No.: 10/6/18942

Date: 4/5/1444 Hijri

Corresponding to: 28/11/2022

Regulating Open Finance Services Procedures Instructions

NO. (12/2022)

Issued pursuant to the provisions of Article (65/b) of the Central Bank of Jordan Law No. (23) Of year 1971 and its amendments, Article (99/b) of the Banking Law No. (28) of year 2000 and its amendments and Article (55) of the Electronic Payment and Money Transfer Bylaw No. (111) of year 2017.

Article (1):

A. These instructions is called " Regulating open Finance services procedures Instructions NO. (12/2022)", and they shall be enforced from the date of their issuance.

B. Every company that have already provides open finance services shall reconcile according to the provisions of these instructions within one year from its effective date, and the Central Bank may extend this period.

Article (2):

A. The following terms and expressions shall have the meanings assigned thereto below wherever mentioned in these instructions, unless the context indicates otherwise:

The term/ expression	The meaning
Company	Any bank licensed to engage in banking activities in the Kingdom in accordance with the provisions of the Banking Law, and any Electronic Payment and Transfer

	of Funds company licensed to operate in the Kingdom in accordance with the provisions of the Electronic Payment and Money Transfer Bylaw No. (111) of 2017.
Board	The Board of Directors of the company and those with same equivalent positions
Senior Executive Management	Includes the general manager of the company or regional manager, deputy general manager or deputy regional manager, assistant general manager or assistant regional manager, Chief Financial Officer "CFO", Internal audit manager, Chief Risk Officer "CRO", Chief Compliance Officer "CCO" and any other employee in the company who has an executive power parallel to the aforementioned powers and is directly reporting to the general manager.
Application Programming Interfaces (APIs)	It is a set of rules, specifications, protocols and tools necessary to create an intermediate interface between different software application and allows them to communicate and facilitates the process of interaction between them.
Customer's account	A financial account for the customer with the company that contains the customer's data according to the nature of the company's business.
Customer's data	Any information or data about customers, their accounts, or any of their transactions within the company
Open Finance Services	Services that aim to enable the company's customers to securely share their financial data with the Third Party Providers (TPPs) to provide value-added financial services and products to them through API technology.
Account Information Service Provider (AISP)	The entity that owns the technical ability and is authorized by the customer (subject to the customer's explicit consent) to access the data/ information of his/ her account within the company and use it to build and provide value-added services by processing this data. This party also provides an alternative access point to multiple sources of data other than those points owned by the company.
Payment Initiation Service Provider (PISP)	The entity that has the technical ability and is authorized by the customer (subject to the customer's explicit consent) to either pass a payment transaction request only and/ or to make a payment on behalf of the customer.
Third Party Provider (TPP)	The entity that uses the Application Programming Interface (API) to access customer data in order to provide value-added financial services and products to customers through API technology. These include, but are not limited to, Payment Initiation Service Providers (PISPs) and/ or Account Information Service Providers (AISPs).
Participant	The party covered by the open finance services ecosystem (they are the company and Third Party Providers (TPPs))
Customer's explicit consent	A prior written consent or its equivalent in accordance with the relevant legislations from the customer (account holder) authorizing the company to share his/ her data.

B. The definitions mentioned in the Central Bank Law, the Electronic Transactions Law, the Banking Law, and the Electronic Payment and Money Transfer Bylaw and any related legislations issued by the Central Bank shall be adopted wherever stated in these instructions, unless the context indicates otherwise.

C. The provisions contained in the Instructions for Regulating Know your Customer Procedures and dealing with him electronically NO. (7/2021) are considered additional requirements to what was stated in these instructions and should be read with them as one unit.

D. The provisions contained in these instructions are considered additional requirements to what was stated in the AML/CFT instructions and should be read with them as one unit.

Article (3): Scope, Application Mechanism and Stakeholders

A. With observance to the provisions mentioned in Paragraph (B) of this Article, the provisions of these instructions shall apply to all banks operating in the Kingdom and electronic payment and money transfer companies licensed in the Kingdom.

B. The branches of foreign banks/ electronic payment and money transfer companies operating in the Kingdom shall comply with these instructions to the extent applicable to them, or by the guides and policies issued by their headquarter (the mother bank/ company) or by the regulatory authority in their home country, whichever is more achieving to the objectives of these instructions. In case that the instructions issued by the mother bank/ company or by the regulatory authority in the home country achieve more the objectives of these instructions on the branch, then the branch must provide the CBJ with supporting documents to prove this, taking into account to not conflict with the legislations in force in the Kingdom. In case of any conflict, the branch shall inform the CBJ and the mother bank/ company of such matter, provide the necessary clarification of such conflict, and obtain the Central Bank's approval on rectifying such conflict.

Article (4): Governance

A. The Board shall have the following responsibilities and duties:
   1. Ensuring the existence of appropriate and effective internal control systems and follow them up by taking into account the understanding of the main risks related to open finance services facing the company and ensuring that the necessary procedures are taken to identify and control these risks.
   2. Adopting the open finance services policy and its amendments.

B. The senior executive management shall have the following responsibilities and duties, each according to his/ her position:
   1. Supervising the development and implementation of the open finance services policy, reviewing it and ensuring its periodic updating.
   2. Ensuring that the opinion of the company's Compliance Department is obtained before contracting with the Third Party Provider (TPP).
   3. Ensuring that the company's business continuity and disaster recovery plans include potential failure and breach scenarios for dealing with the Third Party Provider (TPP) and testing them periodically.
   4. Ensuring that the relationship with the Third Party Provider (TPP) is organized by clear and explicit written contractual agreements that define the roles, tasks, responsibilities and rights

of both parties; the confidentiality, privacy and security of information and non-disclosure thereof; and determine the provisions regarding the termination of the contract between them.

5. Ensuring obtaining the customer's explicit consent in accordance with the applicable laws and instructions related to open finance services, including:
    a. When giving the Third Party Provider (TPP) access to his/ her account or any of his/ her data.
    b. For services whose nature requires the storage of customer data with a Third Party Provider (TPP).
6. Ensuring that all activities and services that the Third Party Provider (TPP) is authorized to perform or provide are reviewed, and that the Board is regularly notified of the risks that may arise therefrom.
7. Ensuring the training, education and awareness of the company's employees about the relevant business to be provided by the Third Party Provider (TPP), and how it relates to their business.
8. Immediately informing the Central Bank of any breach or violation of the laws, regulations, and instructions in force, or of any negative developments during the contracting procedures with the Third Party Provider (TPP) that would negatively affect the company and the company's procedures.

Article (5): Open Finance Services Policy

A. The company is committed to establish the open finance services policy so that it is documented and approved, and covers all security elements related to it. The policy shall be based on the best international practices in the regard and is compatible with the company's information security and cybersecurity policy. The policy must include, at a minimum, the following:
    1. Developing detailed and clear work procedures to regulate dealing with the Third Party Provider (TPP).
    2. Data, information, processes and services that are allowed to be available to the Third Party Provider (TPP).
    3. The basis for contracting with the Third Party Provider (TPP) and the minimum requirements that must be met by the Third Party Provider (TPP) before entering into any contractual relationship with it.
    4. The basis for evaluating the Third Party Provider (TPP) on their ability to use technical solutions capable of interacting with the programs and systems used by the company without any substantial modifications to their systems.
    5. Technical standards and security controls to be followed when dealing with any Third Party Provider (TPP).

6. An appropriate mechanism for continuous monitoring and auditing of the Third Party Provider (TPP) in accordance with the terms and conditions of the agreement signed between the company and the Third Party Provider (TPP).
7. The roles and responsibilities of those involved with the company in dealing with the Third Party Provider (TPP).
8. The basis for assessing the risks of dealing with the Third Party Provider (TPP) and the mechanisms and controls for managing and mitigating them.

B. The company is committed to publish the most important provisions of the open finance services policy, which are not considered confidential, on its approved official channels.

Article (6): Risk Management

The company shall identify, manage and monitor any risks that may result from contracting with the third party provider (TPP) and include them within the comprehensive risk assessment framework of the company and update it, taking into account the following:

A. Determining the sensitivity degree of the information assets and data accessed by the Third Party Provider (TPP).
B. Analyzing and evaluating the impact of dealing with the third party provider (TPP) on the company's risk profile and on achieving its objectives, and documenting and including them in the company's risk register.
C. Evaluating the overall security and operational risks associated with dealing with the Third Party Provider (TPP) and defining the company's role and responsibility in managing them, and documenting this assessment and the acceptable level of risk.
D. Developing a plan to mitigate the security and operational risks that may result from contracting with the third party provider (TPP).
E. Developing key risk indicators to monitor the level of risks related to dealing with the Third Party Provider (TPP) to ensure that the risk appetite and the degree of risk tolerance are not exceeded.
F. Developing a methodology for classifying payment operations based on the risks that these operations may be exposed to and on their being commensurate with the number of customer authentication factors used for customer authentication when performing payment operations.

Article (7): Contracting with a Third Party Provider (TPP)

A. When contracting with a third party provider (TPP), the company shall take into consideration the following at a minimum and within the limits of the contract concluded between them:
    1. The existence of a clear written contractual agreement between the customer and the Third Party Provider (TPP) that defines the roles, duties, responsibilities and rights of both parties.

2. The existence of a security and information protection policy, business continuity plans, and response to cybersecurity incidents at the Third Party Provider (TPP) and ensuring their effectiveness.
3. The Third Party Provider (TPP) shall appoint an external, independent, and specialized party to conduct vulnerabilities assessment at least once every 6 months, and penetration testing at least once a year or after any radical change to it.
4. Ensuring the ability to audit and supervise the Third Party Provider (TPP).
5. Ensuring the ability to determine the minimum and maximum fees charged by the Third Party Provider (TPP) in accordance with the orders issued by the Central Bank.
6. The Central Bank shall have the right to inspect the Third Party Provider (TPP) within regarding the open finance services they provide by the authorized employees of the Central Bank or any external party appointed by the Central Bank at the expense of the company. The Company and the Third Party Provider (TPP) shall cooperate with them to enable them to fully conduct their business.

B. The company shall notify the Central Bank within (15) days as a maximum from the date of contracting with a third party provider (TPP) and after terminating the contract with it.

Article (8): Application Programming Interface (API) requirements

The company shall allow the Third Party Provider (TPP) to access data and customer accounts, using the Application Programming Interface (API), to enable them to provide open finance services to customers, so that the company guarantees the availability of the following as a minimum:

A. Provide, develop, maintain and configure at least one API for Third Party Providers (TPPs) whether it is intended solely for the Third Party Providers (TPPs) or for the interface used for the company's customers.
B. Ensure the identity of the Third Party Provider (TPP) attempting to access data and accounts available by the company.
C. The ability to block data and accounts from those who are not authorized to access them, and to provide the necessary protection controls against any attempts to cyberattacks or to manipulating them.
D. Maintain confidentiality and security of the company and customer data.
E. Use appropriate and robust encryption algorithms when exchanging data and information via the API with the Third Party Provider (TPP).
F. The API shall be appropriate to the nature of the tasks to be performed by the Third Party Provider (TPP).
G. Recording the access of the Third Party Provider (TPP) to customer’s accounts in the access logs of the company and the access logs of the Third Party Provider (TPP) as well as the operations that take place on them, and the possibility of referring to them when needed and specifying the periods of their retention in accordance with the legislations in force in this regard.
H. Ensuring the security of communication sessions between the participants and the customer.

I. Ensuring the retention of the logs of communication sessions between the participants and the customer in accordance with the relevant legislations.
J. Ensuring that the duration of the communication sessions is as short as possible and that the sessions are terminated upon completion of the required work.
K. Ensuring that the company is able to prevent/ stop the Third Party Provider (TPP) from unauthorized access to, storage or processing of data for purposes other than providing the agreed services.
L. Existence of controls to manage customers' access to the services provided by the Third Party Provider (TPP).
M. The Company shall define key performance indicators and operational objectives for the service to measure the availability and performance of the Application Programming Interface (API) provided to the Third Party Provider (TPP), which shall be transparent and be at least of the same level of the indicators, availability, performance and objectives of the company's customized interface available to the company's customers.
N. Ensure that the services provided by the Third Party Provider (TPP) do not affect the services and reputation of the company.
O. Ensure that the failure or inefficiency of the interface dedicated to Third Party Provider (TPPs) does not affect the provision of services by the company.
P. Ensuring that all technical specifications for any of the interfaces are documented to define a set of procedures, protocols and tools necessary for Third Party Providers (TPPs) to allow their programs and applications to interact with the company's systems.
Q. Informing and coordinating with the Third Party Provider (TPP) about any change in the technical specifications of the Application Programming Interface (API), so as to ensure that the services provided by it are not interrupted.
R. Provide a testing platform to enable the Third Party Providers (TPPs) to test their software and applications used to provide open finance services, so that no confidential information is shared through this platform.
S. Ensuring that customers’ data cannot be read by any unauthorized employees of the participants.
T. When designing the Application Programming Interface (API), the company shall include strategies and plans for emergency response in the event of a failure in the operation of the interface or a breakdown in its systems, taking into consideration the following:
    1. The emergency response plans shall include communication plans to inform the Third Party Providers (TPPs) of the necessary procedures to restore service according to the possible and available alternative options immediately.
    2. Agree with the Third Party Providers (TPPs) on a mechanism for reporting API issues.
    3. Notify the participants in the open finance services system of this.
U. The Company shall consider the following when exchanging data and/ or information with the Third Party Provider (TPP):
    1. Providing the Account Information Service Provider (AISP) with the same data and/ or information from the specified customer account and the payment transactions associated

with it, which are available to the customer using the open finance services when requested directly.

2. Providing the Payment Initiation Service Providers (PISP) with the same data and/ or information about the initiation and execution of the payment transaction that is provided to the customer using the open finance services when the transaction is initiated directly from the company.
3. Providing the Payment Initiation Service Providers (PISP) with whether the amount necessary to carry out the payment transaction is available in the payer's account or not.
4. In case that an error or an unexpected event occurs during the exchange of data, the company shall send a notification to the Third Party Provider (TPP) to explain the cause of the unexpected event or error.
5. Designing the API so that the Third Party Provider (TPP) has access only to the data that they have permission to read or process, and that these access rights are appropriately documented, verified, and reviewed periodically (at least twice a year).

Article (9): Third Party Provider (TPP) Standards and Requirements

The company shall take adequate due diligence procedures to identify the identity of the Third Party Provider (TPP) in accordance with the risks that may result from contracting with them, and verify this identity in the appropriate ways and in accordance with the open finance services policy and the regulations, instructions and legislations in force. In addition to the continuous follow-up according to the contractual relationship concluded with them. The company shall take into account the minimum requirements below when dealing with:

A. <u>Account Information Service Provider (AISP)</u>

1. To be a local company or a branch of a foreign company licensed and registered by the relevant regulatory authorities in Jordan, with a good reputation, experience, technical competence, and the ability to meet the requirements of the company and its customer.
2. To be able to make the secure connection to request and receive data and/ or information on one or more of the customer's specific accounts and the financial transactions associated with them.
3. To be able to provide appropriate and effective mechanisms to prevent access to information except through specific customer accounts and associated financial transactions based on the customer's explicit consent.
4. Ensure that there is no error in sending and routing data and/ or information in the case of more than one communication session.
5. Developing a mechanism for handling customer complaints regarding the services provided by the Third Party Provider (TPP), and defining tasks and responsibilities based on different scenarios and make them available to customers.

6. Ensure the existence of internal and security controls applied by the Third Party Provider (TPP) and their compatibility with the nature and sensitivity of the accessible data.
7. Submit a detailed business plan for the company for the services it will perform in accordance with the contract concluded between them.
8. Ensure that the external auditor of the Third Party Provider (TPP) informs the company of weaknesses in the internal control systems or the decline in the financial performance of the Third Party Provider (TPP).
9. Compliance with the relevant legislations in force in the Kingdom.
10. Have policies and procedures in place to detect and prevent fraud.
11. The ability to save data in safe ways that limit cyber-attack attempts.
12. Protect communication sessions from access to and manipulation of transmitted data by unauthorized parties.
13. Not to request any additional data and/ or information that is not required for the service provided to customers by the AISP.
14. Protecting the data and/ or information that they have been granted the right to access by the company and ensuring that it is not accessed or viewed by unauthorized third parties.
15. Not to use, store or process the data for purposes other than providing the services that they are authorized to provide.
16. Not to store any sensitive data pertaining to customers according to the company's approved classification of data and information related to the customer, except within the limits of open finance services that require such and which are agreed upon with the company.
17. Having appropriate business continuity and disaster recovery plans in line with the company's business continuity and disaster recovery plan, and Testing and updating them periodically.
18. Having an information security and cybersecurity policy in line with the company's policies.
19. Commitment to the policies and procedures for identification and authentication of the customer's identity, provided that they are not less than the level of procedures followed by the company.
20. Ensuring the separation between the data of open finance services and their customers and the data of the AISP and/ or their other customers, and providing the company with the evidence of this.
21. Inform the company immediately upon the occurrence of any breach or any negative events that may affect the company.
22. The Third Party Provider (TPP) shall examine the security vulnerabilities on their systems regarding the relationship with the company and provide the company with the results.
23. If the Third Party Provider (TPP) outsource any of their operations technically - within the scope of open finance services – to external parties, then the TPP shall ensure that they:
    a. Inform the company of the details and scope of this contractual relationship.
    b. Provide assurances that such external party will comply with the terms of the contractual relationship between the company and the Third Party Provider (TPP).

c. Have a business continuity plan that is checked periodically.
d. Apply the security and cyber controls necessary to protect data and not to store it in any way.
e. Ensure their right to monitor and audit the external (third) party.

B. Payment Initiation Service Provider (PISP)

1. The Payment Initiation Service Provider (PISP) must be an entity licensed by the Central Bank to practice the activity of electronic payment and money transfer services in case they provide the payment services process through themselves on behalf of the customer and the services that they will provide shall be within the scope of the license granted to them.
2. Fulfill all the requirements mentioned in Article (9/a) of these instructions.
3. To be able to make the secure connection to initiate the payment from the account of the paying customer and to receive all the information related to the initiation of the payment transaction and all available information related to the execution of the transaction within the company.
4. Providing the company with the same information required by the customer using the open finance services when starting the payment transaction directly.
5. Not to retain keep any funds belonging to the company's customers at any moment or in any way, except for companies licensed from the Central Bank to keep customers' funds.
6. Establish mechanisms to monitor the payment processes that a made through them to detect unauthorized or fraudulent payments for the purpose of implementing security measures, and ensuring that monitoring mechanisms take into account the potential risks.
7. Ensuring that all information arising from the provision of the service is available to both parties of the payment process only, with the customer's explicit consent.
8. Not to modify any data or information obtained by the customer or his/ her company to complete the service.
9. It is not possible to change any information or data related to the payment transaction request that is notified by the customer.

Article (10): Security and Technical Standards for Open Finance Services

The company must define and document the standards necessary for providing open finance services based on the best practices in this field, so that the standards include, at a minimum, the following:

A. Open API Standards

The standards that include communication protocols and architecture type, so that recognized architecture methods are adopted in the development of these interfaces.

B. Data Standards

The standards for data formats, data structures and related data protection and privacy rules, so that recognized data formats in this field are adopted.

C. Security Standards

The standards that define the minimum security requirements and specifications that the participants must meet, including reference to good practices in this field, relevant instructions and applicable laws, and the application of the necessary security and cyber controls, in proportion to the risks, to protect their systems as well as customer data. In addition, as a minimum, the participant must apply the latest and most robust authentication and adequate authorization protocols.

Article (11): Consumer Protection, Data Privacy and Data Protection

A. The company shall take the necessary procedures to aware its customers, as a minimum, of the following:
   1. Information protection.
   2. Open finance services.
   3. Actual commissions and costs related to accessing data and/ or information and carrying out financial transactions.
   4. Terms and conditions of open finance services.
   5. Products and services suitable for them.
   6. Procedures for solving problems related to open finance services.

B. The company shall disclose to their customers, before proceeding with any of the open finance services, all potential risks in a clear, fair, non-misleading and continuous manner.

C. Each company shall publish and keep up-to-date a list of the Third Party Providers (TPPs) with which it engages and the related products and services they will provide.

D. Each contract relating to the implementation or use of open finance services and APIs shall contain a term for acknowledgment by each party that the right of the participants to control the use of such data is limited to the extent of the customer's explicit consent.

E. Participants must put in place appropriate mechanisms to ensure that the data and/ or the customers' private information is not used for purposes contrary to the interests of those customers. Participants must continue to obtain the customers' explicit consent on how their data will be used and they (the customers) need to be provided with mechanisms to revoke consent if they want to withdraw or modify its scope.

F. The company must provide a portal or platform for managing customer approvals based on best practices in this regard, in order to record the approvals obtained, the period for them, the services that were accepted/ canceled and other related matters.

G. Participants must have an appropriate mechanism or procedure in accordance with the legislations issued by the Central Bank in this regard to deal with and resolve disputes related to open finance services (Dispute Resolution Mechanism).

H. The Company shall ensure that the Third Party Provider (TPP) discloses to customers the following:

1. The trade name, address and the Third Party Provider (TPP) contact details, depending on the case.
2. Describe the main characteristics of the open finance service that will be provided.
3. The information or its identifier that must be provided by the customer in order to use the open finance services.
4. The form and procedures for granting the customer's explicit consent to provide the account information service, the initiation of payment service, and the withdrawal and modification of consent.
5. Provisions related to the time and maximum period for implementing the payment service to be provided, if any.
6. Transactions limits, if any.
7. All fees and commissions' details to be paid by the customer to the Third Party Provider (TPP).
8. The means of communication agreed upon between the customer and the Third Party Provider (TPP) regarding the transmission of information and notifications.
9. The terms under which the customer may be Withdrawal from service provided by the Third Party Provider (TPP), if any.

I. The Company shall ensure that the Third Party Provider (TPP) discloses to the customer the following information about preventive and corrective measures when contracting with him/ her:

1. A description of the steps that the customer must take in order to maintain the security of open finance services and how to notify the Third Party Provider (TPP) regarding loss, theft and misappropriation.
2. Secure Procedures, through which the Third Party Provider (TPP) will contact the customer in the event of suspected or actual fraud or security threats.
3. The conditions under which the Third Party Provider (TPP) may suspend or prevent the use of open finance services.
4. Customer's responsibility.
5. The responsibility of the participating parties regarding the implementation or delay in the implementation or non-implementation of open finance services and their responsibility when a cyber-event occurs.
6. How and for what period of time the customer notifies the company holding his/ her account of any unauthorized, improperly initiated or executed wrongly payment transaction. Responsibility, if any, for unauthorized payment transactions within the Company holding the Customer's account for unauthorized execution.
7. Provisions for terminating the contract.

Article (12): Examination and Testing

The company shall prepare a list of use cases for open finance services, specifying the technical and security standards required from the Third Party Providers (TPPs), and shall ensure that the Third Party Providers (TPPs) implement security, technical, and functional testing related to the provided open finance services.

Article (13): General Provisions

A. The Central Bank may at any time request the immediate termination of the contract between the company and the Third Party Provider (TPP) completely or partially, or as it deems appropriate.
B. The Central Bank may issue orders to determine the minimum and maximum commissions charged by companies for open finance services.
C. All companies are mandated to provide open finance services by contracting with Third Party Providers (TPP) if they meet all the requirements mentioned in these instructions.
D. Without prejudice to the responsibility of the Third Party Providers, the company is fully responsible towards the Central Bank for all the actions of the Third Party Providers (TPPs) within the limits of the open finance services provided by them, including their compliance with the provisions of these instructions and any instructions or circulars issued later in this regard.

Governor

Dr. Adel Al-Sharkas