APPROVED

by the Finance Committee

JSCB Kapitalbank

September 22, 2026
(Protocol No. 34/26)

AMENDMENTS AND ADDITIONS

TO THE RULES FOR COMPREHENSIVE BANKING SERVICES FOR INDIVIDUALS

IN JSCB KAPITALBANK

(*effective from September 22, 2026*)

Tashkent – 2026

I. Introduce the following additions and amendments to the Rules for Comprehensive Banking Services for Individuals in JSCB Kapitalbank (hereinafter -- CBSA):

1.1. Supplement Appendix No. 3 to the CBSA "Procedure for Conclusion and Execution of an Agreement for the Issuance and Servicing of Bank Cards in National and Foreign Currency for Individuals" (hereinafter -- Appendix No. 3 to the CBSA) with Appendix No. 11 "Rules for Servicing Cards When Using Contactless Payment Services" in the wording given in the annex to these amendments and additions to the CBSA.

1.2. Amend and restate clause 9.1 of Chapter "9. Appendices to this Procedure" of Appendix No. 3 to the CBSA as follows:

9.1. "The following Appendices are an integral part of this Procedure *(depending on the form of submission of applications (electronic or written) and conditions, the form of applications may differ from the attached):*

Appendix No. 1 – "Application for Issuance/Re-issuance/Closure of a Card"

Appendix No. 2 – "Online Application for Issuance of a Bank Card"

Appendix No. 3 – "Application for Issuance of a Bank Card" in the interface of the Bank's partner

Appendix No. 4 – "Rules for Using Cardomats"

Appendix No. 5 – "Rules for Compliance with Security When Conducting Operations via the Internet on Bank Cards"

Appendix No. 6 – "Application for Blocking/Unblocking/Resetting the PIN Code of the Card and Connecting SMS Notification"

Appendix No. 7 – "Conditions for Storage and Use of the Card"

Appendix No. 8 – "Procedure for Accepting and Considering Client Applications on Disputed Operations"

Appendix No. 9 – "Application for Purchase of Foreign Currency"

Appendix No. 10 – "Application for Conversion of Foreign Currency into National Currency"

Appendix No. 11 – "Rules for Servicing Cards When Using Contactless Payment Services".

Annex to the amendments and

additions to the CBSA dated September 22, 2026

APPENDIX No. 11

to the Procedure for Conclusion and

Execution of an Agreement for the Issuance and Servicing

of Bank Cards in National and Foreign Currency for Individuals

Rules for Servicing Cards When Using Contactless Payment Services

1. Additional Terms and Definitions

Contactless Payment – a method of performing an Operation by the Cardholder using a Token by closely bringing or touching a Mobile/Smart device with an installed Token to a reading payment terminal or when paying in the Internet space through the interface of the Payment Service.

CBSA – the Comprehensive Banking Services Agreement concluded between the Client and the Bank by the Client's accession to the Rules for Comprehensive Banking Services in JSCB Kapitalbank, which stipulate the terms and procedure for concluding Agreements and providing services to Clients within the framework of remote banking services (RBS). The Rules and Appendices thereto, the Bank's Tariffs, the Public Offer / Accession Agreement, as well as the Application properly completed by the Client, collectively constitute the CBSA concluded between the Client and the Bank;

Agreement – an agreement concluded between the Bank and the Client within the framework of the CBSA, determining the procedure for conclusion, execution, and termination of the agreement for the issuance and servicing of bank cards in national and foreign currency for individuals;

Cardholder (Holder/Client) – an individual (resident, non-resident) in whose name the Bank, in accordance with the Applicable Legislation, regulatory documents of the Central Bank of the Republic of Uzbekistan, the Agreement, has issued a Card.

Card – for the purposes of these Rules, a Card means a Plastic/metal and/or Virtual card, as defined by the Rules for Comprehensive Banking Services in AKB «Kapitalbank»;

DPAN / Token – a unique digital representation of the Card (virtual token) generated in the Payment Service, representing a set of encrypted Card details and used for making Contactless Payments without the physical use of the Card.

Payment Service (Digital Wallet) – software, a mobile application, or a cloud service of a third-party Provider that allows the Holder to add a Card, store Tokens, and use them for making Contactless Payments.

Service Provider – a legal entity (system integrators, payment system operators, and other third parties) that is the developer and/or operator of the respective Payment Service.

Provider Application – a technical system (mobile application) installed on the Holder's device for managing Tokens.

Mobile / Smart Device – any Subscriber device of the Holder (smartphone, smartwatch, tablet, personal computer, fitness bracelet, etc.) supporting wireless data transmission technologies (NFC and similar) and certified by the Provider for working with the Payment Service.

ODCVM (On-Device Cardholder Verification Method) – a method of verifying the Cardholder on the Mobile/Smart device itself using biometric data (facial recognition, fingerprint, iris) or entering a password/graphical screen unlock key of the device.

Rules – these Rules for Servicing Cards when using contactless payment services.

Other terms and definitions used in these Rules have the same meaning as in the CBSA and the Agreement.

2. General Provisions and Equality of Conditions

2.1. The Bank and the Provider provide Holders with the opportunity to create a Token and make payments using the Token.

2.2. The creation of a Token by the Holder in the manner established by these Rules in any Provider Application means the Holder's full familiarization with and unconditional accession (acceptance) to these Rules.

2.3. These Rules regulate the procedure for using Cards when making payments through any Payment Services of third-party Providers supported by the Bank, supplement and are an integral part of the CBSA and the Agreement.

2.4. The Holder makes payments using the Payment Service in accordance with these Rules, the CBSA, and the Agreement.

2.5. A Token can be issued only to a valid Card, which means a Card issued by the Bank, activated, with an unexpired validity period, and not blocked by the Bank.

2.6. Operations performed by the Holder using the Token (DPAN) are equated to Operations performed by the Holder using the Card. The Bank authorizes Operations on Tokens (DPAN) on the same terms as on Cards. The procedure for settlements on Operations performed using a Token is similar to the procedure for settlements on Operations with the Card to which the corresponding Token was created, and is governed by the provisions of the Agreement concluded between the Bank and the Client.

2.7. By accepting these Rules, the Holder confirms their awareness that the creation and subsequent use of a Token is associated with increased risks of loss of funds, access to which is provided by the Token.

2.8. By accepting these Rules, the Client confirms and expresses consent that Operations using the Token are performed without entering a PIN code. The Token is a sufficient identification means for making a Payment by Card.

2.9. The use of facial recognition technology Face ID, Touch ID, Optic ID, or entering a Verification Code is a sufficient means for Authentication and/or Authorization of Operations, with which the Client fully agrees.

3.Procedure for Creating and Activating a Token

3.1. The Bank accepts applications from Holders for the creation of a Token in the manner described in these Rules.

3.2. The Token is created by the Holder to the Card in the Payment Service either using the Provider Application or using the Mobile Application by the Holder creating a corresponding application to add the Card to the Payment Service and the Bank's counter-approval of the possibility of using the Card in the Payment Service.

3.3. When submitting an application for the creation of a Token through the Bank's Mobile Application, the Client familiarizes themselves with these Rules and the Provider's terms. Familiarization with these Rules is confirmed in the manner provided for in clause 3.6 of these Rules.

3.4. When creating a Token to the Card in the Provider Application, the Holder must enter the Card number, Card expiry date, first and last name of the Cardholder (as indicated on the Card), Card security code (CVC/CVV code), and also confirm their consent to the relevant terms of the Provider and these Rules.

3.5. Creation and activation of the Token is possible:

3.5.1. when submitting an online application for the creation of a Token using the Mobile Application -- after the Holder enters the Verification Code sent to the Mobile Phone Number in the Confirmation window of the Mobile Application.

3.5.2. when submitting an online application for the creation of a Token using the Provider Application -- after receiving confirmation from the Bank in the following order:

- The Holder received an SMS code (Verification Code) sent to the Holder's Mobile Phone Number and entered it in the corresponding field of the Provider Application, while the automated verification of the code gave a positive result.

3.6. In order to minimize unused digital data and ensure security, the Bank has the right to automatically or otherwise delete any Tokens created but not activated by the Holder within 30 (thirty) calendar days.

3.7. Upon expiration of the Card's validity period, the Token's validity period terminates.

3.8. The Provider and/or the Bank have the right to refuse the issuance of a Token, block/annul a Token, including in the event of a change in the status of the Card with which the Token was created, including the expiration of the Card's validity period, the Client's refusal to use the Card, and in other cases.

4. Automated Management of the Card Lifecycle

4.1. Blocking, suspension, re-issuance, or closure of the Card for any reason (including loss, theft, compromise, or expiration) may entail suspension or complete deletion of related Tokens (DPAN) in Payment Services in accordance with the rules of applicable Payment systems and/or in the presence of corresponding restrictions (stop-lists).

4.2. The Bank has the right to block, temporarily suspend, or delete a specific Token in a separate Payment Service (for example, if there is a suspicion of compromise of a specific Mobile/Smart device or for anti-fraud purposes), while keeping the Card itself or Tokens on other devices active.

5. Rights and Obligations

5.1. **The Holder has the right:**

5.1.1. to initiate the creation and addition of a Token to a Card issued in the Holder's name in the Payment Service and/or Mobile Application (depending on the availability of the service)

5.1.2. to manage Tokens in accordance with the rules established by the respective Provider, while management of Tokens using the Mobile Application is carried out in the manner provided for by the Rules, the CBSA, and the Agreement;

5.1.3. to block (suspend operations using the Token)/unblock the Token (resume operations using the Token) regardless of blocking/unblocking of the Card;

5.1.4. to delete the Token from the Payment Service;

5.2. **The Holder is obliged:**

5.2.1. when performing operations using the Token, to measure the amount of the planned operation in such a way that when the amount of this operation is subsequently reflected in the Account for settlements on operations with the Card to which the corresponding Token was issued, to prevent unauthorized overdraft/Indebtedness/ to comply with the payment limit established by the Client on the Card;

5.2.2. to store information about the Token (the last four characters of the Token identifier in the Provider Application) and provide this information to the Bank upon the Bank's first request;

5.2.3. to take sufficient measures to ensure the confidentiality of the Token and to prevent the loss of the Mobile device with which the Token is used;

5.2.4. to create Tokens on Mobile devices used exclusively by the Holder;

5.2.5. to take sufficient measures to ensure the information security of the Mobile device, including not installing applications from sources designated by the Mobile device as "unknown" on the Mobile device;

5.2.6. when making payments using the Token, to comply with the obligations established by the Agreement and the CBSA relating to confirmation of completed operations on the Card, including, before signing the slip or cash terminal receipt, checking the correctness of the following data:

a) the amount of the operation indicated in the "Total" column;

b) the currency of the operation;

c) the date of the operation;

d) the Card number;

e) the name of the merchant/service enterprise or bank.

5.2.7. in the event of loss and/or compromise of the Mobile device on which the Payment Service with an activated Token is installed, to immediately contact the Bank to block the Token in the manner established by the Agreement and the CBSA for blocking the Card;

5.2.8. before transferring the Mobile device to a third party or other alienation of the Mobile device from their possession/use controlled by the Holder, to contact the Bank to block the Token;

5.2.9. not to perform actions with the Mobile device that may lead to obtaining any extended user rights with the ability to make changes to the software installed by the manufacturer of the Mobile device.

5.3. **The Bank has the right:**

5.3.1. to establish limits on operations using the Token and inform the Holder about this by posting information on the Bank's official website on the Internet: www.kapitalbank.uz.

5.3.2. to refuse the issuance/re-issuance/unblocking of the Token, to block/annul the Token, including in the event of a change in the status of the Card with which the Token was created, including the expiration of the Card's validity period, the Holder's/Client's refusal to use the Card, in the event of the Client's violation of their obligations provided for by the Rules, the CBSA and/or the Agreement, as well as in the event of the Bank's suspicion of the use of the Mobile device by a third party with the help of which the Token is used, and in other cases provided for in the CBSA and the Agreement.

6. Liability of the Parties

6.1. The Cardholder bears sole and full responsibility for keeping the Card details, OTP codes, and other types of Verification codes confidential, as well as for restricting third parties' access to their Mobile device (for protection against Authentication/Authorization by third parties, etc.). Transferring a one-time password (OTP)/Verification code for linking the Card to the Provider Application to third parties (including cases committed under the influence of deception or threats from third parties) is regarded as a gross violation of security rules by the Client. In the event of the Client's violation of this clause, the Bank is not liable for Operations performed on the Client's Card.

6.2. The Bank has the right to unilaterally temporarily block or completely refuse the possibility of registering the Card in the Provider Application if the Bank has reason to believe

that the linking procedure is being carried out by an unauthorized person or for fraudulent purposes.

6.3. The Bank has the right to refuse a Chargeback in the event that a dispute of a completed expenditure Operation using the Card is received by the Bank by the Client filing a dispute claim with the Bank, if the Operation on the Card occurred in the event of the Client's violation of clause 5.1 of these Rules.

6.4. Until the Holder notifies the Bank of the loss/compromise of the Mobile device with an activated Token or of the compromise of the Token details, the Holder is liable for all operations performed using the Token.

6.5. The Bank is not liable for non-performance or improper performance of its obligations if such non-performance/improper performance is caused by:

a) non-functioning or incorrect functioning of the Provider Application and/or the Mobile device (including, but not limited to, the operating system of the Mobile device and other software installed on the Mobile device);

b) actions and/or decisions of the Provider;

c) actions and/or decisions of state authorities of the Republic of Uzbekistan/the Central Bank of the Republic of Uzbekistan;

d) actions and/or decisions of state authorities of foreign states whose jurisdiction is applicable to the Provider, if such non-performance by the Bank does not contradict the requirements of the legislation of the Republic of Uzbekistan;

e) actions and/or decisions of the payment system within which the Card was issued, using the details of which the Token was created;

f) reasons beyond the control and responsibility of the Bank, including the refusal of a third party (seller, supplier of goods, works, services, etc.) to perform an Operation using the Token, including (but not limited to) the absence of Provider support in a particular state;

g) the occurrence of force majeure circumstances as defined by the legislation of the Republic of Uzbekistan and the CBSA.

6.6. The terms and procedure for using the Provider Application are outside the sphere of responsibility and control of the Bank. All issues regarding the terms and procedure for the Holder's use of the Provider Application are resolved by the Holder with the Provider independently.

Miscellaneous Provisions

7.1. All disputes that may arise between the Bank and the Holder in connection with these Rules are resolved in the manner established in the CBSA and the Agreement.

7.2. Amendments and/or additions to these Rules are made in the manner provided for in the CBSA and the Agreement.

7.3. In the event of amendments (additions) to the Rules, the Bank communicates to Clients/Holders the proposal (offer) on planned changes (additions) no less than 10 (ten) calendar days before the date of their entry into force by posting relevant information on the Bank's Website on the Internet at www.kapitalbank.uz and/or in another manner provided for in the CBSA and the Agreement.

7.4. The Holder has the right to agree (accept) these Rules in any of the following ways:

- sending Orders and/or Information messages to the Bank within the framework of these Rules, as well as the Holder's performance of other actions indicating the Holder's intention to continue executing these Rules, including submitting applications to the Bank for the provision of services by the Bank within the framework of these Rules.

- expression of the Holder's will to agree with the specified proposal (offer) of the Bank in the form of silence (inaction) of the Holder, which means failure to submit to the Bank a written refusal of such changes and/or additions or a written refusal of the Holder to use the Token in connection with the refusal of changes and/or additions.

- Confirmation of the Client's consent to the Rules, changes and/or additions to the Rules is the Client's performance of Operations, and/or the Client's continued use of the Mobile Application and/or the Token, or the absence of a written refusal of the holder to use the Token.

7.5. In order to ensure guaranteed receipt of the Rules by the Holder, the Holder undertakes to independently or through a representative contact the Bank (the Bank's website) for information on changes and additions that are planned to be made to the Rules at least once every 5 (five) calendar days.

7.6. Everything that is not regulated by these Rules is governed by the provisions of the CBSA and the Agreement.

7.7. If any of the provisions of these Rules for any reason becomes invalid, this does not affect the validity of other provisions of the Rules.