Order N80/04

of 03 May 2023

of the President of the National Bank of Georgia

Tbilisi

On approval of the Rule on Inclusion in Open Banking

In accordance with Paragraph 1(g) of Article 15 of the Organic Law of Georgia on National Bank of Georgia, Paragraph 3 of Article 48 of the same Organic Law, Paragraph 6 of Article 13 of law of Georgia on "Payment System and Payment Service", Paragraph 1 (f^3) of Article 4 of Law of Georgia on Microfinance Organizations and Paragraph 4 of Article 231 of the Law of Georgia on Securities Market, **I hereby order**:

Article 1

Rule on inclusion in Open Banking shall be approved together with its Annex.

Article 2

This order shall enter into force upon publication.

Vice-president of National Bank of Georgia
(Acting President) **Papuna Lejava**

Rule on inclusion in Open Banking

Article 1. General Provisions

1. The Rule on Inclusion in Open Banking (hereinafter - the Rule) defines the necessary requirements that shall be met by a brokerage company, microfinance organization, loan issuing entity, payment service provider, currency exchange point that wants to join Open Banking, as well applicant for registration as an Account information service provider and Payment initiation service provider (hereinafter - Entity). A commercial bank licensed by the National Bank of Georgia is obliged to constantly meet the requirements defined in this Rule, except for the obligation to apply for inclusion in open banking to the National Bank of Georgia and receive appropriate approval.

2. The purpose of this rule, on the one hand, is to regulate the process of inclusion of entities in Open Banking and, on the other hand, to ensure the correctness, reliability and security of services provided by Entities involved in open banking.

3. The Entity which participates in the implementation of the payment initiation service and/or account information service is obliged to comply with the requirements stipulated by the order No. 145/04 of 24 October 2022 of the President of the National Bank of Georgia "On the approval of the statute on uniform and secure open communication standards".

4. The requirements of Articles 6 and 7 of this Rule do not apply to payment service providers, whose registration process is carried out in accordance with the "Rule of Registration and Regulation of the Payment Service Provider" approved by the Order of the President of the National Bank of Georgia.

Article 2. Definition of Terms

For the purposes of this Rule, the terms used have the following definition:

a) Open banking – the immediate exchange of information between different Entities about the user existing in the bases of the Entities, using electronic technologies and the Open Banking standard, on the basis of the user's initiative and consent, in order to offer the customer the Account information service and Payment initiation service;

b) Open Banking Standard – a technical standard developed by the Banking Association of Georgia, based on which information is exchanged between Entities involved in Open Banking.

Article 3. Conditions for inclusion in Open Banking

1. To be included in open banking, the entity:

a) shall meet the criteria set in Paragraphs 1, 2, 4 (in case of payment initiation service) of Article 4 and Clause 3 of Article 5 of this Rule and receive approval for inclusion in Open Banking from the National Bank of Georgia (hereinafter - the National Bank);

b) shall carry out preliminary testing of its services in the test environment of a commercial bank, after the completion of which (also, where relevant, after registration) it can start operating in a real environment.

2. The commercial bank (if applicable), as well as the entity, is entitled to use the test environment of the commercial bank from the moment of submitting an application for inclusion in Open Banking or from the moment of applying to the National Bank for registration as an Account information service provider and Payment initiation service provider.

3. Commercial bank, as an account servicing payment service provider, is obliged to comply with the requirements stipulated by the Order No. 145/04 of the President of the National Bank of Georgia of October 24, 2022 on the "Approval of the Regulation on Unified and Secure Open Standards of Communication", including ensuring the existence of a test environment that includes connection and functionality testing support for the entity and/or other commercial bank to test its software and applications used to offer payment services to customers. It is not allowed to share sensitive information (including sensitive payment data) in the test environment.

Article 4. Criteria for inclusion in Open Banking

1. In order to obtain approval on inclusion in Open Banking an Entity shall meet the following criteria:

a) Submit to the National Bank the information in accordance with Annex N1 of this Rule;

b) In order to ensure confidentiality, integrity and availability of information, including personal data security, shall have implemented information security management system with appropriate policy-procedures. Processes ensuring information security shall serve the protection of information, including sensitive payment and personal data in data-at-rest, data-in-transit, data-in-use and destruction process. Documented policy-procedures of information security shall be submitted to the National Bank;

c) shall submit to the National Bank a relevant schematic description (account information service or payment initiation service), which includes detailed information on the flow of information and/or cash during the service process. If the Entity plans to provide both account information service and payment initiation services, it must submit a separate scheme for each service.

2. In addition to the criteria specified in the first Paragraph of this Article, the Entity is obliged to insure its professional liability and/or provide a bank guarantee in the amount of 50,000 (fifty thousand) GEL in order to compensate for possible material damages caused by non-fulfillment of the requirements established by the Organic Law of Georgia on the National Bank of Georgia and the legal acts of the National Bank issued on this basis. Terms of professional liability insurance and/or bank guarantee terms must be agreed with the National Bank. The National Bank is authorized, if necessary, by a reasoned decision, to require the Entity to submit a professional liability insurance or bank guarantee in an amount greater than that specified in this Paragraph.

3. The requirement specified in Paragraph 2 of this Article does not apply to the Entities that have a minimum supervisory capital requirement and requirements related to supervisory capital established by the legal acts of the National Bank and/or regulatory legislation.

4. If the Entity plans to implement the payment initiation service, in order to obtain approval for inclusion in Open Banking, it is obliged to meet all the following criteria along with the requirements defined in this Article:

a) The Entity must have developed and implemented operational, including cyber security incident management policies/procedures, which must define incident identification, analysis, escalation (if necessary), elimination and monitoring processes to ensure the delivery of services in the minimum time and minimize the negative impact on business operations. The entity must have a major operational, including a procedure for notifying stakeholders of a cyber-security incident. The circle of stakeholders should, at least, include customers, the responsible person(s) determined by the internal organizational arrangement of the entity, the National Bank and, if necessary, law enforcement authorities;

b) the Entity must have a change management practice, which must ensure the analysis, development, testing, approval, implementation and monitoring of changes identified as a result of functioning; As each change is implemented, audits and electronic security logs should be maintained for further investigation and troubleshooting.

5. It is appropriate for an entity that plans to implement payment initiation services to develop a Business Continuity Plan (BCP) for Open Banking services, which includes an Information Technology Infrastructure Disaster Recovery Plan (DRP). Mentioned plan is appropriate to include a description of business continuity arrangements, including clear identification of critical operations, effective emergency/backup plans. It is advisable to test the business continuity plan on a regular basis (at least once a year) in order to assess their adequacy and effectiveness. The entity is advised to review the plan and, if necessary, update it.

Article 5. Obligations of Entities included in Open Banking

1. When performing the Account information service, the Entity included in Open Banking is obliged to:

a) at least once a year conduct penetration testing for all systems connected to the network, including electronic technology and application programming interface (API) security, in accordance with the Open Web Application Security Project (OWASP) standard or other internationally recognized practices in agreement with the National Bank, and submit the test results to the National Bank;

b) agree with the National Bank in advance on any change in the schematic description of the implementation of the account information service defined by subparagraph "c" of the first paragraph of Article 4 of this rule, 30 calendar days before the implementation of the change, and submit the updated schematic description of the implementation of the account information service.

2. When performing the payment initiation service, the Entity included in Open Banking is obliged to:

a) At least once a year, conduct an independent audit of information systems and information security in order to comply with internationally recognized standards (NIST, ISO, COBIT). The Entity must agree with the National Bank on the use of other internationally recognized practices as audit criteria. Said audit shall be performed by an independent and impartial auditor who shall be qualified in information technology (IT) security and payment services and shall be operationally independent from the Entity. The National Bank is authorized to assess the qualification and compliance of the auditor selected by the Entity within the scope of the planned audit and, if necessary, request a change of auditor;

b) at least once a year conduct penetration testing for all systems connected to the network, including electronic technology and application programming interface (API) security, in accordance with the Open Web Application Security Project (OWASP) standard or other internationally recognized practices in agreement with the National Bank. The National Bank is authorized to assess the qualification and compliance of the auditor selected by the Entity within the scope of the planned audit and, if necessary, request a change of auditor;

c) If necessary, at the request of the National Bank, submit to the National Bank the results of testing provided for in sub-paragraphs "a" and "b" of this Paragraph;

d) agree with the National Bank in advance on any change in the schematic description defined by subparagraph "c" of the first paragraph of Article 4 of this rule, 30 calendar days before the implementation of the change, and submit the updated schematic description.

3. Before outsourcing operations, the Entity is obliged to provide the National Bank with information 30 days in advance on the implementation of outsourcing operations.

4. When implementing outsourcing operations, the Entity is obliged to:

a) be fully aware of the risks associated with information technology (IT) outsourcing. Before selecting a service provider, it should be studied to determine its capabilities, reliability, experience and financial status;

b) Ensure that the terms of the contract regulating the parties' relationships, obligations and responsibilities are fully set out in writing. The minimum requirements and conditions specified in the contract shall include performance objectives, service levels, issues related to availability, reliability, scalability, compliance, auditing, security, emergency management, information technology recoverability, backup system processing and service interruption;

c) to have the authority and means to immediately remove and/or destroy the data stored in the service provider's systems defined by the contract, in case of expiration/early termination of the contract with the service provider;

d) have mechanisms for controlling and monitoring outsourcing operations;

e) Maintain a list that lists and describes the third-party information systems it uses.

5. The Entity is obliged to meet the requirements for inclusion in Open Banking set out for in Article 4 of this rule, this Article and other obligations during the entire period of activity.

Article 7. Making decision on inclusion in Open Banking

1. Within 60 calendar days after receiving the application and relevant documentation/information about the inclusion in open banking, the National Bank makes a decision on the Entity about its inclusion in Open Banking or refusal to include it in Open Banking.

2. If the documentation/information submitted by the interested person does not meet the requirements stipulated by this Order, the National Bank will set a period of 30 calendar days for the person to eliminate the deficiency and/or clarify the submitted data. The mentioned period starts from the date of the written notification of the deficiencies by the National Bank to the interested person. From the date of preparation of the letter (from the date of registration of the letter) regarding the identification of deficiencies in the documentation submitted by the Entity or the request for additional information, the time limit provided for in the first paragraph of this Article shall be suspended. It will be renewed after by correcting the deficiencies or submitting the requested additional documentation to the National Bank by the interested person.

3. The National Bank is entitled to request additional documentation/information at any stage of the review of the application submitted by the Entity and to set a deadline for submission of said information/documentation.

4. Failure to fulfill the obligations stipulated within the time limits specified by this Order, as well as the presence of false information in the submitted documentation, are grounds for refusing to inclusion in Open Banking.

5. If the letter prepared by the National Bank regarding deficiencies in the application of the Entity for inclusion in Open Banking or the request for additional information was not delivered to the interested person despite two attempts, after the expiration of 10 calendar days from the date of the second attempt to deliver the letter, the National Bank is entitled to refuse the Entity's inclusion in Open Banking.

6. The National Bank issues an individual administrative-legal act/ an appropriate amendment is made on the decision to include the Entity in Open Banking, in which the Entity's name, identification number and date are indicated along with the mandatory requisites provided for by the Georgian legislation. One copy of the mentioned individual administrative-legal act is provided to the interested person.

7. In case of refusal on the inclusion in Open Banking, the National Bank will inform the interested person in writing about the above, indicating the reason for the refusal on the inclusion in Open Banking.

Article 8. Cancellation of the issued approval on the inclusion in Open Banking

The National Bank is entitled to cancel the approval granted to the Entity on inclusion in Open Banking, if it no longer meets the requirements provided for in Articles 4 and 5 of this Rule and/or the entity is no longer subject to the supervision of the National Bank.

Article 9. Open Banking Registry

The National Bank maintains and publishes on its official website the register of Entities involved in Open Banking and updates it in case of changes.

Article 10. Supervisory measures and/or sanctions

In case of violation of the requirements stipulated in this rule, the National Bank is authorized to apply the supervisory measures and/or sanctions defined by the legislation of Georgia.