'Approved'
Central Bank of
the Republic of Azerbaijan
Decision № 12/2

13 March 2024

Regulation on the application of strong customer authentication

1. General provision

1.1. This Regulation has been developed in accordance with Article 35 of the Law of the Republic of Azerbaijan 'on Payment Services and Payment Systems' (hereinafter – the Law) and determines the instances when the introduction of strong customer authentication (hereinafter – SCA) is not required, as well as SCA requirements when using services of payment service providers.

1.2. The internal audit service should review the compliance of payment service provider's activities with the requirements arising from this Regulation at least once a year, and the review report should be submitted to the Central Bank no later than January 15 of each year. The internal audit's review report should address the assessment of the requirements of this Regulation, as well as the estimation of fraud rates and compliance with the requirements.

1.3. SCA and other definitions used in this Regulation have the meanings specified in the Law.

2. Requirements for the introduction of SCA

2.1. SCA is applied only following the use of two or more of the elements known to, held by, and owned by the payment service user.

2.2. When applying SCA the payment service user should ensure that:

2.2.1. the elements used for SCA, as determined in Item 2.1 of this Regulation, are not detected, or used by unauthorized persons.

2.2.2. passwords entered by the payment service user (excluding OTPs) are hidden or not fully displayed.

2.2.3. the number of consecutive unsuccessful authentication attempts allowed to the user, which results in the blocking of the payment instrument (restriction of access to the payment account) for transactions conducted with the SCA application, does not exceed three (3). The payment service provider shall notify the payment service user of the blocking, where possible before the last authorized authentication attempt or immediately after the blocking at the latest.

2.2.4. the communication session used during the SCA application is not intercepted and/or changed by unauthorized persons.

2.2.5. the duration of the inactive session does not exceed 5 (five) minutes for mobile applications and 30 (thirty) minutes for Internet banking after logging into the payment account with SCA applied.

2.3. When a payment operation is conducted remotely electronically the payment service provider should apply SCA consisting of the elements dynamically linked to the transaction amount and the payee.

2.4. Cash withdrawals through payment terminals should be provided with SCA.

2.5. If software provided by the payment service provider is used for any SCA element, it should ensure that the relevant software is protected from external intrusion.

3. Exceptions on the SCA application

3.1. The following operations may be conducted without applying SCA:

3.1.1. obtaining information about payment account balance(s).

3.1.2. obtaining information about payment operations conducted during the last 180 (one hundred and eighty) days on payment account(s).

3.2. The exceptions specified in Item 3.1 of this Regulation do not apply if one of the following instances exists:

3.2.1. the payment service user obtains the information specified in Item 3.1 of this Regulation remotely for the first time.

3.2.2. more than 180 (one hundred and eighty) days have passed since the payment service user logged in to the payment account for the transaction specified in sub-item 3.1.2 of this Regulation using SCA.

3.2.3. customer's sensitive payment data are disclosed.

3.3. Payment tools can be added to mobile apps and other software without applying SCA.

3.4. When SCA is applied to log in to the payment account, and a transaction requiring SCA is performed within the same continuous session, that transaction can be performed without SCA.

3.5. A payment service provider may not apply SCA if the amount of a single contactless payment is AZN 100 (one hundred) (or equivalent), and the total daily volume of such transactions does not exceed AZN 500 (five hundred) or equivalent.

3.6. In accordance with the requirements of Item 3.7 of this Regulation, payments included by the payer in the list of 'trusted persons (persons in whose favor the payment transaction is conducted without applying SCA)' and the list of periodic payments can be made without applying SCA.

3.7. SCA should be applied when compiling the 'list of trusted persons' and the periodic payments list or making changes to existing lists.

3.8. SCA may not apply in case of credit transfers between payment accounts serviced by a payment service provider for a payment service user.

3.9. If the number of consecutive remote payment transactions after the last payment transaction performed using SCA does not exceed five, or total amount does not exceed AZN300 (three hundred) or equivalent, a payment transaction in the amount of not more than AZN60 (sixty) or equivalent can be performed without applying SCA.

3.10. In accordance with the requirement of Item 4.5 of this Regulation, payment transactions considered low risk according to Item 4.2 of this Regulation by the payment service provider may be conducted without applying SCA.

3.11. SCA may not apply to payments made through special payment channels created by the payment service provider for legal entities that have undergone necessary security measures.

3.12. Payment transactions related to electronic commerce can be conducted without applying SCA until 1 January 2026.

3.13. To ensure security, payment service providers should perform authentication when conducting the operations specified in Items 3.1, 3.3, 3.4, and 3.12 of this Regulation.

4. Monitoring

4.1. The payment service provider should have a transaction monitoring mechanism in place to detect unauthorized or fraudulent transactions. This mechanism should ensure monitoring of at least the following in each operation:

4.1.1. compromised or stolen authentication elements.

4.1.2. known fraudulent scenarios related to payment service provision.

4.1.3. any malware during the authentication procedure.

4.1.4. if the payment service provider provides the hardware or software used to access the payment account, logs of the usage of the hardware or software.

4.2. Payment operations that meet all the following conditions are considered low risk:

4.2.1. if the fraud rate of the payment transaction estimated as per Item 4.4 of this Regulation is not higher than the those specified in Annex No. 1 to this Regulation.

4.2.2. if the amount of the payment transaction is not higher than the limit of the amount set by the fraud rate specified in Annex No. 1 to this Regulation.

4.2.3. if any of the below is not revealed following a real-time risk analysis by the payment service provider:

4.2.3.1. payment service user’s unusual spending or behavior.

4.2.3.2. unusual information on access to a payment service user's hardware or software.

4.2.3.3. malware at any stage of the SCA application.

4.2.3.4. use of fraudulent scenarios on payment services.

4.2.3.5. a suspicious case in the payment service user’s home country.

4.2.3.6. the payee is in a high-risk country.

4.3. The payment service provider should estimate payment transactions’ fraud rates quarterly no later than the first 5 (five) working days of the following month as per Item 4.4 of this Regulation.

4.4. Whether funds are recovered or not, the fraud rate is calculated quarterly for each type of transaction specified in Annex No. 1 to this Regulation by dividing the total volume of remote and/or fraudulent transactions conducted by the total volume of transactions of that type. Payment transactions performed without applying SCA are also considered in the calculation.

4.5. If the fraud rate for any type of payment transaction exceeds the one specified in Annex No. 1 to this Regulation, the payment service provider should immediately stop using the exception as per Item 3.10 of this Regulation. The exception may be re-used only if the fraud rate for the payment transaction in the following quarter meets the rate specified in Annex No. 1 to this Regulation.

4.6. The issuer can entrust the monitoring of suspicious transactions with payment instruments to the payment system operator on a contractual basis. In this case, the issuer is not exempted from the duty stipulated in the legislation, including the legislation on the prevention of the legalization of criminally obtained property and the terrorist financing and targeted financial sanctions, as well as in the contract concluded with the payment service user.

5. Final provisions

Payment service providers should ensure that existing monitoring mechanisms that detect unauthorized or fraudulent transactions are adapted to the requirements of Item 4.1 of this Regulation by 1 January 2025.

Annex 1
to the Regulation on the application of strong
customer authentication

Amount limit set for using the exception	Referred fraud rate (%)	
	Remote card-based payments	Remote credit transfers
Up to AZN500 (five hundred) or equivalent	0.01	0.005
Up to AZN250 (two hundred and fifty) or equivalent	0.06	0.01
Up to AZN100 (one hundred) or equivalent	0.13	0.015