Instructions of Anti Money Laundering and Counter Terrorist Financing For Electronic Payments and Money Transfer Companies No. (12/2018) Issued based on the provisions of Clause (4) of Paragraph (a) of Article (14) and Provisions of Paragraph (b) of Article (18) of the Law of Anti-money Laundering and Counter Terrorist Financing (AML/CTF) in force No. (46) For 2007 and Provisions of Article (53) of the Bylaw of Electronic Payment and Money Transfer No. (111) for 2017

Article (1):

These instructions are called the "Instructions of Anti-money Laundering and Counter Terrorist Financing for Electronic Payment and Money Transfer Companies and shall enter into force as from the date of being approved.

Article (2):

A. The following words and phrases herein shall have the meanings assigned to each hereunder unless otherwise connoted by the context:

The Law	:	The Law of Anti-money Laundering and Counter Terrorist Financing in force.
The Unit	:	The Unit of Anti-money Laundering and Counter Terrorist Financing created in compliance with the provisions of the Law of Anti-money Laundering and Counter Terrorist Financing in force.
The Central bank	:	The Central bank of Jordan
The Payment Service Provider	:	The company licensed by the Central bank to practice any activity of payment services including issuance, management, and transfer of electronic money.
Manager and Operator of E-payment System	:	The company licensed by the Central bank to practice any activity of the management and operating of electronic payment systems.
The Company	:	The payment service provider, and manager and operator of the e-payment system.
Business relationship	;	The relationship that emerges between the company and the customer in relation with the

activities and services of electronic payment and transfer of money provided by the Company to its customers.

Ongoing relationship	:	The business relationship that is expected, when emerged, to extend to a non-definite period of time and to include several operations.
The Customer	:	The person who deals with the company whether a natural person, a legal person, a legal arrangement, or a not-for-profit entity.
Occasional Customer	:	The customer who does not have an ongoing relationship with the company.
Beneficial owner	:	The natural person who has ultimately owns the real interest and the business relationship is taking place to his/her interest or on his/her behalf or has full or effective control of a legal person or a legal arrangement and has the right to do a legal act on behalf of either one.
Not-for-profit Entity	:	Any legal person associated in compliance with the provisions of relevant laws for charity, religious, cultural, educational, social or any other similar purposes and is not aimed at realizing or sharing profit from its activity or at achieving a personal interest including the foreign branches of international not-for-profit organizations and entities.
Control	:	The direct or indirect capacity to exercise an effective impact on the actions and decisions of another person.
Executive	:	The Board of Directors member of the Company whether in his/her personal capacity or as a representative to a legal person, general manager of the company, or any employee working for it.

Foreign Politically Exposed Persons	:	Persons who are or have been entrusted with prominent public functions by a foreign country, for example heads of state or of government, senior politicians, senior government, judicial or military officials; or she/he used to be a prominent politician or "VIP" figure of a political party; or senior executives at state-owned companies. These include, as well, relatives of such persons to the first kinship degree minimum or any persons who act on their behalf or hold authorizations issued thereby.
Domestic Politically Exposed Persons	:	Persons who are or have been entrusted with a senior public job in the kingdom such as a prime minister, a judge, a military official, or a senior governmental position; or used to be a prominent politician or a "VIP" figure at a political party; or the senior executives in state-owned companies including relatives of such persons to the first kinship degree minimal or any persons who act on their behalf or hold authorizations issued thereby.
Persons assigned (at present and in the past) with outstanding tasks by an international organization	:	These are members of the senior management; i.e. directors and their deputies and members of the BOD and equivalent positions in an international organization.
Trust Funds	:	These are the legal relationships that are incepted – between those alive or at death– by a person or custodian when assets have been put under control of the person or custodian to the account of a beneficiary or for a certain purpose. However, the assets must be independent assets and not part of the property of the custodian. The right to the assets of the custodian in his/her name or in name

of another person on behalf of the custodian.

Legal Arrangement	:	Direct trust funds or similar legal arrangements.
Reporting Manager	:	An official of the Senior Management of the company appointed for the purposes of reporting operations suspected to be linked to money laundering or terrorist financing and s/he can be the compliance officer.
Electronic transfer	:	Transfer of money from the electronic transfer issuance requester to the beneficiary as an electronic transfer using electronic means via the electronic system licensed or approved by the central bank. This definition applies even if the requester of the electronic transfer issuance is the same as the beneficiary.
Cross border electronic transfer	:	Any electronic transfer where the company issuing the electronic transfer or the company receiving the electronically transferred money operates outside the Kingdom.
Domestic electronic transfer	:	Any electronic transfer where the company issuing the electronic transfer and the company receiving the electronically transferred money operate in the kingdom.
Non-resident	:	The natural or legal person who usually resides or is based outside the Kingdom or this who has not completed one year of residence in the kingdom apart from his/her nationality. However, individuals who have an ongoing economic activity or a permanent residence inside the Kingdom will be excluded from this definition even if they reside intermittently in the Kingdom.

E-payment Account	:	The non-bank account that the e-transfer requester holds and is linked to any payment instrument issued by the company initiating the e-transfer; or, it is the account that the beneficiary from the e-transfer holds and linked to any payment instrument issued by the company receiving the e-transfer; or, the bank account if the recipient of the e-transfer is a bank.
Unique Reference Number	:	A group of numbers and/or letters and/or codes identified by the Company for each e-transfer transaction according to the mechanism of operation of the e-payment system licensed or approved by the Central bank.
Third Party	:	The agency which the company commissions to deliver some or all the operations it is licensed to do.
The Financial Group	:	A group consisting of a mother company or any other type of natural/legal persons who own the control shares and coordinate the functions with the rest of the group to apply or implement supervision (control) of the group in compliance with the core principles alongside the branches and/or subsidiaries subjected to the policies and procedures of anti-money laundering and counter terrorist financing at the level of the group.

B. Wherever they should be stipulated in these instructions, definitions in the effective Law of Anti-money Laundering and Counter Terrorist Financing and the Bylaw of Electronic Payment and Money Transfer will be used unless otherwise connoted by the context.

Scope of Application

Article (3):

The provisions herein will apply to the following:

A. All companies operating in the Kingdom and licensed by the central bank to practice any activity of payment services including the exchange companies licensed to practice any activity of payment services except for e-transfer of money.
B. As much as applicable thereto, all companies operating in the kingdom including banks, and exchange companies that are licensed by the central bank to do any activity of managing and operating the e-payment system.
C. Branches of foreign companies operating in the Kingdom and licensed by the Central bank to practice any activity of payment services. The stricter parameters must be applied, though, to the extent possible in case the requirements of Anti-money Laundering and Counter Terrorist Financing in the country where their headquarters are based differ from the requirements herein. However, the Central bank must be informed of any impediments or restrictions that can control or prevent the implementation of these instructions.
D. Branches of foreign companies operating in the Kingdom and licensed by the Central bank to do any activity of managing and operating the e-payment system or the agencies assigned with managing and operating the internationally used e-payment systems and approved by the Central bank and to the extent these instructions apply to them. However, the stricter parameters must be applied to the extent possible in case the requirements of AML/CTF in the country of their headquarters differ from the requirements herein. The Central bank must be informed of any impediments or restrictions that can limits or prevent the application of these instructions.
E. Branches of companies operating overseas and subsidiaries outside the Kingdom to the extent permitted by the effective laws and bylaws in the countries where they operate. The stricter parameters must be applied to the extent possible if the requirements of AML/CTF in the hosting country differ from such requirements effective in the Kingdom. The Company must implement relevant additional procedures to manage risks of money laundering and terrorist financing

and must inform the Central bank of any impediments or restrictions that can limits or prevent the implementation of these instructions.

Due Diligence Requirements

Article (4):

A. Customer Due diligence means identifying the customer, his/her legal status and the purpose of the business relationship and its nature as well as the beneficial owner (if any). All of these issues must be verified, and continuous follow up of operations under the ongoing business relationship using any of the methods stipulated in legislation as relevant. Moreover, the identifying the nature of future relationship between the company and the customer and its establishment purpose as well as recording and keeping data related thereto.

B. The company should be required to undertake customer due diligence (CDD) measures when:
   1. Starting the business relation or during it.
   2. There is doubts about the veracity or adequacy of previously obtained customer identification data.
   3. There is a suspicion of money laundering or terrorist financing.
   4. Carrying out occasional transaction to the account of non-permanent customers in the following cases:
      a. If the value of occasional transaction or that of several transactions that seem to be interlinked exceeds (10,000) Dinars or its equivalent in foreign currencies.
      b. If the company has doubts that the occasional transaction is suspected to be related to money laundering or terrorist financing apart from its value.
      c. Any e-transfer transactions done by an occasional customer apart from its value.

C. The Company cannot keep anonymous accounts or accounts with fictitious names or to conclude a business relation with persons of anonymous identity or persons with nick or fictitious names or with shell companies/banks. For the purposes of this paragraph, a shell bank is the bank that does not have a physical presence in the country where it was established and licensed thereby; and the bank which does not keep record of its operations; and does not employ one or more persons practicing actual activity and management; and is not subjected to

inspection by a competent supervisory agency whether in the country where it was established or in any other country. A shell company, however, is the company that is used as a conduit for operations without keeping any assets and does not do operations related to its activity even if registered.

Article (5):

A. The Company must apply the due diligence towards customers (both permanent and occasional) whether they are natural or legal persons, legal arrangements, or not-for-profit entities. Their identity must be verified using official documents, data or information. Copies of these must be obtained with the competent employee's signature affixed thereto to prove that they are "Identical Copies", and must be verified via reliable, independent sources. Such a verification includes contacting the competent agencies issuing the official documents proving such data. The available database and websites of such agencies must be consulted to this effect, and setting the appropriate procedures to ensure this.

B. If the company could not apply the due diligence procedures towards customers, it should not complete the contracting procedures or to open an e-payment account, or enter into any business relationship with the customer or to implement any operation to his/her benefit. Thus, the company must terminate the business relation and inform the Unit immediately if it suspects that the operation is related to money laundering or terrorist financing using the form or method approved by the Unit for this purpose.

C. The Company may postpone the procedures to verify the customer's identity till after the ongoing relation has evolved on condition that:
   1. The Company implements the verification procedures as soon as possible.
   2. The postponement procedures are necessary to keep completion of usual operations and no money laundering or terrorist financing risks are present.
   3. The Company fully controls money laundering and terrorist financing risks effectively as well as taking procedures as necessary to manage risks of circumstances in which can take advantage of the business relation prior to the verification process. This includes

establishing limits for the number, type, and amounts of operations that can be implemented before completing the verification procedures.

D. If the company enters into an ongoing relation with the customer before fulfilling the verification procedures as pointed out in Paragraph (C) of this article and the company could not fulfill them, it must terminate this relation and inform the unit in case of a suspected money laundering/terrorist financing act using the form or method approved by the Unit for this purpose.

E. The Company should not resume the due diligence procedures towards customers in case a money laundering or a terrorist financing operation is suspected thus, if the company believes, for logical reasons, that resuming the due diligence process will alert the customer. However, the Unit must be informed using the form or method approved thereby for this purpose.

F. The Company must implement the due diligence procedures with regard to the present customers who deal with it on the date of issuance of these instructions according to relative materiality and risks. Due diligence procedures with regard to present customers must be made in relevant intervals. For instance, when suspecting a money laundering operation attributed to a certain customer; or when there is a substantial change in the customer's activity; or when processing financial transaction with large amounts or using an e-payment account or payment instruments in unusual way; or when a substantial change happens in the mechanism of documenting the customer's information. In addition, the Company must consider if the due diligence procedures were implemented on customers in the past and the date of their implementation as well as the sufficiency of data obtained.

G. The Company must do due diligence procedures towards customers on an ongoing basis including auditing the operations that take place as long as the ongoing relation is existing, in order to ensure consistency of operations implemented with what the Company knows about the customers, their pattern of activity, and the risks they represent as well as the source of funds if necessary. In addition, the documents, data, or information obtained under the due diligence procedures must be

continuously updated and their adequacy ensured. This can be done by reviewing the existing records especially the high-risk segments of customers.

Article (6):

A. for the natural person, the Identity determination procedures must observe the following:

1. The identity determination data must include customer's full name, the date and place of birth, the national number, nationality, permanent residence address, telephone number, business address and nature, the purpose and nature of the business relationship, and all information related to the identity proof document for Jordanians as well as all information related to the passport or any other identity proof document approved by the official authorities for non-Jordanians, the personal identification number and any other information or documents that the company considers as necessary to be obtained.

2. In terms of incompetent persons such as those of minor age, the company must obtain a copy of the original official documents or a duly ratified copy thereof identifying their legal representative.

3. While obtaining a copy of these documents, the original official documents or a duly ratified copy thereof must be obtained to prove truth of the power of attorney in case the dealing of any person or agency with the Company is upon a power of attorney. In addition, the identity of the customer and the agent must be determined and verified according to the procedures of determining the customer's identity and verifying it as stipulated herein.

B. for the legal person, the procedures to determine the customer's identity must observe the following:

1. The data to determine the identity must include name of the legal person, its legal form, names of owners, equity shares, authorized signatories, address of business headquarters, type of activity, capital, date and number of registration, national number of the company, its tax number [TIN], telephones numbers, persons who occupy the senior management jobs and their nationalities, the purpose and nature of the business relationship, and any other

information or documents that the company deems as necessary to be obtained. All of these data, information and documents must be continuously updated.

2. Obtain the official documents or duly ratified copies thereof which prove the existence of the legal person and its legal entity, names of owners and authorized signatories, by verifying Its registration at the competent authorities and the documents and information that necessary for this purpose including the memorandum of association and articles of association, and certificates issued by the Ministry of Industry, Trade and Supply and the Companies Control Department, certificates issued by the Chambers of Commerce and Industry . In addition, an official certificate issued by the competent agencies must be obtained if the legal person is registered outside the country.

3. Obtain copies of authorizations issued by the legal person to the natural persons who represent it and the nature of their relationship with it, and identifying the authorized natural person and verifying his/her identity according to the procedures to verify the customer's identity as stipulated herein.

4. Obtain information on the provisions that govern the legal person's business including ownership structure and the controlling management. The public shareholding companies shall be exempted from the request of data related to the names of owners and equity shares. It shall be sufficient to request the data of names of shareholders whose shareholding exceeds 10% of the Company's capital.

C. All procedures in Paragraph (B) of this article in terms of determining the customer's identity will apply if it is a legal arrangement (if any).

D. In case of a not-for-profit entity, the procedures to determine the customer's identity must observe the following:

1. The data to determine the customer's identity must include name of the not-for-profit entity, the legal form, headquarters address, type of activity, date of association, names of those authorized on its behalf and their nationalities, telephones numbers, purpose and

nature of the business relationship and any information that the company deems as necessary to be obtained.

2. Existence of the not-for-profit entity and its legal form must be verified by verifying its registration at the competent authorities and the documents and information necessary to prove the same such as certificates issued by the Ministry of Social Development or any other competent agency.

3. Obtain the documents that prove the existence of an authorization by the not-for-profit entity to the natural persons authorized on its behalf in addition to the need to determine the identity of the authorized person and verify the same according to the procedures to determine and verify identity of the customer as stipulated herein.

E. Procedures of determining the beneficial owner identity must observe the following:

1. The company must ask each customer to present a written declaration identifying the beneficial owner who benefits from the relationship to be concluded. The declaration must include, at least, the information to determine the customer's identity.
2. The Company must determine the identity of the beneficial owner and must take reasonable procedures to verify this identity. This includes review of data or information obtained from official documents and data so that the Company will be convinced that it knows the identity of the beneficial owner.
3. In case of a legal person, the procedures to determine the beneficial owner identity must observe the following:
    a. Identity of the natural person (or persons), if any and who has an actual equity share that controls the legal person.
    b. If there is any doubt in terms of determining the identity of the natural person or if being unable to identify him/her according to the above (a) clause, the Company must determine the identity of the natural person who has control on the legal person via other methods.
    c. In case of not identifying any natural person while applying the above (a) and (b) clauses, the Company must identify and take reasonable procedures to verified identity of the relevant natural

person who occupies the position of a senior administrative official at the legal person.

4. If the customer is a legal arrangements:
   a. Trust Funds: the identity of testator, the custodian, or parent (as relevant) and the beneficiaries or category of beneficiaries for each other natural person practicing effective and actual control of the fund.
   b. Other types of legal arrangements: identity of persons who occupy equivalent positions or similar thereto.

Article (7):

A. The Company must categorize its customers as per the risk level related to money laundering or terrorist financing while observing the following:
   1. The extent to which the operations that the customer does consist with his/her activity.
   2. The extent to which the use of e-payment and transfer instruments or orders is diversified, the interrelation between them and their average transactions
   3. The risk factors resulting from evaluating the information and data obtained from customers under the due diligence procedures including the risks of customer type, risks of countries or geographical areas, and the risks of products, services and operations or distribution channels.
   4. Any other factors that the company considers as necessary to identify the risk level of customer.

B. The Company must put in place the necessary procedures to deal with the risks pointed out in Paragraph (A) of this Article as relevant to those levels of risk. However, the customer categorization according to the risk level must be reviewed periodically or in case changes take place and require such a review.

Article (8):

A. In cases of low risk of money laundering or terrorist financing, the Central bank can resolve, upon special orders issued to this effect, the transactions that need to be done or the customers who require simplified due diligence procedures to be taken when determining

the customer's identity and the beneficial owner as well as the verification thereof. However, such procedures must be relevant to the low risk factors as per the limits allowed within the international recommendations and standards as well as the best international practices, which present examples to low risk customers or operations and any international controls or local requirements in this respect.

B. Simplified due diligence procedures cannot be taken in case money laundering or terrorist financing acts are suspected or in case of circumstances with high-risk implications.

Article (9):

In addition to due diligence requirements stipulated herein, the Company must implement enhanced due diligence procedures in any of the following cases:

A. Towards high risk customers in respect of money laundering or terrorist financing operations:
   1. High-risk customers include: Foreign Politically Exposed Persons representing risks, non-resident customers, persons affiliated to countries that do not implement recommendations by the Financial Action Task Force or they do not sufficiently implement them; or countries which the Financial Action Task Force calls on taking procedures against them.

   2. The Company must take the following procedures with regard to high-risk customers mentioned in clause (1) of this paragraph.
      a. Put in place a special system for risk management that signifies if the customer or this who represents him/her or the beneficial owner is among those categories.
      b. Obtain approval of the director general, regional director or his/her deputy or this who she/he authorizes before the establishing a relation with those categories or resume such a relation in in case of existing customers when these instructions are issued, This approval must also be obtained when discovering that a customer or an beneficial owner has been enlisted in any of those categories.

c. Take adequate procedures to know the sources of wealth or assets of customers or beneficial owner who fall under any of those categories.
d. Monitor precisely and continuously the dealings of these customers with the Company and do enhanced due diligence on the business relationships and the operations to take place with any of them.
e. Take necessary procedures to identify the background of circumstances surrounding any business relationships and the complex and big operations that follow unusual pattern and has no clear economic or legal purpose and take place with any of those categories. Results of this process must be recorded in the company's records.

3. In case of domestic politically exposed persons representing risk and persons are or have been entrusted with prominent tasks by an international organization, clause (2 /a) of this Paragraph will be implemented. In case of a high-risk business relationship with these persons, procedures mentioned in clauses from (2/b) to (2/d) will be implemented.

B. Indirect dealing with customers and in this respect, the company must put in place the necessary policies and procedures to avoid risks related to abuse of indirect dealing with the customers which do not take place face-to-face. Such policies and procedures must be effectively implemented especially the ones that use modern technologies such as online transactions, mobile phone applications, or the use of the e-payment systems, instruments and channels. The company must ensure that the level of verifying the customer's identity and activity in such a case is equal to the special verification procedures of direct dealing with the customer.

C. Unusual operations that represent the big or complex operations at an unusual level benchmarked with the customer's dealings and his/her activity, or any operation of an unusual pattern and lacks a clear economic or legal vindication. Or a group of low-value operations that seem to be interlinked and in total they represent a big operation of an unusual pattern for the customer's activity. Accordingly, the Company must do analysis and studies required to verify the sources of assets and any other procedures necessary to

verify the nature of operations, with the need to maintain records of their own regardless of the decision taken in respect thereof.

D. Dealing with foreign companies and in this respect the Company must obtain approval from the director general or the regional director to initiate a business relationship after identifying nature of the foreign company's activity and its reputation in AML/CTF. The company must make sure that the foreign company is subjected to effective supervision and control by the supervisory authority in its homeland and that it has adequate procedure of AML/CTF.
E. Any operation that the central bank or the company deem as high risks of money laundering or terrorist financing operations.

Article (10):

A Third party must adhere to due diligence procedures towards customers of the Company and the final responsibility for such procedures towards customers remain to be of the Company's. Provided that the following requirements must be fulfilled:

A. The Company must determine the identity of a third party and verify it according to procedures stipulated herein to determine identity of the customer and verify it.
B. The Company must observe that the third party implements the due diligence requirements stipulated herein towards customers, and observe the requirements of supervision and record keeping taking into consideration the information available with regard to the level of risks in the third party's country.
C. If third party based outside the Kingdom, the company must ensure that the third party is subjected to regulation, oversight, or supervision and that it is subjected in its country to AML/CTF legislation and it has an applicable policy as well as adequate controls in this respect. Procedures must be taken, as necessary, to verify if any action has been taken against it in this respect and necessary documents must be made available in the Company's headquarters to prove that.
D. The Company must take adequate steps to ensure that the copies of the documents to determine identity of the customer and other documents required for due diligence towards customers will be presented by the third party once requested and without any delay.

E. The Company must keep an updated list of third parties it has contracts with and that this list is accessible for relevant authorities and can immediately retrieve from it the information necessary and as relevant to determine the customers' identity and verify it prior to initiating or continuing the relationship.
F. The Company must inform third parties of its AML/CTF policy and monitor their adherence thereto.
G. The Company can rely on third parties from the same financial group in order to implement the due diligence procedures stipulated herein. provided that, the elements in paragraphs (A) to (F) of this article in addition to elements hereunder whilst final responsibility for the due diligence measures towards customers remains that of the Company relying on the third party:
    1. The financial group fulfills requirements of due diligence towards customers and keep records as well as AML/CTF programs in line with the relevant content herein.
    2. A competent supervisory authority monitors the implementation of due diligence requirements towards customers and that AML/CTF records and programs are kept by the entire financial group.
    3. Reduce any high risks of countries in a sufficient manner via financial group AML/CTF policies.

The Financial Group and External Branches

Article (11):

If the Company is part of a financial group, the group must be required to implement AML/CTF programs at the whole group level and which must apply, as relevant, to all branches and subsidiaries that the group holds a majority of shares therein. These programs must include the following measures:

A. Set policies and internal procedures and controls as well as relevant arrangements with regard to the following:
    1. Compliance management (including appointment of the compliance officer at the management level).
    2. Relevant examination procedures to ensure high efficiency criteria when appointing the employees.
B. Put in place a continuous training program for the employees.

C. Create an independent audit unit to test the system.
D. Set policies and procedures to exchange information required for the purposes of due diligence towards customers and management of money laundering and terrorist financing risks.
E. Provide the information related to customers and operations from branches and subsidiaries for the functions of compliance and audit and/or AML/CTF at the level of the group. These can include information of analysis of unusual operations or activities and can inform of reporting the operation to the Unit if necessary for the purposes of AML/CTF and risk management.
F. Present sufficient guarantees with regard to confidentiality and the use of exchanged information as well as ensuring that the customer is not alerted.

E-transfers of Money

Article (12):

First: Scope of Application:

A. Provisions of this articles will apply to domestic and cross border e-transfers which value exceeds seven hundred Dinars or their equivalent in foreign currencies.
B. Notwithstanding what is stipulated in Paragraph (A) of this Clause, the Company will be committed to ensure that all e-transfers less than seven hundred Dinars or their equivalent in foreign currencies include all the information of the requester of e-transfer and the beneficiary of such transfer as stipulated in this Article. However, it is not necessary to verify the accuracy of such information unless there is a suspected money laundering or terrorist financing operation.
C. The following will be excluded from the provisions of this article:
    1. Any e-transfer resulting from an operation done using the credit or pre-paid payment instruments to purchase goods or pay in lieu of services as long as the number of the payment instrument accompanies all the transfers resulting from the operation. However, when using the credit payment or pre-paid instruments as a means of payment to do a transfer from one person to another, this operation will fall within the scope of implementation of the provisions in this Article and the information required must be included in the transfer.

2. E-transfers and settlements where the requester and recipient of issuance is the same company and acts to its own account.
3. Domestic e-transfers taking place within the national switch system for payment using the mobile phone on condition that those e-transfers include number of the e-payment account or the unique reference number which allow tracking the operation to identify the e-transfer requester or beneficiary. The company issuing the e-transfer or director of the national switch system for payment via the mobile phone must be able to provide the company receiving the e-transfer or the official competent authorities with all the required information within three business days as from the date of receiving the application to obtain the same. They must be able to promptly respond to any order issued by the competent official agencies that require them to avail such information for their review.

Second: Commitments of the Company Issuing the E-transfer

A. The Company must obtain the following information for the purposes of processing an e-transfer:
   1. Information of the e-transfer issuance requester on condition that they include: full name of the e-transfer issuance requester, number of the e-payment account (if any), his/her address, the national number for Jordanians or the personal number, number of passport or any other ID proof document approved by competent authorities for non-Jordanians and their nationalities.
   2. Information of the beneficiary of e-transfer on condition that they include: full name of beneficiary, number of the e-payment account (if any).
   3. The purpose of transfer and the relationship between the requester of the e-transfer issuance and the beneficiary from it as well as a declaration by the e-transfer issuance requester that she/he is the actual issuer thereof.

B. If there is no e-payment account for the e-transfer issuance requester or the beneficiary of the e-transfer, the Company must give a unique reference number identifying the operation via its electronic system in order to track the operation.

C. The Company must apply due diligence procedures for the requester of e-transfer issuance and verify all information according to the elements and procedures stipulated herein prior to implementing the e-transfer.

D. The Company must attach to the e-transfer all the data necessary for its processing and must keep them entirely.

E. In case several e-transfers are processed for the same e-transfer issuance requester within one e-transfer file, it is sufficient that the Company attaches the e-payment account number for the e-transfer issuance requester or the reference number identifying the operation in case there is no e-payment account therefor. This applies to each e-transfer separately and the e-transfer file must include, in general, the information required for the requester of e-transfer issuance and the beneficiary (beneficiaries) of e-transfer in a manner that enables full tracking of such information by the agency receiving the e-transfer to the account of the e-transfer beneficiary.

F. Notwithstanding what is stipulated in paragraph (E) of this clause, the company must ensure that the non-routine e-transfers are not sent within the same e-transfer file in cases that can increase risks of money laundering or terrorist financing.

G. If the e-transfer is domestic, the company must ensure that the information attached thereto include all the information of the e-transfer issuance requester and the beneficiary therefrom. Otherwise, the company must provide such information to the company receiving the e-transfer via other methods on condition that:

1. The Company includes the e-payment account number or the unique reference number for the e-transfer operation in order to enable tracking of the operation to identify the e-transfer issuance requester or the beneficiary therefrom.
2. The Company must be able to provide the company receiving the e-transfer or the competent official authorities with all the required information within three days as from the date of receiving the request to obtain them.
3. The Company must be able to immediately respond to any order issued by the official competent authorities that require the Company to make such information available for their review.

Third: Obligations of the Company Receiving the E-transfer

A. The Company must put in place effective systems to detect any missing information provided for in paragraphs (A) and (B) of the Second Clause including procedures of post or immediate monitoring whenever possible.
B. When handing over the amount of e-transfer to its beneficiary, the Company must obtain information of the beneficiary including his/her full name and nationality, venue of residence, and the relationship between the e-transfer issuance requester and beneficiary as well as a declaration by the beneficiary on the beneficial owner from the e-transfer. In addition, due diligence procedures towards customers must be taken and the identity of the beneficiary and the actual beneficiary from the e-transfer (if any) must be verified if not so verified beforehand. The information of the e-transfer must be fully kept.
C. The Company must implement effective procedures based on the assessed risk level when dealing with e-transfers where the information of the e-transfer issuance requester or its beneficiary are not completed. These procedures include the request of information not completed by the company issuing the e-transfer. In case such information are not obtained, the Company must take the necessary procedures according to the risk level assessment including declination of the e-transfer. Provided that, this must be an indicator used by the Company to assess the extent to which there is suspicion of that operation and report to the unit immediately.
D. If the beneficiary from the e-transfer is a not-for-profit entity, the Company must ensure that the entity obtaines the official approvals required for receiving the money according to effictive legislation especially in terms of e-transfers coming from outside the Kingdom.

Four: Obligations of the Intermediary Company

A. If the Company participates in processing the e-transfers without being the issuer or the recipient thereof, it must ensure that all information attached to the e-transfers accompany the transfer when done.

B. If the Company could not keep the information attached to the e-transfer for technical and technological reasons, it must keep all the attached information as received for five years apart from

completion/missing of such information, and in a way enable the company to provide the information available for its to the company receiving the e-transfer within three days as from the date of being requested.

C. The Company must take reasonable procedures that correspond to the automatic processing of e-transfers in order to identify the e-transfers that lack the information required about the e-transfer issuance requester or the e-transfer beneficiary. The Company must, also inform the company receiving the e-transfer of missing information about the e-transfer issuance requester or the beneficiary from the e-transfer when processing the transfer.

D. The Company must put in place effective policies and procedures based on the assessed risk level when dealing with the e-transfers where there is incomplete information on the e-transfer issuance requester or beneficiary. Among such procedures, requesting completion of incomplete information from the company issuing the e-transfer. In case of not receiving such information, the company must take procedures as necessary according to the assessed risk level including declination of the e-transfer. However, this must be an indicator used when the Company assesses the extent to which there is a suspected operation and report it to the Unit immediately.

Fifth: General Provisions

A. The Company must adhere to all requirements and terms in this Article whether the e-transfer is processed directly by the Company or via a third party.

B. If the e-transfer issuance requester and its beneficiary are customers for the same company, the Company must obtain all information of the e-transfer issuance requester and beneficiary in order to identify the extent to which it is necessary to submit a suspect act report (SAR) and report to the Unit if there is an operation suspected to be linked to money laundering or terrorist financing using the form or method approved by the Unit for this purpose.

C. Comparing the names and tabs within the e-transfer messages with the lists of penalties stated in Article (18) herein or any other penalty lists issued upon special instructions by the Central bank. The obligations of

those resolutions related to those lists must be implemented including freezing the assets.

Record Keeping

Article (13):

A. The Company must keep the records and documents related to the domestic or international operations it implements including the e-transfers and the results of any analysis done. These must be kept for five years at least as from the date of completing the operation or terminating the relation as relevant.
B. The Company must keep the records and documents related to customers due diligence and the records and documents proving ongoing relationships that it obtains when implementing the obligations stipulated herein. However, these must include original documents or duly ratified copies thereof in a form accepted for courts in compliance with effective legislation in the Kingdom for five years at least as from the date of completing the operation or terminating the relation, as relevant.
C. The company must keep the records and documents stipulated in Paragraphs (A) and (B) of this Article in a form that allows reconstruction of individual operations including amounts and types of currencies used (if any). The same must be availed when needed as an evidence to the prosecution of a criminal activity and to enable response to request by the Unit and competent official authorities of any data or information completely and promptly especially any data showing if the Company has an ongoing relationship with a certain person during the past five years and provide information on the nature of the relationship.

Internal Procedures and Controls

Article (14):

The Company must put in place a convenient internal system including the internal policies, procedures, and controls that must be made available to manage and mitigate risks of money laundering and terrorist financing. The system must be tested for effectiveness and must include the following:

A. A clear policy for AML/CTF including identification, assessment, understanding, stopping, monitoring and effectively regulating money laundering and terrorist financing risks including risks of customers, countries or geographic areas, modern technology, products, services, operations, systems instruments and channels of e-payment and transfer used by the Company to deliver its activities, and approve it by the board or regional director of the foreign company branch and must be updated on a continuous basis.

B. The risk assessment processes must be documented whilst observing all relevant risk factors prior to identifying the overall risk level and the adequate level for the procedures to be implemented to mitigate risks. However, the categorization of those risks must be reviewed and updated every two years or once there are changes that require this. Suitable mechanisms must be provided to inform the competent authorities, upon their request of the identified risks.

C. Detailed written procedures of AML/CTF that accurately identify the duties and responsibilities in line with the approved policy, law, bylaws and instructions issued in compliance therewith including these instructions.

D. Put in place the systems needed to categorize customers as per the risk level in light of the information and data availed for the company, these systems must be reviewed on a continuous basis.

E. Assign independent and qualified staff within the internal audit function and provide them with sufficient resources to test the internal procedures, policies, and controls of AML/CTF.

F. A suitable mechanism to verify adherence to effective AML/CTF instructions, policies, and procedures by the staff stipulated in Paragraph (E) of this Article and the Reporting Manager. Provided that the privileges and responsibilities among them must be coordinated.

G. Assign the Reporting Manager and another replacement for her/him in case of absence and inform the Unit in case either of them has been changed. They both must have adequate qualifications.

H. Assign privileges of the Reporting Manager on condition that they include at least what can enable her/him to do her/his functions independently and in a manner to secure confidentiality of information she/he receives and the procedures she/he implements. For this

purpose, s/he must be able to have access to records and data needed to examine and review the system and procedures that the Company puts in place for AML/CTF.

I. Assign the competencies/ duties of the Reporting Manager on condition that they include the following at the minimal level:
   1. Receiving information and reports on unusual operations or those operations suspected to be related to money laundering or terrorist financing. Such information and reports must be examined and relevant decision must be made with regard to reporting the information to the Unit or keep them; if kept, the decision to do so must be justifiable.
   2. Provide the Unit and competent authorities with the data related to operations suspected to be related to money laundering or terrorist financing and any other information requested therefrom. Access by the Unit and competent authorities to relevant records and information must be availed so that they can do their functions.
   3. Keep all the documents and reports s/he receives.
   4. Produce periodical reports to be submitted to the board on the unusual operations or those operations suspected to be related to money laundering or terrorist financing.

J. Put in place relevant procedures when appointing employees; and when appointing them, it must be ensured that they were not convicted with any offence involving breach of honor or trust unless and they were not criminalized for a money laundering or terrorist financing case.

K. Put in place continuous training plans and programs for employees in the field of AML/CTF and keep the records of the delivered training programs for five years at least. Those programs must include the following:
   1. Texts of the Law, bylaws, and instructions issued in compliance therewith.
   2. Techniques of money laundering and terrorist financing and how to detect them.
   3. Procedures of reporting operations suspected as related to money laundering or terrorist financing.

4. Internal policies, principles, procedures, and controls used by the Company for AML/CTF based on the risk level.

Reporting Operations Suspected to be related to Money Laundering or Terrorist Financing

Article (15):

A. If any administrative staffer in the Company has doubt that the operation to be implemented is suspected to be related to money laundering or terrorist financing, s/he must immediately inform the Reporting Manager.
B. The Reporting Manager must immediately report to the Unit the operations s/he doubts to be related to money laundering or terrorist financing whether such operations are implemented or not. Reporting must be in the method or form approved at the Unit and without notifying the suspected person or stopping the payment instrument or the payment account that belongs to her/him.
C. The Reporting Manager will provide the Unit and competent agencies with data related to operations suspected to be related to money laundering or terrorist financing and any other information s/he is requested to provide. The Unit and competent authorities access to relevant records and information must be facilitated so that they can deliver their tasks.
D. The administrative staffer shall be prohibited from disclosing the report to the Unit directly or indirectly or via any method whatsoever. S/He shall also be prohibited from disclosing any of the reporting procedures taken for the operations suspected to be related to money laundering or terrorist financing or any information and data related thereto.
E. Every one having access or learning of any information directly, indirectly or by virtue of her/his job or work is prohibited from disclosing any information provided or exchanged in any from whatsoever in compliance with the provisions of Law, bylaws and instructions issued in compliance therewith including these instructions.
F. The Company must prepare files of operations suspected to be related to money laundering or terrorist financing where it keeps copies of notifications of such operations as well as the data and documents related thereto. These files must be kept for five years at least as from

the date of notification or till a final irrevocable judicial verdict has been issued with regard to such operations whichever is longer.

General Provisions

Article (16):

A. The Company must identify and assess the money laundering and terrorist financing risks that can emerge from developing new products or operations including the new mechanisms for service delivery or that can emerge from using modern technologies or technologies in the process of being developed in relation with both the new and existing products.
B. The Company must assess risks before launching or using new products, operations, or technologies, and must take measures as needed to manage and mitigate risks.

Article (17):

The Company must incorporate in the agreement signed with the external auditor a text needed for the external auditor to ensure that the Company is implementing these instructions and the extent of sufficiency of the policies and procedures of the Company in this respect. Results of this must be provided in his/her report and s/he (the Auditor) must immediately inform the Central bank of any breach of such instructions once detected.

Article (18):

While observing the provisions of instructions issued pursuant to with the provisions of Law, the agencies subjected to the provisions herein must implement the obligations stipulated in the relevant mandatory international resolutions which the Central bank or the competent agencies serve the company in this respect.

Article (19):

If the Company breaches any of the provisions herein, it will be liable to penalty or procedure(s) or more of penalties and procedures provided for in the effective AML/CTF Law or the effective e-payment and transfer bylaw.

Article (20):

AML/CTF Instructions for Payment Services via the Mobile Phone No (1/2014) for 2014 must be nullified as from the date of approving these instructions. Payment Service Providers via Mobile Phone participating in the national switch system for payment via the mobile phone will adhere to the provisions herein as from the date of being approved.

Governor

Dr. Ziad Fareez