Instructions No. (2/ES/507/2023) Concerning Anti-Money Laundering & Combating the Financing of Terrorism

N.B.: This English translation is prepared by the Central Bank of Kuwait for information purposes only. In case of any variance between Arabic and English versions, Arabic text shall prevail.

Instructions No. (2/ES/507/2023) Concerning Anti-Money Laundering & Combating the Financing of Terrorism

In the context of reinforcing Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) efforts, and in order to ensure the required compliance with the application of the international standards issued by the Financial Action Task Force "FATF" in this regard, and in line with the provisions of the Law No. (106) of 2013 Concerning Anti-Money Laundering and Combating the Financing of Terrorism, its Executive Regulations and the relevant promulgated ministerial resolutions, as well as the provisions of Articles No. (14) and (15) of the said Law, which provided that the regulatory authorities shall supervise and monitor compliance with the requirements of anti-money laundering and combating the financing of terrorism, and imposing the appropriate penalties and sanctions on the units subject to their supervision.

And, whereas the banking and financial institutions are the most targeted entities for money launderers and terrorism financers, for the purpose of concealing and disguising the illegal sources of their funds. As such, these institutions are always exposed to risks arising from such acts. And, in order to protect the banking and financial institutions from such illegitimate practices and to avoid any adverse impacts they may face due to these risks, it is necessary for all banking and financial institutions to take the measures which ensure that they are not manipulated by such operations, in addition to ensuring compliance with the full implementation of the requirements under the recommendations issued by FATF and the provisions of the referred to Law, and,

In view of the above, CBK has updated the instructions issued on 23rd July 2013 to all exchange companies under No. (2/ES/310/2013) concerning Anti-Money Laundering and Combating the financing of terrorism. This update has been introduced to enhance and clarify some of the needed requirements revealed by CBK during its recent monitoring to achieve the full and optimal compliance with these requirements by the CBK-regulated exchange companies.

Accordingly, all exchange companies subject to CBK supervision and operate in the State of Kuwait shall comply with the requirements of anti-money laundering and combating the financing of terrorism as follows:

First: Determining the Risks Associated with Money Laundering and Financing of Terrorism:

1. The exchange company shall prepare a written study, updated every two years, addressing all risks associated with money laundering and the financing of terrorism that it may be exposed to as it operates within its mandate that befits the scale of its activity and the nature of its transactions. As a minimum, the study shall address risks associated with:

    a) The different types of customers the company interacts with and types of customers it may not interact with (should there be any).

    b) The countries and geographical regions where any of the requested transactions are processed.

    c) The products and services, whether currently provided to customers or those being developed.

    The level of risk the exchange company is exposed to in terms of the items mentioned above shall be assessed within a three-level scale of (Low, Moderate, High) and the measures appropriate and necessary to monitor and manage each level shall be put in place to reduce impact on company activity.

2. Within the scope of identification of the risks associated with the elements mentioned in paragraph (1) above, the study of these elements shall consider the factors that may increase the risks associated with each element, and put the appropriate measures in place, such as:

    a) As for the different types of customers:

    1. The nature of the customer's business/activity.

    2. The unusual activities and risks associated related thereto.

    3. The legal form of the customer.

    4. The ownership structure of the customer, clarity of ownership and whether there is any unusual ownership.

    5. The existence of an actual activity for the customer, with clear lawful economic purposes consistent with the business he/she is authorized to exercise.

6. The customer is resident in the State of Kuwait or a non-resident customer.

7. The purpose of transactions to be executed for the customer.

8. The volume of annual transactions executed by the customer.

9. Frequency of transactions executed for the customer.

10. The period prior to the transactions with the customer (how long since relationship was established with the customer).

11. Risks associated with Politically Exposed Persons (PEPs) and individuals connected to them.

12. Customers who own massive assets.

13. Customers for whom no clear information are available about the source of income or owned assets.

14. The customer's business associated with high risks related to money laundering or terrorism financing.

15. Customers for whom transactions are executed without the requirement of their physical presence.

16. Customer has business/social relationship with individuals residing in high-risk countries.

b) As for Countries and Geographical Regions

1. The Financial Action Task Force (FATF) classification of the countries concerned, whether in terms of level of compliance with international AML/CFT standards, or in terms of sufficiency of the counter-measures they have in place according to the published assessment reports, where such reports may indicate inadequacies in this respect.

2. The list issued by Kuwait Financial Intelligence Unit (KFIU) on high-risk countries and the amendments made by the Unit to this list in view of its continuous monitoring.

3. The countries concerning which United Nations Security Council (UNSC) resolutions are issued, or those currently subject to UN sanctions, boycotts, or like measures.

4. Classifications issued by reliable sources concerning corruption, criminal activities, and country rankings in this regard.

5. Classifications issued by reliable sources identifying countries which are funding or supporting terrorist activities or where specific terrorist organizations are active.

c) As for Products and Services

1. Requirements and conditions for provision of product or service.

2. Services rendered through various cards.

3. Services or products whose execution does not require the presence of the customer for identity confirmation purposes.

4. Unusual patterns of transactions.

5. Any new product or service being developed and to be offered to customers.

3. In light of the findings of the assessment and identification of risks to which the exchange company is exposed as required above, the type of due diligence applied with regard to the execution of transactions, shall be identified, taking into consideration the following measures as a minimum limit:

a) Documents to be collected based on the level of risks associated with transactions and customers.

b) Information customers shall be required to be submitted, identified in view of the level of associated risks.

c) Documents and information to be collected regarding the transaction to be executed, verification of the beneficial owner customer (actual requester of the transaction), and obtaining the full name of the party to receive the funds (party benefiting from the transaction).

d) Procedures to be applied upon execution of transactions across any of the other countries, in accordance with the level of risks associated with each.

e) Enhanced due diligence measures that shall be followed in case of high risks, whether related to customers, to countries, or to product/service.

f) Updating customers' information and data on periodic basis commensurate with the degree of the associated risks (one year or less for high-risk customers, two years or less for medium-risk customers, three years at most for low-risk customers).

4. The study on risks associated with money laundering and terrorism financing and its results shall be approved by all partners and the Managing Director (whether the company's manager or the board of directors, where there is one).

The prepared study and all updates incorporated therein shall be maintained according to the requirement of documents and records keeping mentioned in Item Seventeenth.

Second: AML/CFT Policy:

1. Each company shall have in place a policy covering the targets and scope of anti-money laundering and combating of terrorism financing requirements to be observed, and the policy shall, at a minimum, stress the following:

    a. Complete compliance with provisions of Law No. (106) of 2013 concerning countering money laundering and combatting the financing of terrorism and its executive regulations, as well as all relevant ministerial decisions and CBK instructions.

    b. Refer to developed and approved procedures including steps to be followed to achieve compliance with the requirements of anti-money laundering and combating of terrorism financing and develop internal control systems which shall be followed in order to implement the required combating requirements.

    c. Develop procedures to be followed upon dealing with high-risk persons, especially Politically Exposed Persons (PEPs).

    d. Identify and assess the risks the company is vulnerable to while operating, whether related to customers, the nature of the company's services and operations, or those related to correspondents and countries it deals with. Risks are classified within three levels (low, medium, and high) to help determine the counter measures the company needs to employ.

    e. Apply due diligence measures proportionate to the level of risk, which shall be satisfied before executing requested transactions.

    f. Follow specific procedures to apply the principle of "Know Your Customer" and use a form designated for this purpose, which specify the information that shall be obtained and the intervals for their update in view of customer-related risks.

    g. Comply with the requirements relative to freezing or to abstaining from all dealings with names included in the lists issued by the UN Security Council (UNSC) sanctions committees or pursuant to local resolutions issued by the Ministry of Foreign Affairs' committee overseeing the implementation of UNSC resolutions in view of Chapter VII of the UN Charter concerning financing of terrorism and of proliferation of Weapons of Mass Destruction (WMD).

h. Commitment to notifying the FIU of any suspected money laundering or terrorism financing cases identified by the company during the period defined for that purpose.

i. Have procedures for dealing with high-risk persons, especially Politically Exposed Persons (PEPs).

j. Save and maintain documents, records, and information pertaining to customers and the transactions executed for the legally specified period.

k. Commitment to appoint a compliance controller/officer entrusted with verifying the level of the exchange company's compliance with provisions of Law No. (106) of 2013, its executive regulations, and relevant ministerial decisions.

l. Prepare quarterly reports by the compliance controller/officer to be presented to the company's manager and all partners, including the efforts of the compliance officer towards verifying compliance with (AML/CFT) requirements.

m. Ensuring that all company branches comply with all requirements and provisions of the law and ministerial decisions and these instructions and recommendations issued regarding FATF (AML/CFT) standards in effect at a minimum, as well as stressing the importance of cooperation on the exchange of information and safeguarding confidentiality thereof, along with putting in place the appropriate methods to ensure compliance.

n. Commitment to compliance with standards of integrity and appropriate experience when appointing new staff at exchange companies.

o. All company's staff should be aware of suspicious patterns which are published and updated continuously by KFIU, and records on this regard shall be documented.

p. Having in place a continuous training plan, prepared at appropriate periodic intervals, where staff (new recruits as well as current) take part in training programs addressing issues of countering money laundering and combatting the financing of terrorism.

2. The company's policy shall be compatible with the size, nature and scope of transactions it executes and said policy shall be continuously updated (every two years at least) in view of periodic review thereof to stay abreast with any developments in AML/CFT-related efforts.

3. The exchange company's policy shall be approved by the official in charge of its management (the General Manager or the Board of Directors, where there is one) and all partners.

Third: Applicable Procedures and Internal Control Systems:

1) The company shall develop **written procedures** including steps to be followed and applied for the execution of transactions in view of its activity and the internal supervision controls it has in place to ensure full compliance with (AML/CFT) requirements. The procedures shall also be reviewed at regular intervals parallel to the revision of the policy in place in this area (once every two years at least), and it shall, at a minimum, address the following:

   a. Steps to be applied to meet due diligence requirements as per associated risks, be that ordinary or enhanced due diligence.
   b. Nature and type of documents required to be collected from customers in view of risk associated with to each of them.
   c. Nature of information to be collected from customers in line with regular due diligence, as well as that to be collected from high-risk customers, especially Politically Exposed Persons (PEPs) and individuals dealing with whom requires enhanced due diligence.
   d. Steps to be followed in implementation of the (KYC) principle and completion of a form designated for this purpose, taking into consideration customers' associated risks, information and data to be collected and the appropriate intervals for the update of information in line with level of risk.

   e. Procedures to be followed to identify the beneficial owner (real) (natural persons, legal persons and legal arrangements), and procedures necessary to understand the equity of persons dealt with.

   f. Procedures necessary to identify whether the customer is the beneficial owner of the required transaction or he is acting on behalf of one or more other beneficiaries.
   g. Using a form (with a serial number) to prove the request to implement any transaction for any of the company's customers, and keeping it within the documents whether the transaction was executed or not.
   h. Steps to be followed for the continued monitoring of customers' transactions.

   i. Steps to be applied for offering services or products to customers in view of risk of money laundering and financing of terrorism, especially for the following:

      1. Buying and selling cash foreign currency, and buying and selling of precious metals.

      2. Foreign remittances whether inward or outward transactions.

      3. Transactions required by a customer to be executed through a proxy to another person(s) without the customer's presence.

   j. Steps to be followed to verify the commitment not to deal with any of the names included in the freezing lists issued by the Security Council sanction

committees or pursuant to local resolutions issued by a committee of the Ministry of Foreign Affairs to implement the Security Council resolutions in accordance with the Chapter VII of United Nations Charter related to combating terrorism and financing the spread of mass destruction weapons.

k. Measures to be followed for detecting operations and transactions that warrant suspicion of money laundering or financing of terrorism, where the KFIU is to be notified of any confirmation of grounds for suspicion within the legally specified period. The steps that shall be followed for preparing reports on suspicious cases and for determining administrative levels that shall grant approval on notifying the KFIU must also be determined.

2) Written procedures must be proportionate to the volume of the company's activity as well as the nature and scope of its transactions while taking into account guidelines stated in the guidebook prepared by the KFIU concerning the identification of types of money laundering and financing of terrorism.

3) The exchange company shall get the approval of the person in charge of management (general manager or Board of Directors, where there is one) on the procedures, as well as that of all partners.

Fourth: Customer Identification Requirements:

1) Exchange company shall not establish any business relations with any customer without verifying his full name, and identifying whether the service requester is the beneficial owner of the required transaction or he is acting on behalf of another beneficiary based on a legal document proving that. Also, exchange companies may not execute any transactions under names of unknown identity or dummy names.

2) Exchange company shall identify and verify the identity of the customer and the beneficial owner in the following case:

a. Prior to executing any transaction with any customer.

b. When delivering a service or executing a transaction, whether in Kuwaiti Dinar or in foreign currency (be that a single transaction or a series of connected transactions), specifically in relation to the following:

1. Buying and selling cash foreign currency, and buying and selling of precious metals.

2. Local or oversees electronic fund transfer.

3. Issuing a prepaid card in cooperation with any local bank.

c. Where the company desires to ascertain the validity of the identification data previously obtained from the customer.

d. Where there is suspicion of money laundering or financing of terrorism in connection with a transaction requested for any customer, regardless of the value of said transaction.

Fifth: Due diligence measures towards customers:

1. Due diligence measures towards customers, whether natural persons, legal persons and legal arrangements, in view of the risk-based approach, are realized through the following:

   a. Verifying the identity of the customer using documents or recognized tools obtained from trusted and independent sources.

   b. Identifying the beneficial owner of the requested transaction – the real requestor of the transaction – and employing reasonable measures to ascertain his/her identity in such a manner that he/she is fully identified/known to the exchange company.

   c. Understanding the purpose of the customer's transactions with the company as well as the type and nature of the requested transactions through obtaining the information the company needs for this purpose.

   d. Exerting continuous due diligence in connection with business relations and closely examining transactions executed during the period of such relations to ensure transactions executed are in harmony with what the company knows about the customer, his/her activity, and the level of associated risk.

2. The exchange company shall review identity confirmation documents or legal tools, which must be valid, and obtain a copy thereof that shall be signed by the concerned staff to attest it is an exact copy of the original that had been presented and reviewed where the following is required:

   a) For natural persons:

      1. Civil ID card for citizens or non-citizens (residents), whether the actual Civil ID card or by using the second level of Kuwait Mobile ID application.

      2. Passport or travel documents used to enter the country for non-residents.

      3. Official identification document issued and certified by the relevant official authority or body for customers who do not fall under the previous two items.

      4. The official document issued by the requester of the transaction authorizing the person dealing with the company on his behalf, as follows:

- A power of attorney issued from the Ministry of Justice by the customer requesting the transaction to the person dealing with the exchange company on his/her behalf.
- A previous authorization by the customer to the proxy, issued by the customer, which is to be signed in actual presence of the customer at company premises after verifying his/her identity.

The company - when executing any transaction under the customer's name – shall require a request for the transaction issued by said customer indicating his/her proxy for the transaction and his/her Civil ID number. The company shall ascertain authenticity of the customer signature on the request through comparison to that obtained in a previous authorization issued by the customer, and shall ascertain authenticity of documents relating to the authorized proxy named in the request for the transaction, where a copy of which is to be saved along with/attached to the document ascertaining the identity of the customer.

b) For Legal Persons or Legal Arrangements:

1. Full name of the legal person, date of incorporation, the headquarter business address and the names of the authorized signatories.
2. Documents evidencing incorporation of the legal person or legal arrangement and that it is entitled to exercise business according to the documents issued by the concerned authorities.
3. Legal documents indicating the names of the authorized signatory/ signatories on behalf of the legal person or legal arrangement, and documents indicating the names of the management's personnel, provided that copies thereof are included in the documents evidencing execution of the transaction.
4. Where a person is to represent an institution/company for dealing with the exchange company, legal documents or legal verdicts issued in this regard shall be submitted as proof.

Sixth: Identifying the Beneficial Owner (actual requester of the transaction):

1. The company shall take the necessary measures to identify whether the customer (natural person) is the beneficial owner (real) or acting on behalf of an beneficial owner (real) or more, through obtaining a certificate signed by the customer stating that the customer is the beneficial owner and not acting or executing the transaction on another party's behalf.

2. If the exchange company detects that the customer is acting on behalf of another beneficiary or more, it shall do what is necessary to ascertain the identity of the true beneficiary through obtaining related information or data from a reliable source in a manner that enables the company to be confident of the identity of the true beneficiary (true requester of the transaction). It must meanwhile

implement due diligence measures proportionate to the risk associated with the true beneficiary.

3. If the customer is a legal person or legal arrangement, the company should be required to take the appropriate measures to understand the equity and control structure for such customer, to reach the ultimate person in possession or in control of the customer, if there is a doubt whether this natural person controls or is responsible for managing the legal person, the company should take cascading steps to reach the beneficial owner (real) (to be followed according to a cascading approach, so that each following step is taken in case the previous one was not sufficient in verifying the beneficial owner (real) as follows:

    a. Verify the identity of natural person who possesses and controls interest of over 25% of a legal person or legal arrangement (of one or both).

    b. If the natural person who possesses and controls interest is not identified by the aforementioned ownership shares, any other available means shall be used to identity the natural persons who control the management.

    c. If the natural person is not identified by following the previous clauses (a, b), the company shall develop procedures in order to reach the natural person(s) who hold senior management position and through which the management of the legal person or legal arrangement is controlled.

4. For legal arrangements, company shall verify the identity of the person acting on behalf of the customer, the custodian, the beneficiary or any other person entrusted with these functions.

Seventh: Abstention from accepting new customers:

Exchange companies shall refrain from initiating a business relation or executing a transaction where it is not possible to ascertain the identity of the customer or the true beneficiary (true requester of the transaction), and consideration shall also be given to whether the situation merits notifying the KFIU and proof in relation to that shall be maintained.

Eighth: Enhanced due diligence measures for high risk customers and when providing specific services or performing certain operations

1) Exchange companies shall take additional measures to apply enhanced due diligence for customers classified as high risk, customers for whom transactions are executed without their physical presence and politically exposed persons the company has business with. This specifically includes increasing the degree and nature of supervision on the business relationship in order to determine whether the transactions executed or to be executed appear unusual or suspicious.

In this regard, exchange companies shall examine all complex and unusual transactions to identify the purposes, and verify all unusual patterns of transactions which have no clear economic or lawful purposes and objectives.

2) Enhanced due diligence measures shall be taken for business relations with correspondents across borders, especially those operating in countries previously classified "high-risk" or that do not fully comply with Financial Action Task Force (FATF) global (AML/CFT) standards mentioned in the issued lists.

3) Enhanced due diligence measures shall also be applied for services provided via modern technologies (Online Services).

4) Enhanced due diligence measures include, for example, the following:

   a. Obtaining additional information on the customer (natural person), the purpose of the transactions executed or expected to be executed, and the sources of his funds and wealth.

   b. Obtaining additional information on the customer (legal person), the nature of the expected business relationship with the customer, the volume of business and obtaining the latest available financial statements.

   c. Obtaining approval of the company's manager for establishing or continuing the business relationships.

   d. Conducting monitoring of the customer's transactions through strengthened and periodic monitoring, as well as determining whether certain types of transactions merit additional scrutiny.

5) Enhanced due diligence measures for customers referred to in paragraph (1) shall be implemented constantly during all stages of due diligence processes.

6) Enhanced due diligence measures concerning business relationships with customers who are not present in person shall include the obtaining of the customer's contact information, be that personal email or phone numbers through which they could be reached.

Ninth: Politically Exposed Persons (PEPs):

1) Exchange companies shall take appropriate measures to determine whether the customer or the beneficial owner (real transaction requestor) is a Politically Exposed Person (PEP), or is kin of (up to a second degree relative) with a PEP, and the measures shall at a minimum guarantee the following:

   a. Develop a list of jobs and positions whose occupants are considered to be politically exposed persons, or use electronic databases - if possible - provided by specialized companies for PEPs to collect information and data.

b. The information required to be obtained from customers to determine whether he is a political person posing risk or a person assigned or previously assigned with a key position by an international organization or is kin of with a PEP, if so, what degree is that kinship.

c. Continuous follow-up to update customer information.

2) Should the exchange company determine that the customer or beneficial owner is a PEP, the additional following measures shall be taken:

a. the preapproval of the company manager on dealing with the PEP shall be obtained prior to initiating a business relationship with said person.

b. Specific procedures must be drawn on dealing with transactions such customers request, information must be updated routinely, and follow up on the transactions shall be maintained.

c. Measures shall be taken to determine sources of funds and wealth.

d. Enhanced and continuous monitoring of the business relationship shall be maintained.

Tenth: Keeping Customer Information (Know Your Customer "KYC")

Exchange companies, for the purpose of gathering information on customer and on beneficial owner (real) prior to executing any transaction, **shall use a form designated for the same**, and keep the documents, data and information collected updated on continued basis and verify their validity through reviewing records on regular intervals proportionate to the level of risk associated with the customer and shall maintain said information throughout the period of the business relationship. Said template shall cover, at a minimum, the following:

a. For Natural Persons:

1. Personal information (name, profession or job, identity document number, nationality and birth date.
2. Average annual income and its sources.
3. Number of transactions expected (monthly, annually).
4. Value of transactions expected (monthly, annually).
5. Nature of transactions requested to be executed for the customer by the company (purchase of foreign currency, external remittances, etc.)
6. All relevant parties shall be named/specified, as well as the beneficiaries on whose behalf the customer requests transactions to be executed.

7. Asking for customer clarification whether he/she currently holds a political or international post, whether he/she did so in the past, the nature of such post, if any, and whether he/she has kin currently in such posts and the degree of kinship, if any.

b. For Legal Persons:

In addition to the aforementioned in (a), the following information shall be collected:

1. Nature and type of activity.
2. Legal form and the commercial registration number.
3. Clarifying and mentioning the name of the authorized manager and all partners.
4. Clarifying and mentioning the volume of the registered capital and the working capital.
5. For shareholding companies, clarifying the names of main owners or shareholders holding 25% or more of the capital.

Eleventh: Continuous monitoring of customer's transactions:

Exchange company shall use automated systems to constantly monitor the customer's transactions, where possible, or have a mechanism to verify that transactions are executed in harmony with the information it has available on the customer and the type of risk identified in connection to his/her transactions, and shall specify the procedures the company adopts to adhere to the above as well as the person(s) assigned to this task as part of the company's approved business procedures.

In addition, the exchange companies shall also take special and exceptional care regarding complex, large, or frequent transactions or deals. Such care is also required for all types of unusual transactions that serve no clear economic goals and purposes, or those incongruent with the customer's activity or with the average sums seen in previous transactions where the company is required to obtain supporting documents, where possible. The compliance officer shall write a report indicating the justification for decision taken, be that executing the requested transaction or notifying the KFIU where the transaction is deemed suspicious.

Twelfth: Terminating the Relationship with the Customer

The exchange company shall terminate the relationship with the customer and consider whether there is a need to notify the KFIU of any specific case in the following situations:

1. Inability to implement the due diligence measures required for the specific customers.

2. In cases where the customer fails to provide any clarifications or information requested from him/her concerning any of the transactions requested which do not match the volume of previous dealings or information obtained earlier regarding his/her activity.

Thirteenth: Relationship with Foreign Correspondent Institutions (Cross-Border Transactions)

1) Exchange company may not establish correspondent or business relationships with shell banks. It is also prohibited to do so with any correspondent financial institution in any foreign country allowing the use of its accounts by shell banks.

2) Exchange companies shall not deal with any correspondent institution without being subject to an authority or regulatory body entrusted with supervising this correspondent to verify its compliance with all the requirements contained in the recommendations issued by FATF.

3) Prior to initiating a business relationship with foreign correspondents or any other relationship, it shall take extra precautions, beyond due diligence, through the following:

   a. Gathering sufficient information about the correspondent financial institution.
   b. Understanding the nature of the operation of the correspondent financial institution to be engaged with.
   c. Evaluating the reputation of the correspondent financial institution to be engaged with, the type and level of supervision it is subjected to, and whether it had previously been subjected to investigations or regulatory measures in connection with money laundering and financing of terrorism.
   d. Evaluating the controls imposed by the financial institutions the company intends to engaged with as correspondents in the areas of (AML/CFT) efforts and taking the necessary procedures to clearly ascertain that their systems in this regard are consistent with the requirements that must be adhered to in accordance with the provisions of all relevant instructions issued by CBK.

4) When an exchange company intends to engage in a contract with any correspondent institution abroad, an integrated written study should first be prepared including the need for such dealings, information collected on this correspondent in accordance with the measures mentioned in Clause (3) above, as well as the following information which shall be obtained from the correspondent:
   a) A copy of the license issued to the correspondent to carry out financial transfers.
   b) A document proving that the correspondent is under the supervision of an authority concerned with combating money laundering and terrorist financing.
   c) An acknowledgment by the correspondent of his full compliance with the requirements of due diligence in accordance with the requirements of combating money laundering and terrorist financing when carrying out the required transactions at the request of the exchange company's customer.

d) An acknowledgment from the correspondent to carry out the transfers required by the exchange company at the request of its customers through familiar methods.

e) An acknowledgment by the correspondent, upon the company's request and within three business days of receiving the request, to submit a copy of all documents proving the implementation of the required transaction or any information related to the execution of a transfer, and a document proving that the beneficiary received the transferred amount, whether by depositing into his bank account or by receiving in cash from the correspondent.

5) Signing contracts with any correspondent institution abroad, including those dealt with previously without a contract, prior to initiating the business relationship that specify the responsibilities of each party (financial institution) concerning compliance with (AML/CFT) requirements in accordance to Item (4) above.

6) All requirements stated above shall be documented and applied to external relationships (cross-border relations) and all similar relations, those to be initiated as well as those already initiated prior to these instructions coming into effect.

Fourteenth: Transactions related to remittances:

1) With regard to the outward external remittances, companies shall have full and accurate information about the transferor, the beneficiary and the purpose of the remittances, and ensure that such information are attached to the electronic transfer or related messages within the payment chain at all stages. In addition, a unique serial identification number should be used for each transaction executed, which shall aid in saving and maintaining the documents related to such transactions, and the information attached to all electronic transfers shall always include the following:

   a) Full name of the transferor (as mentioned in the identification evidencing document of the inquired party).

   b) Account number of the transferor in case the account is used for the transaction.

   c) The Civil ID number and address of the transferor.

   d) Name of beneficiary, at a minimum the first name and family name, and his/her account number, if it is the account into which the transferred sum is to be deposited.

2) For inward cross-border remittances, the exchange company shall verify that all information required in paragraph (1) above is included within data and information attached with the remittance. Remittances that do not attach said information shall be monitored and the identity of the beneficiary ascertained, if

that had not been checked before. Such information shall be saved and maintained within the documents evidencing the transaction.

3) Should the exchange company fail to comply with these requirements, it shall abstain from executing the requested remittance.

4) The exchange company shall comply with all requirements relative to freezing or prohibition of dealing with any persons, entities, or groups named in UN sanctions lists in line with UNSC resolutions issued virtue of Chapter VII of the United Nations Charter concerning the countering of terrorism and the financing of proliferation of Weapons of Mass Destruction (WMD), within the scope of addressing electronic money transfers.

5) In case of several cross-border remittances, issued as separate transactions requested through a single order and to be collectively paid to one beneficiary, it is permissible not to apply all above-mentioned requirements for every single remittance where the transferor is concerned, on condition that the remittances show the transferor's account number or the remittance reference number that allows its tracking. The bundled remittances shall meanwhile include all required and accurate information concerning the transferor and full information on the transferee that allows for full tracking within the country where the beneficiary resides.

6) For cross-border remittances, exchange company processing an intermediary element of payment chains should retain all wire transfer information including the originator and beneficiary information.

7) All information and copies of documents relating the electronic transfers should be made available by the ordering exchange company within three business days of receiving the request either from CBK or KFIU, whether that information is available with the company or that is provided by previous correspondent who executed the transfer.

8) The exchange company shall have in place risk-based business procedures to identify the following:

   a) Cases for executing, rejecting, or suspending the execution of an electronic remittance due to insufficiency of information attached concerning the transferor or the transferee, and the company shall consider whether there is need to notify the KFIU.

   b) The appropriate follow-up action, which might include restricting or terminating the business relationship.

9) The exchange company must execute the transfer issued based on the customer request, within a maximum of the one business day following the date of receiving the request. In the event of non-implementation during this period, the customer must be informed of this, and if he expresses his desire not to continue

the transfer, the company is obliged immediately to refund the value of the transfer including the fees to the customer. Moreover, the exchange company shall follow up remittances processed through its correspondents abroad and verify the beneficiary's receipt of the value of the remittance and inform the transferor, within a maximum of five business days, of the justifications where a remittance cannot be processed.

Fifteenth: Dealing with associations of public interest and charitable institutions

1) When dealing with public benefit associations or charitable institutions subject to the supervision of the Ministry of Social Affairs and Labor in accordance with the provisions of the Law No. 24 of 1962 concerning Clubs and Public Benefit Associations and amendments thereof, the exchange company shall comply with instructions issued by the Central Bank of Kuwait in this regard, and have specific procedures to be followed when dealing with these institutions. Enhanced due diligence measures are also to be implemented since the collection of donations and transfer of sums thus obtained to other parties is considered a high-risk activity.

2) All paperwork and documents shall be provided if any public benefit associations or charitable institutions wants to execute an out-ward cross-border remittance in compliance with Cabinet of Ministers Resolution No. 868 of 2001, issued 14/10/2001.

Sixteenth: Commitments to Reporting the Suspicious Transactions:

1) The exchange company shall conduct background check, investigate, and gather information in the event of suspecting a transaction that may constitute proceeds of crime or may be related to money laundering and financing of terrorism, including all parties related to the transaction, without informing or revealing such procedures to any of the parties. The findings of these investigations shall be documented in printed form and the supporting documents shall be maintained and presented when requested.

2) The exchange company shall notify KFIU, within two business days, of any transaction or attempted transaction (regardless of its value) if it is suspected to be conducted with money constituting proceeds of crime or funds related to money laundering and financing of terrorism or that it is conducted or required to be conducted in these transactions.

3) All staff, directors, and other parties within the exchange company with access to information are prohibited from reporting, whether to the customer or to others, that such notice had been sent and from releasing any information forwarded or to be forwarded to the KFIU. They are also prohibited from revealing that there is an ongoing investigation over suspicion of money laundering or financing of terrorism in connection with transactions executed or were to be executed for customers. This prohibition does not apply to revealing and exchanging information between company manager and staff or with

attorneys, specialized authorities, and the Public Prosecution regarding these transactions.

Seventeenth: Record Keeping Requirements:

The exchange company shall maintain the following documents and records:

1. All documents obtained in line with due diligence processes, including copies of the documents evidencing identities of customers and beneficiaries owner, and the accounting files and business correspondences, and these shall all be maintained for a minimum of five years after the termination/end of the business relationship or the execution of the transaction for any customer.

2. All documents related to local or cross-border transactions, whether those executed or those attempted, which shall be maintained for a minimum of five years after the execution or attempted execution of the transaction, and the records shall be sufficiently detailed to allow for re-creation of all steps of each transaction individually.

3. Copies of the notices sent to the KFIU and connected documents for a minimum of five years since presentation of the notice to the KFIU, so that said documents allow for re-arrangement of the individual transactions in a manner that would enable – should need arise – evidence to be gathered to file suit against criminal activity.

4. The study conducted to identify and assess risks and all connected information for a minimum of five years since the conducting or the updating of said assessment.

Eighteenth: Requirements of Combating Terrorism

Pursuant to the provisions of Article (25) of Law No. (106) of 2013 on Anti-Money Laundering and Financing of Terrorism, all exchange companies shall comply with all provisions of Resolution No. 35 of 2019 issued on 04/08/2019 by the committee formed by the Ministry of Foreign Affairs (the Committee for the Implementation of Security Council Resolutions under Chapter VII of the United Nations Charter on Terrorism and the Financing of Terrorism) regarding the regulations of implementation of Security Council Resolutions under Chapter VII of the United Nations Charter related to terrorism and financing of the proliferation of weapons of mass destruction. The exchange shall also comply with the mechanism issued concerning the procedures to be followed towards implementation of said decision. This shall involve the following:

a. Developing automated systems to ensure full compliance with requirements of decisions issued in connection to countering terrorism and the financing of proliferation of Weapons of Mass Destruction (WMD). Companies may consider seeking the services of specialized companies in connection with names of customers, names of those granted power of agent by customers to

deal with the company, as well as names of beneficiaries owner of requested transactions,

b. No financial or other connected service shall be provided to any individual, entity, or group included listed by the UN Security Council Sanctions Committee under the Security Council resolutions Nos. 1267/1999 and 1988/2011, and listed by the resolutions issued by a committee of implementing the Security Council resolutions established by the Ministry of Foreign Affairs, pursuant to the decision No 1373/2001. This shall apply immediately upon the inclusion of any party in any such list.

Nineteenth: AML/CFT Compliance Officer

1) The exchange company shall appoint a competent Compliance Controller/ officer with the mandate to verify the company complies with requirements of provisions of Law No. (106) of 2013 concerning countering money laundering and combatting the financing of terrorism and its executive regulations, as well as all relevant ministerial decisions and CBK instructions.

2) The compliance controller /officer and his/her assistants within the company shall have the appropriate qualifications and expertise in the areas of countering money laundering and financing of terrorism. The company shall provide the CBK with detailed information of the compliance officer and of those serving in his/her stead during his/her absence, and this shall include the name, qualifications, landline and mobile numbers, and email address. The CBK is to be apprised of any change in the above immediately.

3) A job description shall be drawn for the compliance controller /officer and for his/her assistants and it shall cover their tasks, including the periodical reports required for the review of the company manager and partners to follow up on developments. The job description for each employee shall be initialed in an indication that he/she is fully aware of all the tasks required of him/her.

4) The compliance controller/ officer shall have the authority to work independently, while subordinate to company manager administratively. He/she and other concerned staff shall have direct access to data indicating customer identity and other information connected to due diligence measures, records of transactions, and other relevant information.

5) The exchange companies shall conduct independent thorough scrutiny and examination to ascertain that the compliance officer and his/her assistants perform their tasks in harmony with company policies and controls in connection with countering money laundering and the financing of terrorism, and this shall be included in the company's annual internal audit.

6) The compliance officer must draw up a report to be presented to the company manager or board of directors, should there be one, as well as to all partners concerning efforts exerted to ensure company compliance with provisions of Law No. (106) of 2013 concerning countering money laundering and combatting the financing of terrorism on a quarterly basis at least. Said report shall state all suspicious transactions detected along with their implications and the measures taken by compliance staff to enhance policies, business processes, and company systems and controls with respect to countering money laundering and the financing of terrorism.

Twentieth: Other Requirements

1) The exchange company shall have in place an automated audit system to evidence all its transaction, which enables it to prepare its financial position statements accurately. It shall also adopt internal audit systems befitting the volume of its activity and use serial numbers for all transactions requested by customer, fully executed or otherwise.

2) The exchange company shall commit to implementation of all due diligence measures as indicated in these instructions when dealing with exchange companies/institutions operating in the State of Kuwait but not regulated by the CBK, where such companies/institutions are to be included among the company's customers.

3) When dealing with other exchange companies within the State of Kuwait, the exchange company regulated by the CBK shall comply with the requirements indicated for the signing of contracts in line with requirements for transactions with correspondents. Contracts signed shall specify the types of transactions to be covered and the mutually agreed procedures in this regard.

4) The exchange company may not accept cash sums from customers as payment for execution of transactions valued above KD 3,000 or an equal value in foreign currency within one day. Payments above that sum shall be deducted from the customer's account with any bank or settled by other payment methods allowed by the CBK (cheques, ATM card).

5) There is no maximum transactions value the company can make payment for to its customers using foreign currency or Kuwaiti Dinar within one day, without breach of what is stated in paragraph (4) above for purchases of foreign currency where payment is made in Kuwaiti Dinar. The exchange company shall also issue a bill of sale in the customer's name after implementing all due diligence measures required, and the bill shall indicate the currency sold and the total value of banknotes sold.

6) Where ATM cards are used to pay for a transaction through deduction from a bank account, the exchange company shall verify that the card is issued under the name of the customer requesting the transaction, and where there is discrepancy, an authorization from the person whose name is on the card is

required approving payment for the transaction. The company shall also verify that the beneficial owner is the person requesting the transaction.

7) In line with provisions of Article (13) of Law No. (106) of 2013 on countering money laundering and the financing of terrorism, and in connection with declaring information in this regard, the exchange company shall present all information and documents requested by specialized authorities, each befitting its mandate. This most especially applies to information requested by both the KFIU and the Ministry of Foreign Affairs' committee overseeing the implementation of UNSC resolutions in view of Chapter VII of the UN Charter.

8) The auditors' report prepared for assessment of the internal control system in an exchange company should include an item on his/her assessment of compliance by the company with locally applicable laws, and the relevant ministerial resolutions and CBK instructions promulgated with respect to AML/CFT, and with the company's approved policies and procedures as we all the internal controls.

9) The partners should be informed of the findings of any on-site inspection conducted by CBK in terms of CML/CFT, including the corrective measures that should be undertaken by the company, and the actions taken by the company in this respect.

10) In recruiting its staff, the company shall identify the requirements of integrity, experience and efficiency, and set the rules and procedures to ensure that:
    a. Staff have the expertise necessary for conducting their duties.

    b. Staff have the integrity required for carrying out the various activities of an exchange company.

    c. No person convicted of crimes involving fraud, dishonesty and the like shall not be appointed by the company.

11) The exchange company should have an approved training plan that considers periodic training programs for the new and existing staff in the area of AML/CFT. All the company's partners and the general manager should attend similar programs to stay abreast of the new developments including those relating to the prevailing patterns in AML/CFT, in accordance with the obligations under the Law No. 106 of 2013 regarding Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) and its executive regulations, and all related instructions issued by CBK.

Twenty First: Penalties and Legal Actions

Penalties stated under article (15) of the Law No. (106) of 2013 concerning combating money laundering and financing of terrorism shall be applicable to any exchange company violating these instructions.