the names of persons authorized or commissioned to manage the account and their nationalities and phone numbers, the purpose of the business relationship, the records of board election or appointment, and any other information the institution deems necessary to obtain.

Second: The institutions must verify the existence of the non-profit organization in as well as through the appropriate documents, the Certificate of registration of the organization from the competent authority, Memorandum and Articles of Association.

Third: A letter specifying the bank in which the checking account is to be opened signed by the head or his deputy and including the names of the persons authorized to sign on behalf of the relevant party and the limits of their powers to use that account.

Fourth: Financial institutions shall obtain copies of documents proving the authorization from the organization or association to a person representing them or of documents establishing the commissioning of natural persons to manage the account. In addition the financial institution shall identify such

authorized persons in accordance with the customer identification procedures stipulated in the present Instructions.

Fifth: obtaining the identity's data of the donors and the beneficiary of the funds deposited or\and withdrawn.

Article 6.

Procedures related to a trust or legal arrangement

Financial institutions shall obtain the following information as a part of the identification measures regarding a trust or legal arrangement:

First- Name, legal form and proof of existence of the trust or legal arrangement, the trust deed or other document containing the powers that regulate and bind the trust or legal arrangement.

Second- Names of all trustees, mailing address of the trustee(s), Contact telephone number and other contact details of the trustee(s), as applicable, Description of the purpose/activities of the trust or legal arrangement.

Third- Intended purpose and nature of the business relationship.

Fourth- Signature of the trustee(s).

Article 7.

The main procedure for verifying the Beneficial Owner Identification:

First-The financial institution shall request each customer when opening an account or commencing a business relationship to sign an affidavit which identifies the beneficial owner of the intended relationship. Such affidavit shall include at minimum customer identification information.

Second- The financial institution shall identify beneficial owners, and take reasonable steps to verify their identity, based on documents, data or information obtained from reliable and independent sources, in a manner to allow the institution to be satisfied that it has identified the beneficial owner.

Third- for identifying the beneficial owner of legal persons and legal arrangements, reasonable steps should be taken to understand the ownership and control structure of the legal person or legal arrangement.

Article 8.

Actions to be taken concerning AML/CFT Risk Management System

In implementing the AML/CFT program, the requirements for which are set out in this Instruction, financial institutions shall establish an AML/CFT Risk Management System that includes:

First:

a - Determining risk categories for customers on the basis of risk level and materiality, and setting necessary procedures to deal with such risks. Customers shall be divided into the following categories:

1- High-risk customers, to whom, in addition to the CDD measures to be applied under Article 10 of this instructions in addition to Article 10 of the

AML&CFT Law no. 39 of year 2015, this Instruction shall be applied, on the basis of risk level and materiality.

2- Medium-risk customers, to whom standard CDD measures shall be implemented, pursuant to Article 10 of the Law, and

3- Low-risk customers, to whom a simplified version of the standard CDD measures may be applied if the financial institution so decides, on the basis of risk level and materiality.

b -The financial institution should review the risk categorization of its customers at least once every year or whenever there are changes during the year requiring such review. Changes include the repeated appearance of the customer's name in STRs or reporting any suspicious transaction linked to the customer to the Office.

Second- Financial institutions shall also ensure that their AML/CFT risk management system includes policies and procedures based on identifying, assessing, monitoring and reporting risks and that it takes into consideration all types of risks including at a minimum:

a- **Risks related to products and services:**

Those can be exploited for money laundering or terrorism financing, such as the following:

1- Products and services include new or inventive Products or Services that are identified by the Central Bank of Iraq and\ or the Office as high risk products or services.

2- Services Products or services that do not allow the disclosure of most required information concerning the identity of its users or those of an international nature such as internet banking services and stored-value cards.

3- Business relationships conducted other than face-to-face.

4- Private banking services.

b- **Customer Risks:**

These risks related to customers or their dealings with the financial institutions, or with the sectors to which they belonged, so when the financial institution identifying these risks, it should rely on information obtained through verifying the identification documents and the public information known or available to the financial institution, and as well as through the activity nature of customer's transactions, the financial institution should follow the below-mentioned issues when seeking to identify these risks:

1- The risks related to customers:

First: Difficulties to identify the beneficial owner, of customer's transactions for example due to the complexity of the ownership structure of legal persons or legal arrangements.

Second: Customers with tainted reputations or previous suspicious dealings.

Third: Non-resident customers.

Four: High-level officials with risks, their close associates and close family members.

2-The risks related to customer's transactions include but not limited to:

First- Transactions that do not correspond to the declared purpose of the business relationship

Second-Services required by the customer do not correspond to the nature of their activity.

Three-Carrying out complex or large transactions with no clear justification

Four- Dealing with a branch of the institution located far from the customer's place of residence of work with no clear justification

Five- Customers having numerous or diverse accounts at the same financial institution or in more than one institution in the same area with no clear justification

Sixth- Customers that suddenly change their transaction pattern with the financial institution with no clear justification.

Seven- Customers reportedly involved in illegitimate activities

Eighth-The unjustified use of brokers to carry out transactions

Ninth- Customers overly requesting confidentiality to be respected for certain transactions.

Tenth-Indirect transactions and those carried out using the latest technologies .

3-**Risks related to customer's activities**:

First-Cash-intensive activities including some activities linked to the provision of financial services such as remittance companies and foreign exchange institutions when not subject to the same high level of monitoring as the institution.

Second- Charities and other non-profit organizations.

Third- Dealers in precious metals and stones, antiquities and art work.

C-Geographic risks:

These include risks related to the country of nationality of the customer, their place of residence or work, or the source or destination of their transactions, in terms of the adequacy of AML/CFT systems in identifying risks of such country\countries, which include the following:

1- Countries that do not apply the recommendations of the Financial Action Task Force (FATF), and with no adequate AML/CFT laws and systems.
2- Countries subject to sanctions, embargos or similar measures issued by the United Nations.
3- Countries with a poor rating in terms of transparency.
4- Countries classified as providing funding or supporting the terrorism, or suffering from high levels of crimes such as drug or human trafficking.

Article 9.

The procedures of the simplified customer due diligence will be implemented as follows:

First: The financial institution may decide which transactions or customers are to be subject to simplified due diligence procedures, when verifying the identification documents of the customer and the beneficiary owner, and taking into account the international standards, recommendations and the best practices, that identify examples of low-risk customers or transactions, in addition to any international controls or domestic requirements issued in this regard.

Second: The procedures of the simplified due diligence shall not be applied in case of suspicion arising from transactions related to money laundering ,financing the terrorism, and high-risks circumstances**.**

Article 10

Enhanced due diligence for high-risk customers, services and transactions requiring special attention:

In addition to regular CDD measures, financial institutions shall apply Enhanced due diligence for high-risk customers, services and transactions, through taking into consideration the following procedures:

First-High-level officials with risks:

a. Financial institutions must take reasonable measures to determine whether or not a customer or beneficial owner is a High-level officials with risks.
b. The institution shall develop a risk management system for the High-level officials with risks or beneficial owners of High-level officials. This system shall include a determination of whether a future customer is High-level officials or not .
c. Senior management approval must be obtained before establishing a business relationship with such person and upon discovery that a customer or beneficial owner has become a High-level official with risks.
d. Financial institutions shall take adequate measures to identify the source of wealth and funds of any customer or beneficial owner who is a High-level officials with risks.
e. Financial institutions shall apply enhanced ongoing monitoring to their dealings with High-level officials.

Second: Unusual transactions:

Those represent large or complex transactions that do not correspond with the customer's account movements or activities, so Institutions should give special attention to unusual transactions, with the need to keep records for these transactions regardless of the decision taken in their regard. Financial institutions should examine, as far as reasonably possible, the background

and purpose of all such transactions and keep written records of these results for five years.

Third: Private banking services:

Financial institutions shall give special attention to customers benefiting from private banking services. The institution shall obtain senior management approval to provide such services to clients and apply identification procedures as well as due diligence based on the risk level of such customers. The institution shall take the following factors into account in assessing the customer's risk level:

a- The nature, activity and source of wealth of the customer.
b- The purpose of requesting the private banking service.
c- The relationship of the customer with the financial institution (its establishment and development).
d- The corporate structure of the customer using such services, where applicable.
e- Countries where the customer operates and the presence of AML regulations and controls in such countries.
f- General information available on the customer and his/her commercial reputation.

Fourth: Transactions involving persons in countries that do not or insufficiently apply FATF recommendations, so that the below-mentioned procedures should be followed:

a- Financial institutions shall give special attention to transactions carried out with persons from or present in countries that do not or insufficiently apply FATF recommendations. In cases where such transactions do not have an apparent economic purpose, financial institutions shall take necessary measures to examine the background and purpose of such transactions and keep written records of these results available to the Bank or the Office and to the financial institution's auditors.
b- In case of the country's continued failure to apply the FATF standard and continuing to apply them insufficiently according to the information available to the financial institution, the institution shall select from the following list of measures, on the basis of materiality and level of risk and apply the measures accordingly to persons from or present in such countries:

1- Continue to apply enhanced due diligence measures to such customers
2- Closely monitor and identify the purpose of transactions linked to such persons.
3- Send a statement of transactions linked to such persons to the Office.
4- End the business relationship or limit financial dealings with such customers in any case in which the financial institution is unable to implement effective due diligence measures.

c- Financial institutions shall give special attention to their branches and subsidiaries in countries that do not or insufficiently apply FATF recommendations.

Fifth: Non-resident customers:

This category includes non-resident customers whether natural or legal persons that do not have a permanent place of residence or business in Iraq. In case of opening an account for a non-resident customer, financial institutions must apply the following procedures:

a- In case of natural persons: after verification procedure of the visa validity, the financial institution should obtain a copy of visa through which that person entered the country.

b- In case of legal persons or legal arrangement, the institution is to apply the following procedures:

1- Obtain copies of documents, evidencing the establishment of legal person or legal arrangement, and authenticated by the embassy existing in the original country.

2- Obtain copies of official document, evidencing the registration of the legal person or legal arrangement, and authenticated by the competent authority of the original country.

3- Obtain the approval of the supervisory authority to which the legal person or the legal arrangement is subject in the original country to deal with the bank, in case this condition is mentioned in the internal articles of the legal person or legal arrangement.

c- The financial institution is to supervise the non-resident customers' accounts, whether they are natural, legal person or legal arrangement, to ensure that these accounts may not be used for the purpose other than that was opened for, and to identify any unusual and suspicious transaction that may be implemented, as well as the financial institution should prepare special periodic reports, on the activity of these accounts, to be submitted to the reporting official of that financial institution.

Sixth-Correspondent banks: the procedures will be applied as follows**:-**

a) Gather sufficient information about the respondent bank to understand the nature of its business and evaluate, using publicly available information, the reputation of the respondent institution and the level of supervision to which it is subject, including whether the institution or any of its board members or owners of its controlling stake has been subject to a money laundering or terrorist financing investigation or regulatory action.

b) Evaluate the AML/CFT controls implemented by the respondent institution and verify their efficiency and adequacy.

c) Obtain approval from the institution’s board of directors before establishing relationships with foreign financial institutions.

d) Document the respective AML/CFT responsibilities of each institution with regard to correspondent banking.

e) Ensure that the respondent banks has performed CDD obligations on any customers having direct access to the correspondent account by means of payable-through accounts services and are able to provide relevant information about these customers when necessary.
f) Institutions shall not open a correspondent account for any shell bank or for any bank providing correspondent services to shell banks. It is also forbidden to continue any existing banking relationship with a shell bank. Financial institutions should ensure that respondent institutions do not allow their accounts to be used by a shell bank.
g) Complete a written questionnaire showing the position of the correspondent institution regarding compliance with local AML/CFT legislation and supervisory controls, standards of due diligence applied by the institution to its customers, and the availability of effective internal policies and procedures in that regard.
h) Regularly monitor transactions using correspondent bank accounts to ensure that they are in line with the purpose behind opening the account.
i) When implementing due diligence procedures for correspondent banks, institutions must determine their risk level based on available information on such banks, including the following:
   1- The parent bank is existed in a high-risk country.
   2- The extent to which the correspondent bank provides private banking services.
   3- The extent to which the correspondent bank holds accounts for PEPs.
   4- The quality of monitoring and supervisory systems it is subject to
   5- Regular/abnormal changes in the correspondent bank's management or business plan.
j) The institution shall establish a clear policy on updating and assessing the correspondent banks information at least yearly, including to ensure that no relationship with a shell bank exists.

Seventh: Other cases:

In addition to situations described above, financial institutions shall apply enhanced CDD in the following cases:

a- Requesting financing against deposits
b- Renting out safety deposit boxes
c- When depositing cash or traveler checks into an existing account by a person/persons whose names are not mentioned in a power of attorney related to such account or if such person is not authorized by the owner of the account to deposit funds in it.
d- Renting deposited assets at unreasonable high-value.
e- Other situations which may be specified by the financial institution.

Article 11

Modern techniques and new technologies.

First: Institutions shall identify, assess, and manage the risk of ML/FT that may arise as a result of the following:

a) The development of new products and new business practices including new electronic delivery mechanisms for services;

b) The use of new or developing technologies for both new and pre-existing products.

Second: When providing payment services through **mobile phone**, the financial institution shall implement the following:

a. Ensure that it obtains adequate information on money transfer controls, when using this service in the transfer of money.
b. Ensure the ability to stop the service in the event of misuse by the customer, and include this condition in the service contract.
c. Exercise ongoing monitoring of transactions and retrieval of unusual transaction reports generated by the use of such service.
d. Set reasonable limits to deposit into accounts used in this service, as well as the value of the transaction that can be executed.

Article: 12

Updating Customer Information:

First: Financial institutions must keep customer due diligence information updated. For customers who were subject to the identification procedures set out in the AML Law and this Instruction, financial institutions must periodically and adequately update information and documents obtained based on materiality and risk, when such measures were implemented. At minimum, customer information shall be updated at least once every three years for customers assessed as posing a standard ML/TF risk, while information on higher-risk customers should be updated at least once every year.

Second: By the exception of paragraph first of this article regarding updating customer due diligence information on a regular basis, the financial institutions shall apply such updating procedures to customers immediately in the following cases:

a. When carrying out a large or complex transaction for any such customer
b. When changes are known to have occurred to necessary client identification documents
c. When a significant change is seen in the way the customer deals with his/her account or with the business relationship with the financial institution.

Article 13:

Transfers:

Scope of execution

The provisions of this paragraph shall apply to transfers (wire or regular) sent or received by the financial institution in any currency, including when a credit, debit or prepaid card is used as a payment system to effect a person-to-person wire transfer. All transfers originating from such transactions must have a unique reference number to track the transaction back to the originator and beneficiary of the transfer, in addition to follow the below mentioned procedures:

First: Obligations of originating financial institutions:

a-

1- The institution originating the transfer (whether domestic or external) shall obtain full information about the transfer originator, including: the transfer number, its date, amount, name of originator, his/her nationality, address, occupation, identification number, or tax number, account number, the purpose of the transfer, correspondent bank, the beneficiary, his/her nationality and account number if available.

2- In the absence of an account number for the originator, the institution shall give a unique transaction reference number to the transaction.

b- The originating institution shall verify the accuracy of the information about the originator before sending the transfer, using official documents and information

c- The financial institution should include in the transfer form all the data referred to in paragraphs (a) 1 and 2 above.

d- Where several transfers from a single originator are bundled in a batch file, the originating financial institution shall include the originator's account number or unique transaction reference number in the absence of an account, provided that:

1- The institution keeps all the information on the originator as stipulated in paragraphs (a) 1 and 2.

2- The institution has the ability to provide the beneficiary institution with all required information within one business day from the date of receipt of the request for information.

3- The institution responds immediately to any order issued by the Bank, the Office or competent law enforcement authority to access all required information.

Second: Obligations of beneficiary institution:

a- The beneficiary institution shall establish effective systems to detect any lack in the required information on the originator of the transfer under paragraph first (a) 1and 2 of this article.

b- The beneficiary institution shall adopt effective risk-based policies and procedures to deal with transfers that lack required originator information, these procedures may include requesting missing information from the originating financial institution. In case of failure to obtain the required information, the institution must take risk-based action, which may include the rejection of the transfer and/or reporting the situation to the Office.

Third: Obligations of intermediary financial institutions:

a- If intermediary institutions are involved in executing the transfer without being its originators or beneficiary institutions, they should ensure that all information accompanying the transfer is retained with it.

b- Where technical limitations prevent the required information from remaining with the wire transfer, the intermediary institution shall keep a record, for at least five years, of all accompanying information, regardless of completeness or lack thereof, and it should be able to provide this information to beneficiary financial institutions within three business days from the date of request.

c- In case that the intermediary institution have received incomplete information about the sender from the originating institution, so this intermediary financial institution should take reasonable measures to inform the beneficiary institution which will implement receiving procedure .

Article 14

Reporting suspicious transactions:

First: The compliance officer at the institution is the person in charge of reporting suspicious transactions to the Office.

Second: The compliance officer must report to the Office immediately concerning any transaction or attempted transaction it suspects or has reasonable grounds to suspect that it is linked to proceeds of a crime, money laundering, related to terrorism, used for terrorism, used to commit terrorist acts, used by a terrorist organization, or used by those who finance terrorism.

Third: If any employee of the institution suspects there is a transaction or attempted transaction it suspects or has reasonable grounds to suspect that it is linked to proceeds of a crime, money laundering, related to terrorism, used for terrorism, used to commit terrorist acts, used by a terrorist organization, or used by those who finance terrorism, he/she should inform immediately the compliance officer of the basis for the suspicion, and attach all the data and copies of documents related to that transaction or attempted transaction..

Fourth: If the Compliance Officer decides that a transaction or activity is suspicious, he/she shall provide the Office with an information report (STR) and facilitate access by the Office to the relevant records and information held by the financial institution.

Article 15

Books and Record Keeping

Institutions must retain the following records and documents for a period of 5 years following the termination of the business relationship, the closing of the customer's accounts, or the execution of a transaction with a customer with whom it is not in an established business relationship, whichever is longer, and they shall guarantee their availability to competent authorities as swiftly as possible:

First: Copies of all records obtained through CDD measures, including documents proving the identity of customers and beneficial owners, accounting files and business correspondence.

Second: Records and data of transactions, both local and international, executed or attempted. These records should be detailed in a way that permits the reconstruction of the steps of each individual transaction.

Third: Copies of STRs submitted to the Office and related documents for at least five years after the date of notifying the Office, or the date of issuing a final ruling in a related criminal lawsuit, even if the legally set record keeping period is exceeded.

Fourth: Records relating to risk assessments and any relevant information from the date of the assessment or its update.

Fifth: Any other information related to AML/CFT operations.

Article 16.

Establishing and implementing AML/CFT programs

Financial institutions shall establish and implement AML/CFT programs including:

first- Carrying out an ML/FT risk assessment including identifying, assessing and documenting the institution's understanding of such risks, taking effective measures to mitigate them and making such assessment available to supervising authorities.

Second-Establishing internal policies, procedures and controls in line with the requirements of the Law and this Instruction to mitigate identified risks.

Third-Adopting and implementing adequate standards of integrity in the recruitment of staff.

Fourth-Continuous AML/CFT training programs for staff to enhance their capacities in understanding AML/CFT risks, identifying suspicious transactions and behavior, knowing how to deal with such, and effectively implementing required measures.

Fifth - Independent auditing to test the level of effectiveness and implementation of AML/CFT policies and procedures.

Sixth: Records of training programs including training material, dates, names of trainers, and signatures of trainees in order to document the training activity.

Seventh: The implementation of mechanisms for exchanging information within the financial institution and, where appropriate, between different units of a financial group and for maintaining confidentiality.

Eighth: Financial groups shall implement group-wide programs against ML/TF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group. These should include the measures set out under items 1 to 4 above, and also:

(a) Policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

(b) The provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and

(c) Adequate safeguards on the confidentiality and use of information exchanged.

Article 17:

The present instructions shall enter into force on the date of its publication in the official gazette.

Ali Mohsen Ismail

Governor of the Central Bank of Iraq