Instructions for Regulating Know your Customer Procedures and dealing with him electronically

NO. (7/2021)

Issued Based on the Provisions of Article (65/b) of the Central bank of Jordan Law No. (23) of 1971, as amended, in implementation of the provisions of Clause (3), (4) and (5) of Paragraph (b) of Article (4) of the same Law and based on the provisions of Articles (53) and (55) of the bylaw of Electronic Payment and Money Transfer No. (111) of 2017

Article (1):

These Instructions are called "Instructions for Regulating Know your Customer Procedures and dealing with him electronically" and shall enter into force as of their issuance date.

Article (2):

a. The following words and terms, wherever mentioned in these Instructions, shall have the meanings assigned to each hereunder, unless the context indicates otherwise:

Central Bank:	Central Bank of Jordan.
Company:	Any bank licensed to engage in banking activities in the Kingdom in accordance with the provisions of the Banking Law, as well as any electronic payment and money transfer companies licensed to operate in the Kingdom in accordance with the provisions of the Electronic Payment and Money Transfer bylaw No. (111) of 2017.
Board:	Company's board of directors.
E-Know Your Customer (E-KYC):	Application of know your customer procedures and verify his identity using electronic means for the purpose of establishing a remote banking or business relationship without the need to the customer's presence(face to face) at the company or any kind of its presence or any other third parties, etc.

Customer Electronic Registration:	Arrangements and procedures used by the Company to implement the requirements of E-KYC that lead to accepting the person as a customer at the Company.
Financial or Banking Services:	Any of the services or products provided by the Company to its customers who have been registered electronically.
Electronic Authentication System:	A set of coordinated and integrated elements that contains the electronic intermediaries through which the electronic authentication certificate is issued and managed.
Person:	Natural or legal person desiring to establish a remote banking or business relationship with the Company using electronic means.
Customer:	The Person who is electronically registered and receives financial or banking services from the Company.

b. The definitions contained in the Banking Law, Electronic Transactions Law, Electronic Payment and Money Transfer bylaw, Anti Money Laundering and Counter Terrorist Financing Instructions of Banks and Electronic Payment and Money Transfer Companies shall be adopted wherever provided for herein, unless the context indicates otherwise.

c. The definitions of “Data”, “Information” and “Website” contained in the Cyber Crimes Law shall be adopted wherever provided for herein, unless the context indicates otherwise.

Article (3):

a. The provisions of these instructions shall apply to the banks and companies licensed by the Central Bank to practice the activities of payment services or management and operating of electronic payment systems.

b. The provisions of these instructions shall not apply to exchange companies and other companies licensed by the Central Bank in accordance with the legislation in force, except under special orders issued for this purpose.

c. The provisions of these instructions shall be applied when establishing a remote banking or business relationship with natural persons only as a first stage, provided

that this is allowed for legal persons at a later stage according to a notice issued by the Central Bank in this regard.

Article (4):

a. The provisions contained herein shall be deemed as additional requirements to those contained in the "Anti Money Laundering and Counter Terrorist Financing Instructions" upon implementation of the E-KYC procedures and shall be read therewith as one unit.

b. The Company shall not always classify its electronically registered customers as high-risk customers, taking into consideration all relevant risk factors before determining the overall risk level for the customer and the appropriate level of risk reduction measures to be applied.

c. The Company is not required, in the case of registering the customer electronically, in the context of implementing the E-KYC procedures or provision of financial or banking services, to keep the relevant records or documents in a material form, which shall be replaced by electronic record pursuant to the following provisions:

   1. The electronic record containing any register, contract, record or document made in the context of customer electronic registration procedures or in the context of provision of financial or banking services shall be acceptable and produce the same legal effects as any register, contract or record or document required to be submitted in writing under any legislation, provided that all the requirements provided for in the Electronic Transactions Law and these instructions shall be satisfied.

   2. Electronic signature made in the context of customer electronic registration or in the context of provision of financial or banking services shall be acceptable and produce the same legal effects as the written signature, provided that all the requirements provided for in the Electronic Transactions Law and these instructions shall be satisfied.

Article (5):

Upon implementation of E-KYC procedures, the Company shall obtain and verify all the data, information and documents relevant to the identity and legal position of the persons in a manner that satisfies the requirements of Anti Money Laundering and Counter Terrorist Financing. The efficiency of the said procedures shall be equivalent to the efficiency of the procedures followed in registration of customers in their

presence. In addition, the electronic systems required for this purpose shall be provided and used, so that the Company satisfies the following minimum requirements:

a. Obtaining the person's data and information and copies of the identity proof document and all the documents required pursuant to the instructions in force, including machine-readable paper documents (through scanning or optical or photography recognition) or electronically-readable electronic document (through but not limited to barcode or QR code), with the possibility to modify any of these machine- or electronically-readable data, if necessary, in accordance with the company's risk management policy. .

b. Obtaining the biometrics of the natural person or the representative of the legal person, such as the iris recognition, fingerprint, or face recognition, etc.

c. Using the technologies necessary to conduct liveness detection on the natural person or the representative of the legal person, such as audio-visual communication technologies or other technologies and the ability to determine the date and time of audio-visual communication recording.

d. Using the technologies necessary to detect any forgery or falsification of documents together with using the technologies necessary to prevent manipulation or fraud during the registration process, such as uploading photographs or recorded video.

e. In case of using modern technologies such as artificial intelligence or machine learning or any of the other prediction technologies that enable full or partial identification or verification of a person's identity, ensuring the ability of these technologies to distinguish and detect any cases of forgery or fraud in accordance with the matching percentages determined in accordance with the company's internal policies approved by the board.

f. Verifying the data, information and documents set out in paragraphs (a) and (b) of this Article from neutral and reliable sources, including the competent bodies that issued these documents and proofs these data and information, pursuant to the instructions in force, through connection to and integration with the electronic systems, websites or databases of these bodies –whenever available- in order to ensure:

    1. Matching the documents or data and information obtained therefrom and the data relevant to the biometrics pursuant to the matching percentages determined in accordance with the company's internal policies approved by the board, taking into consideration the results of its risk assessment.

    2. Verifying the validity of documents.

g. Verifying the validity of the person's mobile phone number by making sure that it belongs to the said person by appropriate means, such as sending a one-time password (OTP) to the registered phone number and requesting from the said person to re-enter it on the electronic system during the process of electronic registration.

Article (6):

In the context of customer electronic registration, the Company shall:

a. Satisfy all the requirements of security and protection stipulated in the provisions of the Cyber Risk Resilience Instructions in force, in particular upon connecting to the other electronic systems, websites or databases inside and outside the Company.

b. Satisfy all the technical and technological requirements for the information and communications technology environment stipulated in the provisions of the Technical and Technological Requirements Instructions for Electronic Payment and Money Transfer Companies in force.

c. Satisfy all the requirements and conditions stipulated in the Technical and Technological Outsourcing Instructions for Electronic Payment and Money Transfer Companies in force, if the Company decides to outsource the technical and technological works to a third party, taking in consideration ensuring that the third party to which the technical and technological works are assigned is adhering to the procedures and provisions provided for herein.

d. Provide electronic regulatory compliance systems in order to detect any deficiencies in the E-KYC procedures in consistency with the conditions and requirements set out in these Instructions and in the other relevant legislation.

e. Appoint one or more specialized independent bodies, before actual final launch of customer electronic registration, in order to periodically test, evaluate and review the adequacy and efficiency of the electronic systems and E-KYC procedures provided by the Company or the third party, and to express its opinion regarding the overall risk level under a comprehensive audit program in consistency with the legislation in force, and to provide the Central Bank with a copy of its report no later than (10) days as of the date of its submission to the Company, together with obliging the specialized body, in accordance with the provisions of this paragraph, to immediately inform the Central Bank of any matters that have a negative material impact that it determined during its test, evaluation or review, including any security gaps, material violations, or breaches of the requirements of Anti money Laundering and Counter Terrorist Financing.

Article (7):

The Company shall ensure satisfaction of all the conditions and requirements provided for in the Electronic Transactions Law and in these instructions whether in respect of electronic signatures or electronic records, particularly:

a. When the customer electronically signs an acknowledgment of the validity and accuracy of the data, information and documents provided by him that are included in the E-KYC form and when the customer electronically signs the terms and conditions of the account opening contract.

b. When the customer electronically signs the operations, he makes in the context of provision of financial or banking services.

c. Upon keeping the electronic record made in the context of customer electronic registration provided for in paragraphs (a) and (b) of this Article, which shall be linked to an electronic signature that is protected or authenticated in accordance with the provisions of Article (8) hereof.

Article (8):

The Company shall, when using the electronic signatures system, satisfy the conditions and requirements of protected or authenticated electronic signature, as follows:

a. Relying on an electronic authentication system from an electronic authentication party licensed or accredited for the purposes of implementing the provisions of Paragraph (a) of Article (7) hereof.

b. Relying on the electronic authentication system of the Central Bank for the purposes of implementing the provisions of paragraph (b) of Article (7) hereof.

c. Notwithstanding the provisions of paragraphs (a) and (b) of this Article, until an electronic authentication system is provided, whether by the Central Bank or by any licensed or accredited electronic authentication parties, the Company shall:

    1. Rely on the protected electronic signature system for the purposes of implementing the provisions of Article (7) hereof.

    2. If the electronic authentication system of the Central Bank is available, the Company shall rely on it for the purposes of implementing the provisions of Article (7) hereof.

3. If the electronic authentication system of any licensed or accredited electronic authentication party is available, the Company shall rely on this system for the purposes of implementing the provisions of Article (7) hereof.

d. The company shall continue to adopt the protected electronic signature system to provide financial or banking services to its customers with whom a banking or business relationship has been established outside the context of the customer electronic registration (face to face) in accordance with the company's risk management policy.

Article (9):

In the context of customer electronic registration, the board shall:

a. Verify provision of appropriate governance arrangements that qualify the Company to electronically register the Customer and ensure reflecting them to the Company's policies, in consistency with the corporate governance instructions of every type of companies, in particular the provisions of the Cyber Risks Resilience Instructions in force in this regard.

b. Adopt a comprehensive framework for risks management relevant to customer electronic registration and provision of financial or banking services carried out in this context, and after acceptance of the customer, or inclusion thereof in the general risks framework of the Company, and developing the main strategies for management of these risks and the supporting policies, in a manner that enables the Company, at all times, to address the risks that might arise and minimize the probability of occurrence of significant risks and effectively manage them in a manner that enables the Company to satisfy all the requirements of Anti Money Laundering and Counter Terrorist Financing.

c. Ensure prior determination and assessment of the risks relevant to customer electronic registration or provision of financial or banking services, in particular the risks relevant to money laundering and terrorism financing, cybersecurity risks, and risks of outsourcing to third parties whether such outsourcing is technical and technological or functional; and ensure updating risk assessment at least annually or when the need arises, and documenting the risk assessment process and its results.

d. Ensure development of the measures and procedures appropriate and necessary for risk management and mitigating it to acceptable levels.

Article (10):

The board shall, upon determination of the financial or banking services that the Company is permitted to provide to the electronically registered customers, particularly take the following into consideration:

a. Type, nature and profession of customer, geographical areas, type of the financial or banking services and their distribution channels, customer assessed risk level, the controls and risk mitigations including limits specified for the values or number of transactions, and the other controls, pursuant to the policies adopted by the board and the results of the risk assessment made by the Company.

b. Nature and availability of the electronic signature system in force in accordance with the provisions of Article (8) hereof.

Article (11):

The Company may functionally outsource the procedures of customer electronic registration, including the E-KYC procedures, whether in whole or in part, to a third party, provided that:

a. The Company shall include in its policies approved by the board the main conditions to be satisfied by the third party with which the contract will be concluded and determine the functions that can be outsourced in the context of customer electronic registration, including E-KYC procedures, whether in whole or in part, and the considerations to be taken into account upon taking the outsourcing decision.

b. The third party shall be a qualified company that is permitted by the competent bodies, which issue the documents relevant to the E-KYC requirements, to log into or have access to their electronic systems, websites or databases, for the purposes of checking the validity of these documents, data or information, in a manner that satisfies the requirements of these instructions and the Anti Money Laundering and Counter Terrorist Financing Instructions.

c. The relationship between the Company and the third party shall be governed in writing under a contract that at least covers the following:

    1. The obligations of the Company relevant to Anti Money Laundering and Counter Terrorist Financing and the method of implementation by the third party shall be determined in a manner that ensures satisfaction of all the requirements stipulated in these instructions or in the Anti Money Laundering and Counter Terrorist Financing Instructions.

2. Arrangements of keeping registers and managing data, information, and document and maintaining their confidentiality.
3. Systematic periodic revision of the quality of the data, information and documents collected and documented in the context of E-KYC by the third party in order to ensure its continuity to satisfy the Company's requirements.
4. Clear determination of the cases in which the Company might examine the third party's failure in performance of its duties under the contract and take the necessary action, including termination of the contract, pursuant to the size of these failures and their impact or based on the request of the Central Bank.
5. The Company's right to receive all the data, information and documents relevant to E-KYC procedures from the third party on time.
6. Restricting the third party from disclosing the data, information and documents relevant to E-KYC procedures to the Company or any other entity except in the presence of a prior approval from the customer.
7. Systematic periodic revision of the contracts concluded with third parties and updating the same, as necessary, in order to ensure the Company's continuity to manage the role of third parties accurately and to reflect any necessary updates, if any.

d. Outsourcing to third parties pursuant to the provisions of this Article shall not exempt the Company, in any manner, from its final liability for the third party's implementation of E-KYC policies and procedures and from the Company's satisfaction of the requirements of Anti Money Laundering and Counter Terrorist Financing and any special requirements provided for hereunder.

Article (12):

In the context of customer electronic registration and implementation of E-KYC procedures, the Company must:

a. Inform the Central Bank of satisfaction of the requirements set out in Article (9) hereof.

b. Immediately inform the Central Bank upon occurrence of any technical or technological or functional failures or deficiencies relevant to implementation of the provisions of these instructions and the requirements of Anti Money Laundering and Counter Terrorism Financing, together with determining the nature of the deficiency or failure and its reasons or the breaches and the measures taken by the Company in this regard.

c. Immediately inform the Central Bank and the other related bodies upon occurrence of any incidents or fraud or forgery experienced by the Company or any third party, whether or not any material losses are generated.

Article (13):

The company may update the documents, data or information obtained in the context of customer electronic registration using electronic means and without the need to the customer's presence (face to face) at the company or any kind of its presence or any other third parties, etc.

Article (14):

Upon entry into force of the provisions of these instructions, every Company that is registering its Customers electronically or providing financial or banking services to the Electronically Registered Customers shall adjust its status pursuant to the provisions of these instructions within a period not exceeding six months as of the date of entry into force. The Central Bank may extend this duration for another six months.

Article (15):

If any of the banks or electronic payment and money transfer companies violate any provision contained in these instructions or violate the legislations relevant to their operation, the Central Bank may impose any of the penalties or take any of the measures provided for in the legislation governing their operation. The Central Bank may also prevent these banks or companies from continuing to register the Customers electronically if they fail to adjust their status pursuant to the provisions of these instructions or if the Central Bank finds that customer electronic registration, including implementation of E-KYC procedures, is suffering from significant issues that affect the safety and integrity of the financial or banking Services provided in this context.