

Regulation on remote opening of accounts

1. General provisions

1.1. This Regulation has been developed in accordance with Article 36.2 of the Law of the Republic of Azerbaijan on Banks, Article 13-3.1 of the Law on Postal Service, Article 15.1 of the Law on Non-bank Credit Institutions, and Article 30.6 of the Law on the Securities Market and determines the procedure for the remote opening of accounts at credit institutions, investment firms, the national postal operator, payment institutions (excluding payment institutions that exclusively provide payment initiation services and/or account information services), and electronic money institutions (hereinafter – ‘supervised entities’).

1.2. Where a joint account is opened remotely for two or more people, the requirements of this Regulation apply separately to each of them.

1.3. In the course of remote account opening, the requirements of the Civil Code of the Republic of Azerbaijan, the ‘Regulation on opening, maintaining and closing bank accounts’ approved by Decision No. 04/2 of the Management Board of the Central Bank of the Republic of Azerbaijan dated 4 February 2022, and the ‘Regulation on provision of investment services (operations) by investment companies and banks’ approved by Decision No. 23/1 of the Management Board of the Central Bank of the Republic of Azerbaijan dated 31 August 2021 should be complied with. The information and documents prescribed by those Regulations should also be obtained.

2. Main definitions

2.1. The definitions used in this Regulation bear the following meaning:

2.1.1. remote account opening – the opening of an account through information technology solutions without the simultaneous physical presence of an employee of the supervised entity and the person applying for the remote opening of the account (hereinafter – customer).

2.1.2. account – a bank or other payment account, or a customer account (a depo account and a margin account).

2.1.3. identification of a person – the identification and verification of a customer by means of photographic capture, video recording, or a video call.

2.1.4. video call – the real time identification of a person through information technology solutions in a video-recorded format with the participation of an employee of the supervised entity and the customer.

2.1.5. photographic capture – the identification of a person through information technology solutions in the form of a photographic record without the direct participation of an employee of the supervised entity.

2.1.6. video recording – the identification of a person through information technology solutions in a video-recorded format without the direct participation of an employee of the supervised entity.

2.2. The definition ‘advanced electronic signature’ as used herein have the meaning assigned to it under the Law of the Republic of Azerbaijan on Electronic Signature and Electronic Document.

2.3. Any definitions used in this Regulation have the meanings assigned to them in other normative legal acts and regulations.

3. Remote account opening

3.1. Information technology solutions used by the supervised entity for the remote opening of accounts, including information systems and software, should comply with the requirements established by the Law of the Republic of Azerbaijan on Personal Data and other applicable legal acts.

3.2. Remote account opening through an authorized representative is not permitted, except where the customer is represented by a parent, adoptive parent, or guardian, in the case of a customer who is an individual; or a legal representative, in the case of a customer who is a legal person.

3.3. Where the supervised entity establishes limits in respect of accounts opened remotely, the customer should be informed thereof, and such limits should be observed at the time the account is opened.

3.4. The supervised entity should provide people to whom it offers services with the possibility of restricting the remote opening of accounts upon their written request. Any such restriction may be lifted only on the basis of a written request submitted by the person concerned in the course of their physical presence at the supervised entity.

4. Submission of the application

4.1. An application for the remote opening of an account is submitted by the customer to the supervised entity in electronic form.

4.2. Except as provided in Item 4.3, a customer should submit to the supervised entity the information and documents required by law for opening an account. Where such information and documents are submitted electronically, the information should be authenticated using the customer's advanced electronic signature, and documents should be authenticated using the advanced electronic signatures of the persons who issued or prepared them. Where such information and documents are submitted on

paper, the customer provides original documents or copies certified in accordance with applicable law.

4.3. The customer is not required to submit information and documents to the supervised entity where:

4.3.1. The relevant information and documents obtained during a previous account-opening process are already available to the supervised entity and have been updated through the ongoing application of customer due diligence measures.

4.3.2. the supervised entity has obtained the information and documents required under the 'Regulations on customer due diligence, verification measures in the use of new technologies, identification of risk factors and assignment of customer risk profiles to risk categories (the – CDD Regulations), adopted pursuant to the Law of the Republic of Azerbaijan on the Prevention of the Legalization of Criminally Obtained Property and the Financing of Terrorism (hereinafter – the AML/CFT Law), by relying on third parties in accordance with Article 5 of the AML/CFT Law, or

4.3.3. The supervised entity obtains the relevant information and documents from public information systems with which it has established integration.

4.4. On the basis of the information and documents obtained, the supervised entity carries out verification measures in accordance with the CDD Regulations and conducts a risk assessment in accordance with its internal policies. The circumstances in which the process may be terminated on the basis of the results of the risk assessment is determined by internal policies of the supervised entity.

4.5. On the basis of the information and documents obtained, the supervised entity verifies the customer's legal capacity, authority, and advanced electronic signature in accordance with the applicable legislation.

5. Identification of the Person

5.1. Prior to establishing business processes and control mechanisms for the application of the identification requirements laid down herein, the supervised entity analyzes operational and compliance risks and implements measures, including appropriate security measures, to ensure their effective management.

5.2. Before the identification, the supervised entity informs the customer of the procedures and conditions applicable to the identification process and obtains the customer's written consent to the collection and processing of the personal data required by law for the opening of an account, in accordance with the Law of the Republic of Azerbaijan on Personal Data.

5.3. The identification process commences only in respect of a person who has successfully completed the procedures in accordance with Part 4 of this Regulation.

5.4. Taking into account the risk-based approach, identification is carried out in accordance with internal policies approved by the supervised entity through one or more of the following methods:

5.4.1. identification by photographic capture.

5.4.2. identification by video recording; or

5.4.3. identification by video call.

5.5. The supervised entity should obtain relevant images and recordings resulting from the photographic capture, video recording, or video call. Such images and recordings should meet the following requirements:

5.5.1. The image and audio quality should enable identification and verification of the person throughout the entire process, including through synchronized audio and visual recording.

5.5.2. The image should be in color.

5.5.3. The person's facial image should be clearly visible, unobstructed, adequately illuminated, and free from shadows, and should not be covered by any object, including eyeglasses or any face-covering item.

5.5.4. No third party should be present in the image, nor should any assistance from a third party be used during the process.

5.6. A video call should be conducted in real time and without interruption.

5.7. Methods for detecting the liveness of an individual should be used during the identification process. Liveness detection should be performed by means of software. To establish that the person is a live human being, he/she is required to perform at least three actions in a random sequence. The software analyses whether the person's responses correspond to the instructions provided, as well as the live dynamics of his/her facial image, including natural physiological reactions that cannot be consciously controlled.

5.8. During the identification, the person's facial image is matched by means of software against the photograph contained in the relevant public information system.

5.9. Where a customer already holds an account with the supervised entity and seeks to open an additional account remotely with the same supervised entity, identification of the person is not required. Where the supervised entity considers such account opening risky, it may apply one or more of the methods referred to in Item 5.4 herein.

5.10. During the identification process, the integrity and confidentiality of communications between the supervised entity and the customer, including the full encryption of data transmission channels, is ensured.

6. Conclusion of agreements

6.1. Where the requirements of this Regulation are complied with and the remote account opening is not rejected, the relevant agreement governing the opening of the account is concluded between the customer and the supervised entity.

6.2. The supervised entity provides the customer with a draft of the relevant agreement in a clear and legible form on a durable medium (any instrument which enables information to be stored for a period adequate for its purposes and permits the unchanged reproduction of the information stored).

6.3. The customer reviews the draft agreement and, where he/she agrees to its terms, authenticates the agreement and any related documents using an advanced electronic signature.

6.4. The supervised entity authenticates the agreement using an advanced electronic signature and provides it to the customer on a durable medium. Upon the customer's request, the supervised entity should make available a copy of the agreement concluded remotely in the form chosen by the customer (paper or another durable medium).

6.5. The opening of an account remotely is refused where:

6.5.1. any of the circumstances specified in the legal acts referred to in Item 1.3 herein exist.

6.5.2. the verification conducted in accordance with Item 4.5 herein demonstrates that the account cannot be opened remotely; or

6.5.3. Identification of the person cannot be completed in accordance with the requirements set out in Part 5 herein.

6.6. Where the supervised entity refuses to open an account remotely, it notifies the customer through the contact details provided by the customer (SMS notification, electronic mail, etc.) and states the reasons for the refusal in the notification.

7. Final provisions

7.1. The supervisory board (board of directors) of the supervised entity providing remote account-opening services, (where no such body exists, the executive body of the supervised entity), approves internal policies governing such services. The adequacy of the identification process is reviewed at least annually and with such frequency as may be specified in internal policies of the supervised entity.

7.2. Remote account-opening processes are reviewed where security breaches are detected or occur; amendments are made to relevant legal acts; the supervised entity becomes aware of potential fraud or other misconduct; or deficiencies in the identification process are identified. Such review also takes into account technological developments and experience gained from the implementation of the process. Where necessary, appropriate amendments are made to internal policies.

7.3. All information and documents obtained during the remote account-opening, including video and audio files, images and logs generated during the identification process, are retained in accordance with the procedures and retention periods prescribed by law.