Official Gazette of Iraq

Al-Waqai’ Al-Iraqiyya

الوقائع العراقيـة

وەقایعی عیراقی

الجريدة الرسمية لجمهورية العراق

ڕۆژنامەی فەرمی کۆماری عیراق

تصدر عن وزارة العدل

وەزارەتی داد دەری دەکات

Legislation

No. 1

Instructions of Rules of Due Diligence towards the Financial Institutions Clients

No. (1) of 2017

With their amendment

تعليمات قواعد العناية الواجبة تجاه العملاء للمؤسسات المالية

مع تعديلها

Translated in

Ministry Of Justice

Iraqi Official Gazette Department

Translation Section

2022

Instructions

In accordance to the provision of Item (Fourth) of Article (10) of the law of anti-Money Laundering and Terrorist Financing No.(39) of 2015

The following instruction has been issued:

Instruction of the Rules of Due Diligence towards the Financial Institutions Clients

No.(1) of 2017

Article 1

For the purpose of this instruction, the following expressions shall have the meanings indicated next to them:

First: Due diligence towards Client: Identifying the client's identity, legal status and activity, and the purpose of the working relationship and its nature, and the real beneficiary if any, and verifying all this and continuously following-up operations that are in a continuous relationship with any of the means specified under the relevant legislation and identifying of the future relationship between the financial institution and the client and its purpose.

Second: Dangerous high-level position holders: Persons who have been entrusted with prominent public duties in the Republic of Iraq or foreign state, like president of states or governments, high-rank politicians and officials, senior judges, senior military personnel, senior executives in stated-owned companies, leaderships of political parties or those who have been entrusted with outstanding duties in an international organization like the members of senior management and their deputies and members of the board of directors and the like, widely and publicly known personal advisors or anyone who works in a position allows him/ her to benefit greatly from the close practical association with the danger-represented politicians and their immediate relatives up to the second degree.

Third: Associations and non-profit organizations: Any moral person established in accordance with the law whose main purpose is to provide social or voluntary services without the aim of his/ her activity to achieve profit or personal benefit, including local and foreign civil society organizations.

Fourth: Immediately: Within hours not exceeding one working day.

Fifth: Reporting Officer: Head of Formation provided for in Article (14) of the Anti-Money Laundering and Terrorist Financing Act No. (39) of 2015, who is appointed by the Senior Management for the purpose of reporting operations suspected of being linked to money laundering and terrorist financing.

Sixth: Financial Group: A company or any other type of natural or moral persons who possess control shares and coordinate functions with the rest of the Group to apply or implement or Group control under the basic principles along with branches or subsidiaries that are subject to policies and procedures to combat money laundering and terrorist financing at the Group level .

Seventh: Intermediary Financial Institution: The financial institution that, whether in the series of payment procedures or in covering the payment, receives and transfers wire transfer on behalf of the financial institution exporting the transfer and the financial institution receiving the transfer or another intermediary financial Institution.

Eighth: Financial institution exporting transfer: The financial institution that begins wire transfer and transfers money upon receiving wire transfer request on behalf of the transfer originator.

Ninth: Financial institution receiving transfer: The financial institution receiving wire transfer from the financial institution exporting the transfer directly or through an intermediary financial institution and making money available to the beneficiary .

Article 2

The financial institutions shall apply the following general rules of due diligence towards the clients:

Instructions

First:

a. Anonymous or digital accounts or aliases or pseudo names may not be dealt with, kept or provided any services to them, and taking due diligence measures towards the owners or beneficiaries of such accounts as soon as possible and in any case before or during their use.
b. Identifying and verifying the client and the real beneficiary using original documents and reliable data or information from independent sources in accordance with the provisions stipulated in these instructions.
c. Understanding the purpose and intended nature of the working relationship and requesting, where appropriate, additional information in this regard.
d. Using automated systems that continuously monitor the relationship with the client to identify the pattern of his/ her transactions and detecting any transactions that are incompatible with this pattern or the institution's information about its client, his/ her activity and his/ her danger profile, including the funds' and wealth's source for any client classified as high-danger.
e. Taking due diligence procedures themselves and not relying on a third party to take them.

Second: The scope of due diligence measures provided for in Item (1) of this article shall be determined by using the danger-based approach.

Third: The financial institutions shall execute the due diligence measures in the cases stipulated in Item (First) of Article (10) of anti-money laundering and terrorist financing law.

Fourth: The financial institutions may postpone the procedures of verifying the identity of the client until after the banking relationship is established in accordance with the following:

a. The postponement of verification procedures shall be necessary for the normal functioning of the procedures.

b. The financial institution shall perform due diligence procedures towards clients under the Anti-Money Laundering and Terrorist Financing Law and these instructions as soon as possible after the establishment of the business relationship.

c. The financial institution shall has taken the necessary procedures to assess the dangers of money laundering and terrorist financing in relation to the case where the postponement has been taken, including setting limits on the number, type and value of operations that can be carried out before the information verification procedure is completed.

Fifth: If the financial institution is unable to comply fully with the due diligence measures towards clients provided for in the law or these instructions, the account may not be opened, the business relationship may not be initiated, the transaction may not be executed or any other operations, and work relationship shall be terminated if it exists and inform the Office for Combating Money Laundering and Terrorist Financing about the client.

Sixth: Due diligence procedures may be not completed in case of suspected money laundering or terrorist financing at the financial institution, if case the execution of these procedures may alert the client, provided that the suspicious operation is immediately reported to the money laundering and terrorist financing referral office.

Seventh: Due diligence procedures shall be applied on the basis of relative importance and dangers towards the relationships that existed with clients prior to the entry into force of the Anti-Money laundering and terrorism financing law, and taking due diligence measures towards current business relationship, taking into account whether the due diligence measures were taken before the date of their taking and the adequacy of the data obtained.

Eighth: Ensuring that the client is not included in the lists of prohibited clients in accordance with the provisions of the Anti-Money Laundering and Terrorist Financing Law before entering into an on-going relationship with him/ her, and not to perform any operation for a client listed on the ban lists and shall not have a business relationship with him/ her.

Ninth: Relying on identification papers to prove client's identity as well as ensuring its validity, and keeping a copy thereof signed by the competent employee indicating that it is a true copy, and the institution shall, when doubt in the validity of the documents or data submitted to it, verify their authenticity by all possible ways, including contacting the authorities that issued these documents or data.

Article 3

The financial institution shall take the following to identify the natural person:

First: Verifying the identity of the person by relying on valid supporting official documents, such as the personal card, driving license, residence card, passport or travel document, taking into account that the identification data includes the full name of the client, his/ her nationality, date of birth, permanent residence address, phone numbers, work address, type of activity, purpose of dealing, names, data of those authorized to deal with the account and any other information that the financial institution deems necessary to obtain.

Second: Obtaining documents that authorize the legal representative to deal with the financial institution for incapacitated persons.

Third: Verifying the existence of an official agency that authorizes the agent to deal on the principal's account, and to identify the agent in accordance with the procedures for identifying the client stipulated in the Anti-Money Laundering and Terrorist Financing Law and these instructions, while keeping an true or certified copy of the agency.

Article 4

The financial institution shall take the following to identify the legal person:

First: Identifying the name of the legal person, legal form, address of headquarters, type of activity, the capital, the names of those delegated or authorized to deal on the account, their nationalities, phone numbers, the purpose of the dealing and any other information the Corporation considers it necessary to obtain it.

Second:

a. Verifying the existence of the legal person of the company and its legal entity through the articles of incorporation or incorporation statement, the bylaw, the company's address and headquarters, the company's accounts, the company's registration certificate with the Registrar of Companies, and the start-up certificate for The public joint-stock companies and the decisions of the company's board of directors or the manager authorized to open the account with the financial institution and the appointment of those authorized to manage the company's accounts and the limits of their powers.
b. Verifying the existence of the legal person as for the state departments through the legal means that established it and the approval of the Supreme Head who is legally authorized to open the account and the document of authorising those authorized to sign the account and the limits of their powers, signed by the legally-authorized Supreme Head.

Third: Obtaining the delegation or authorization documents from the legal person for the natural persons authorized to deal on the account, in addition to identifying the person authorized to deal on the account in accordance with the procedures for identifying the client stipulated in these instructions.

Fourth: Mixed joint-stock companies shall be excluded with respect to the government's share from the request for data related to the names of owners and ownership shares. It shall be only asked the data for the names of shareholders whose contribution percentage exceeds (10%) ten per cent of the company's capital.

Article 5

The financial institution shall take the following to determine the identity of associations and non-profit organizations:

First: Identifying the association or organization, its official name, legal form, headquarters address, type of activity, date of incorporation, organizational structure, the minutes of the board of directors' election or its appointment decision, and the names of the authorized persons in dealing on the account, phone numbers, the purpose of the dealing, and any other information that the institution deems necessary to obtain.

Second: Verifying the existence of the association or organization and its legal entity through a certificate of incorporation from the competent authority and the bylaw of the association or organization.

Third: Submitting a letter specifying the bank in which the account is opened, signed by the competent authority.

Fourth: Obtaining documents indicating the existence of an authorization from the association or organization for natural persons authorized to deal on the account and identifying the person authorized to deal in accordance with the procedures for identifying the client stipulated in these instructions.

Fifth: Obtaining identity information for donors and beneficiaries of deposited and withdrawn funds.

Article 6

The financial institution shall take the following when identifying the credit fund:

First: Identifying the credit fund, its official name, legal form, instrument of existence, credit contract and purpose, and the type of its activity.

Second: The name of the trustee or trustees, his/ her address, e-mail address if any, phone number, and any other means of communication.

Third: The purpose of the business relationship.

Fourth: The trustee's signature.

Article 7

The financial institution takes the following to determine the identity of the real beneficiary:

First: Requiring each client, upon opening the account or starting the business relationship, to submit a written declaration specifying the identity of the real beneficiary of the operation to be performed. The declaration shall include at least client identification information.

Second: Identifying the real beneficiary, and taking reasonable measures to verify this identity, based on data or information included in the official documents and data, in a manner that constitutes the conviction of institution's knowledge of the true beneficiary's identity.

Third: Identify the real beneficiary in the case of the legal person and the legal arrangements by taking reasonable measures to identify the ownership structure and the controlling management of the client.

Article 8

Financial institutions shall be obligated to set rules for managing the dangers of money laundering and terrorist financing, including the following:

First:

a. Classifying clients into the following categories in accordance with the levels of dangers and their relative importance, and setting the necessary procedures to deal with these dangers in proportion to each degree:

1. (Clients with high-dangers): The strict due diligence measures stipulated in Article (10) of these instructions shall be applied to them, in addition to the due diligence measures stipulated in Article (10) of the Anti-Money Laundering and Terrorist Financing Law, in accordance with the degree of dangers and their relative importance
2. (Clients with medium dangers): The normal due diligence measures stipulated in Article (10) of the Anti-Money Laundering and Financing Terrorism Law shall be applied to them.
3. (Clients with Low-danger): A simplified version of the normal due diligence measures shall be applied to them if the financial institution so decides in accordance with the degree of dangers and their relative importance.

b. Reviewing the rating of clients in accordance with the degree of dangers at least once a year or in the event of changes during the year that require so, and it shall be deemed one of these changes is the repeated appearance of the client’s name in the reports deduced from the unusual operations, and the notification of the Anti-Money Laundering and Terrorist Financing Office of a case of suspicion related to the client.

Second: Laying down policies and procedures based on identifying, evaluating, controlling and reporting dangers. The rules shall include all areas of danger, including, at a minimum, the following:

a. Dangers of banking products and services that can be exploited in money laundering and terrorist financing, including new innovative products or services, whether offered by the financial institution or a party to it. The financial institution shall be guided by the following factors in determining these dangers:

1. Products and services that are identified as having high dangers by the Money Laundering and Terrorist Financing Office in coordination with the Iraqi central Bank.
2. Products or services that do not allow the disclosure of a large amount of information that related to the identity of their users, or those that have international nature, such as banking services provided through the internet and stored-value payment cards.
3. Work relationships that are not done face to face.
4. Private banking services.

b. Client's dangers: These include dangers related to clients or their dealing with the financial institution or the sector to which they belong. The financial institution shall, when determining these dangers, depend on the information obtained through identification procedures and public information known or available to the financial institution, and by following up the pattern of client's operations. the financial institution shall guide by the following factors when determining these dangers:

1. Client dangers:

First: Clients are difficult to identify the true beneficiary of their dealings for any reason, including the complexity of their ownership structure in the case of moral personalities or legal arrangements.

Second: Clients whose reputation or previous dealing have been tarnished.

Third: Non-resident Clients

Fourth: Clients who are considered dangerous high-position holders or those who are associated with them.

2. Dangers related to clients' transactions:

First: The transactions are inconsistent with the stated purpose of the transaction.

Second: The services requested from clients are not commensurate with the nature of their activity.
Third: Carrying out complex or great operations without a clear justification.
Fourth: Dealing with an institution's headquarters away from the client's residence or place of work without a clear justification.
Fifth: Multiple accounts of the client or its bifurcation with the financial institution or more than one financial institution in the same region without a clear justification.
Sixth: Clients whose a clear change in the pattern of their de with the financial institution without a clear justification.
Seventh: Clients whose information about their involvement in illegal activities received by the financial institution.
Eight: An justified use of intermediaries in transitions.
Ninth: The client requests that some operations be kept with an exaggerated amount of secret
Tenth: Indirect operations that are carried out by using modern technological means.

3. Dangers related to the clients-practiced activities sectors:

First: Activities that are characterized by intensive cash dealing, including some commercial activities and some activities related to submitting financial services, such as money transfer companies and foreign exchange companies in the event that they are not subject to the level of control to which the financial institution is subject.
Second: The organizations and charities which do not aim to achieve the profit.

Third: Merchants of minerals, precious stones, antiques and works of art.

c. Dangers related to specific geographic areas, including dangers related to the client's place of residence or work, and the source and destination of operations carried out on the account. The financial institution shall be guided by the following in identifying the high-danger geographic areas:

1. Countries that do not implement the recommendations of the financial work collection and that do not have appropriate legislation and systems to combat money laundering terrorist financing.
2. Countries that are subject to sanctions, prohibition of dealing or other similar measures of the united nations .
3. Countries that have a poor rating in terms of transparency .

4. Countries classified as financing or supporting terrorism or suffering from a high level of crime such as human or drug trafficking.

Article 9

The measures of simplified due diligence shall be as follows:

First: The financial institution may specify the transactions that are required to be performed or the clients for whom it is necessary to take simplified due diligence measures when identifying the and verifying client's and beneficiary's ID, taking into account the recommendations and international standards and the best international practices that establish examples of clients or operations with low dangers and any international controls or local requirements in this regards.

Second: It is not permissible to take simplified due diligence measures in the event of suspected money laundering and terrorist financing operations or in the event of high-danger circumstances.

Article 10

The Financial institution shall take strict due diligence measures for clients and high-danger financial services and operations, in addition to the normal due diligence measures, in the following cases:

First: Dangerous high-position holders

a. Taking reasonable measures to determine whether the client or the real beneficiary dangerous high-position holders.
b. Establishing danger management rules for dangerous high-position holders or the beneficiaries to whom they belong, provided that these rules include determining whether the future client is one of them who poses a dangers.
c. Obtaining the approval of senior management when establishing a relationship with dangerous high-position holders and upon discovering one of the clients or real beneficiaries of these category.
d. Taking adequate measures to verify the sources of wealth of any client or real beneficiary from dangerous high-position holders.

e. Accurately and continuously following-up the transactions of dangerous high-position holders with the financial institution.

Second: Unusual operations: The large or complex operations in a degree that is incompatible with a movement occurs on the account of the client and his/ her activity, or the operation of an unusual pattern that does not have a clear economic justification, in which, examining the background of the transactions shall be taken into consideration to examining and their purpose to the maximum extent possible, and registering the results reached in records shall be kept for this purpose and kept for a period of at least (5) five years.

Third: Private banking service: Those in which it shall be taken into account to obtain the approval of the senior management for them when providing banking services to clients and the application of identification procedures, and the following danger factors shall be taken into consideration in evaluation of the degree of dangers for the client:

a. The nature of the client, his/ her activity and sources of wealth.
b. Purpose of requesting private banking services.
c. The client's relationship with the financial institution in terms of its origin and development.
d. The structure of the client's companies that use these services.
e. The country in which the client carries out his/ her activity and the extent to which there are money laundering or terrorist financing dangers related to the concerned country, or the strength of the combating systems existing in this country.
f. General information available about the client and his/ her commercial reputation.

Fourth: Operations that are carried out with persons who are present in countries that do not apply the recommendations of the Financial Work Group or that they apply insufficiently, taking into account the following:

a. Taking what is necessary to examine backgrounds of operations that do not have a legitimate and clear economic purpose, verifying their purpose, and writing down what the results reached in writing in a manner that ensures that the bank, the Anti-Money laundering and Terrorist Financing office and the auditors of the financial institution have access to them.
b. In the event that countries continue not to implement the recommendations of the Financial Work Group or not to apply them with the required efficiency in accordance

with the information available to them, the institution shall take any of the following measures in accordance with the degree of dangers and their relative importance, and they shall take appropriate measures against the people who belong to this country or are present in it:

1. Continuing to apply strict due diligence measures against these clients.
2. Close monitoring of the operations associated with these people and identifying its purpose.
3. Sending a statement of the operations related to these clients to the Anti-Money Laundry and Terrorist Financing Office.
4. Ending of business relationships with the clients or limitation of financial transactions with them when the financial institution is unable to implement effective due diligence.

c. The financial institution shall pay special attention to its branches and subsidiaries in countries that do not implement or inadequately implement the recommendations of the financial work group.

Fifth: Non-resident clients: It includes the category of clients, whether they are natural or legal persons, who do not have a place of residence or a permanent address in the country in which they are located, taking into account the following:

a. For natural persons, the entry visa to the country shall be reviewed, made sure that it is valid and obtaining a true copy of it.

b. For legal persons or legal arrangements, the following shall be done:

1. Obtaining a copy of document of establishing the legal person or legal arrangement, certified by the embassy located in the home country.
2. Obtaining an official document copy stating the registration of the legal person or the legal arrangement, certified by the competent authority in the home country.
3. Obtaining the approval of the controlling authority to which the legal person or legal arrangement in the home country is subject to deal with bank, in the event that such entry exists in the internal system of legal person or arrangement.

c. The financial institution shall monitor the accounts of non-resident clients, whether they are natural persons, legal persons or legal arrangement, to ensure that they are used for the purpose for which they have been established, and to identify any unusual or suspicious operation that takes place on them, and prepare special periodic reports on the activity of those accounts that shall be presented to official responsible for reporting in the financial institution.

Sixth: Corresponded banks, about which the following shall be taken into account:

a. Collecting sufficient information about corresponded banks to understand the nature of their activities, their ownership and management structure, the most prominent activities and works they carry out, their location and headquarters of the home institution and to make a decision in the light of the available information to determine the reputation of the original corresponded bank, the level of the control it is subject to and the extent of an investigation or civil or penal lawsuit against the bank or any of its management members or owners of the dominant share in the subject of money laundry and terrorist financing, or the existence of a controlling measure in this regard.
b. Assessing anti-money laundry and terrorist financing controls in the original corresponded bank and ascertaining their effectiveness and adequacy.
c. Obtaining the approval of the senior management of the financial institution when establishing a dealing relationship with foreign financial institutions.
d. Documenting the money laundry and terrorist financing responsibilities of each financial institution in relation to correspondent banking relationship.
e. Ensuring that the financial institution receiving the transfer implements the due diligence procedure for its clients who have direct access to the accounts of the corresponded financial institution, and the ability to provide information related to the clients of these operations when necessary.
f. Not to enter into a correspondence relationship with a sham bank or a bank that provides correspondence service to sham banks, or to continue an existing banking relationship with a sham bank.
g. The financial institution itself shall verify that the original correspondence institution do not allow the use of their accounts of sham banks.
h. Obtaining a written survey showing the position of correspondence banks regarding compliance with their local legislation and regulatory controls in the field of money laundry and terrorist financing, the due diligence standards they apply to their clients and the extent of availability of effective internal policies and procedures in them.

i. Periodic review of the operations carried out on the accounts of corresponded banks to ensure that those operations are consistent with the purpose of opening the account.

j. Determining the degree of danger of corresponded banks, guided by the available information about them, including the following:

1. The presence of the corresponded home bank in a high-danger country.
2. The extent to which corresponded bank provide private bank services.
3. The extent to which there are accounts for danger high-position holders in corresponded banks.
4. The extent of the quality of the control and supervisory systems to which they are subject.
5. The presence of continuous abnormal changes in the management of corresponded banks or their work plan.

k. Establishing a specific policy about updating and evaluating the corresponded bank data on an annual basis, and ensuring that no relationship with sham banks.

Seventh: Other cases shall include the following:

a. Financing request in return for seizing deposits.
b. Renting safety deposit boxes.
c. Depositing cash or tourist checks in an existing account by a person or persons whose names do not appear in a contract of attorney relating to that account or a person is not of those persons legally authorized by the account holder to deposit fund in this account.
d. Renting assets valued at unrealistic values.
e. Any other cases specified by the financial institution.

Article 11

First: The financial institution shall take appropriate measures to manage the dangers of money laundry and terrorist financing that arise from the following:

a. Developing new products and professional practices, including new means of providing services.
b. Using new technologies or developing the techniques used, whether related to existing or new products.

Second: The financial institution shall consider the following when providing mobile payment services:

a. The available of sufficient information about the rules of money transfer.

b. Ensuring the possibility of stopping the service in the event of its misuse, with including this condition in the terms of the contract to provide the service.
c. Continuously monitoring the operations and drawing up the exceptional reports for any unusual operations carried out by using this service.
d. Setting reasonable limits for feeding the accounts used in the service and the value of the operations that can be used by them.

Article 12

First: The financial institution shall update the information and documents it obtained in accordance with the degree of dangers and their relative importance when applying the due diligence procedures for clients who have been subject to the identification procedures contained in the anti-money laundry and terrorist financing law and in these instructions at least every (3) three years for all normal-danger clients and every year for high-danger clients on continuous and appropriate basis.

Second: An exception to the provision of Item (First) of this article, the updating procedure shall be immediate in the following cases:

a. Executing a large and complex operation for the client.
b. Warning of changes in the documents necessary to identify the client.
c. A significant change occurs in the way of dealing with the account or the business relationship with the institution.

Article 13

Financial institutions that work in electronic or ordinary transfers in any currency that they export or receive, including transactions made using payment or debit cards or any other similar payment method, shall oblige to keep an up-to-date list of their agents and make it available for inspection upon request, and the transfers rising from the transactions shall compare with recognizable reference number allow to follow up the transaction until they reach the person requesting exporting or person receiving the financial transfer, in addition to:

First: Obligations of the financial institution exporting the transfer:

a.

1. Obtaining complete information about the person requesting the exporting the transfer, including the money transfer's number and date, the amount of transfer, the transferee's name, nationality, profession, identity number, tax accounting number, account number and purpose of transfer, and corresponded beneficiary bank if it exists, its nationality and account number.
2. Establishing a system whereby the transfer applicant shall be given a recognizable reference number in the absence of an account number for the transfer applicant with the financial institution.

b. Sending the transfer after verifying all the information related to the transfer sender through official documents and data.

c. Ensuring that all data stipulated in the Para (a) of this Item is included in the transfer form and ensuring its presence.

d. For transfers that are sent in one package, the exporting financial institution shall attach the transfer applicant's account number or his/ her recognizable reference number in event that he/ she doesn't have an account, provided that:

1. The financial institution retains the full information about the transfer applicant stipulated in the Para (a) of this item.
2. The exporting financial institution have the ability to provide the receiving financial institution with the information requested in full within one working day from the date of receiving the request for information.
3. The financial institution have the ability to respond immediately to any order issued by the central bank, the office or the competent law enforcement authorities to view this information.

Second: Obligations of the financial institution receiving the transfer:

a. Developing effective systems to detect any lack of information related to applicant of transfer issuing stipulated in (1) and (2) of Para (a) of Item (First) of this article.

b. Adopting an effective policy and procedures based on an assessment of the degree of danger in dealing with the transfers in which information about the transfer applicant has not been completed, and among these procedures, requesting incomplete information from the financial institution exporting the transfer, in the event that they are not met, the financial institution shall take measures based on an assessment of danger degree which may include refusing the transfer or informing the office of the case.

Third: Obligations of the intermediary financial institution:

a. Ensuring that all information accompanying the transfer shall remain accompanying it upon the transfer in the event that the financial institution participates in the implementation of the transfer without being exporting or receiving it.
b. If the financial institution shall not be able to keep the information attached to the transfer for technical reasons, it shall keep all the accompanying information as received for a period of at least (5) five years, regardless of the completeness or lack of this information, and to enable it to provide this information to the receiving financial institutions within (3) three working days from the date of its request.
c. If the intermediary institution shall receive incomplete information about the transfer applicant from the institution sending the transfer, it shall inform the recipient institution about making the transfer.

Article 14

First: The official responsible for reporting shall be responsible for reporting suspected cases to the Anti-Money Laundering and Terrorist Financing Office.

Second: The official responsible for reporting shall obligate to notify the office immediately of any transaction or attempt to conduct a transaction whenever he/ she suspects or has reasonable grounds to suspect that they are related to the proceeds of crime or related to money laundering or terrorist financing.

Third: If any of the employees of the financial institution suspects that any transaction linked to the proceeds of crime, an attempt to conduct it or money laundering or terrorist financing, he/ she shall inform the official responsible for reporting about so, provided that he/ she attaches all data and copies of documents related to that transaction or attempt to perform it.

Fourth: If the official responsible for reporting finds a suspect in a process or activity, he/ she shall submit a report to the office with the data and facilitating his/ her access to the relevant records and information kept by the institution.

Article 15

The financial institution shall keep the following records, documents and instruments for a period of (5) five years from the date of the end of the relationship with the client or from the date of closing the account or implementing a transaction for a client with whom it doesn't have a business relationship, whichever is longer, and ensures their availability to the competent authorities as soon as possible:

First: Copies of all records obtained through the due diligence process in transaction verification, including documents indicating the identities of the actual beneficiary clients, accounting files and business correspondences.

Second: All records of local and international transactions, whether actually executed or that there has been an attempt to implement them, provided that these records shall be detailed to the extent that allows re-representation of the steps of each transaction separately.

Third: Copies of notifications sent to the Anti-Money Laundering and Terrorist Financing Office and what is related thereto up to the lapse of (5) five years from the date of submitting a notification or the date of the final judgment in a lawsuit related to it, even if it exceeds that period.

Fourth: Records related to the danger assessment or information scheduled for conducting or updating it.

Fifth: Any other information related to anti-money laundering and terrorist financing operations.

Article 16

The financial institution shall commit to preparing and implementing money laundering and terrorist financing programs that include the following:

First: Conducting an assessment of the money laundering and terrorist financing dangers that are subjected to, including the institution's identifying, evaluating, documenting and understanding these dangers and taking effective measures to reduce them and providing this assessment to the controlling authorities.

Second: Establishing internal policies, procedures and controls commensurate with the implementation of the obligations imposed in the law and these instructions, leading to the reduction of the assessed dangers.

Third: Establishing and applying appropriate integrity standards when selecting employees and ensuring that they don't have a conflict of interests.

Fourth: Continuous training for officials and workers to ensure raising their capabilities in understanding the dangers of money laundering and terrorist financing, identifying un usual or suspicious operations and behaviors, how to deal with them, and applying the measures to be followed effectively.

Fifth: Independent audit to select the extent of effectiveness of policies and special procedures for combating money laundering and terrorist financing and extent of its application.

Sixth: Keeping training records, which include training materials, dates of training sessions, names of lecturers for these training courses and signatures of attendance, through which the training activity shall be documented.

Seventh: Applying mechanisms for exchanging information and maintaining confidentiality within the financial institution, and when necessary, between the different units within the financial group.

Eighth: Applying anti-money laundering and terrorist financing programs at the level of the financial group and all its branches and subsidiaries that own the majority of its shares, and this includes the measures stipulated in the Item (First), (Second), (Third) and (Fourth) of this article in addition to:

a. Policies and procedures for exchanging information required for the purposes of due diligence measures and managing money laundering and terrorist financing dangers.
b. Adhering to the procedures of combating money laundering and terrorist financing and auditing them at the level of the financial group with information about the client, accounts and operations from branches and subsidiaries when necessary for the purposes of money laundering and terrorist financing.
c. Adhering to appropriate preventive measures about confidentiality and using of exchanged information.

Article 17

These instructions shall be effective from the date of its publication in the Official Gazette.

Ali Muhsin Ismael
Governor of the Central Bank of Iraq

In accordance with the provisions of Paragraph (Four) of Article (10) of Anti-Money Laundry and Terrorist Financing Law no. (39) of 2015, we have issued the following instructions:

Instructions no (2) of 2017

First Amendment to the Rules of Due Diligence towards the Financial Institutions Clients

No. (1) of 2017

Article 1

The texts of Items (Second and Third) of Article (14) of the instructions of the Rules of Due Diligence towards Financial Institutions Clients no. (1) of 2017 shall be repealed and replaced with the following:

Second: The official responsible for reporting shall be obliged to immediately notify the office of any transaction or attempt to conduct a transaction whenever he/ she suspects or has reasonable grounds to suspect that they are linked to criminal proceeds or related to money laundry, financing terrorist or terrorists or used for terrorism, used by a terrorist acts, terrorist organization or used by terrorist financiers.

Third: If any of the employees of the financial institution suspects that any transaction is linked to the criminal proceeds or an attempt to conduct a transaction, whenever he/ she suspects or has reasonable grounds for suspicion in connection with criminal proceeds or related to money laundering or financing terrorism or terrorists or used for terrorism, used for terrorist acts, used by a terrorist organization or used by terrorist financiers, he/ she shall inform the official responsible for reporting thereon, provided that he/ she attaches all data and copies of documents related to that operation or attempt to conduct it.

Article 2

This instruction shall be effective from the date of its publication in the Official Gazette.

Ali Muhsin Ismael

Central Bank Governor