Appendix 26
to the Regulations on issuance and servicing
of payment cards for individuals of Jusan Bank JSC

Rules for using a payment card

1. General provisions

1.1. The payment card is the property of the Bank. The payment card is valid until the end of the month and year indicated on it. Card transactions cannot be carried out using expired payment cards or those whose validity period has not yet begun.

1.2. The procedure and conditions for using the payment card are regulated by the legislation of the Republic of Kazakhstan, the Comprehensive Agreement, the operational rules of the international payment systems Visa International, MasterCard Worldwide, and the Bank's internal regulations, including these Rules for using a payment card (hereinafter referred to as the "Rules").

1.3. A client may be denied the execution of a card transaction if it contradicts the requirements of the legislation of the Republic of Kazakhstan, in cases stipulated by these Rules, the Comprehensive Agreement, or the operational rules of the international payment systems Visa International and MasterCard Worldwide.

1.4. The cardholder must store the payment card securely and take measures to prevent its loss or theft. The loss or theft of a payment card (if the cardholder fails to take necessary measures to prevent such loss or theft) may be considered by the Bank as a violation of the terms of the Comprehensive Agreement by the client.

1.5. The Rules use the following terms and definitions. Terms and definitions not specified in the Rules are described in the Bank's Comprehensive Agreement:

1.5.1. Bank Account for a Payment Card (hereinafter - the Account) – a current account linked to a payment card, opened by the Bank for the primary cardholder based on an application for joining the Comprehensive Agreement and a request for card issuance, to carry out card transactions, settlements, and store funds;

1.5.2. Statement – a document containing information about payments, transfers, and other transactions, including those made using the payment card;

1.5.3. Payment Cardholder or Cardholder – an individual authorized to use the payment card under the Bank’s Comprehensive Agreement. The cardholder who owns the account is the client;

1.5.4. Client – an individual who has entered into the Comprehensive Agreement with the Bank and is the owner of the bank account and/or an individual authorized to use the payment card under the terms set by the Bank, or a potential client of the Bank;

1.5.5. Comprehensive Banking Service Agreement for Individuals (hereinafter – the Comprehensive Agreement) – an agreement concluded between the Bank and an individual under which the payment card is issued;

1.5.6. Mobile Application – software installed and running on a mobile device (smartphone, tablet, etc.), providing access to electronic banking services;

1.5.7. PIN Code – a personal identification number, a secret code assigned to the payment card for client identification;

1.5.8. Payment Card – an electronic payment instrument containing information that allows the client to make payments and/or money transfers, withdraw cash, exchange currency, and perform other operations defined by the card issuer and under its terms via electronic terminals or other communication channels;

1.5.9. Entrepreneur – a legal entity or an individual engaged in entrepreneurial activity without forming a legal entity, accepting payment cards for cashless payment of goods and/or services supplied by them;

1.5.10. Trade and Service Enterprise (hereinafter – TSE) – an individual entrepreneur or legal entity accepting payment cards for cashless payment for the goods and/or services supplied. TSEs may impose restrictions on the types of payment cards accepted and transaction amounts;

1.5.11. Stop List – a list of payment card numbers banned from use and subject to confiscation upon presentation for service. The stop list is formed by the payment system based on online (electronic) or written requests from issuers;

1.5.12. 3D Secure (Visa International/MasterCard International Technology) – a technology developed by the international payment systems Visa International and MasterCard Worldwide for additional cardholder authentication by entering a secret password during an online transaction to reduce the risk of unauthorized card transactions and ensure transaction security on the Internet;

1.5.13. CVV2 or CVC2 ("CVV2" – abbreviation for "Card Verification Value 2," "CVC2" – "Card Validation Code 2") – a three-digit identification code (CVV2 for Visa cards, CVC2 for MasterCard cards) used to identify the payment cardholder when making online payments for goods and services. CVV2 or CVC2 is printed on the card's surface or displayed in the Bank's mobile application.

2. Issuance and storage of the Payment Card

2.1. The Bank issues the manufactured Payment Card directly to the Cardholder or to their authorized representative acting on the basis of a power of attorney issued by the Cardholder. Upon receiving the Payment Card, the Cardholder must sign in the designated field on the back of the Payment Card.

2.2. The transfer of the Payment Card for use or as collateral to third parties is prohibited. A Payment Card presented by a person who is not the Cardholder is subject to confiscation.

2.3. The front side of the Payment Card may contain a microprocessor (chip) with encoded information. The microprocessor (chip) is resistant to electromagnetic fields and atmospheric influences; however, mechanical damage (scratches, contamination, creases, etc.) that could damage the chip must be avoided, as this may result in the inability to conduct Card Transactions.
2.4. The back side of the Payment Card contains a magnetic stripe with encoded information, as well as a three-digit CVV2/CVC2 identification code used to verify the Payment Card when paying for goods and services online. This excludes certain card products where the CVV2/CVC2 code is displayed in the Bank's mobile application (in the case of a virtual payment card used exclusively for Card Transactions online, a separate CVV2/CVC2 code is issued). The Payment Card should be protected from adverse factors such as electromagnetic fields (proximity to screens, magnetized or magnetic-containing objects such as keys or magnetic locks on bags), mechanical damage (scratches, contamination, overheating from sunlight), etc., as these factors may damage the magnetic stripe and prevent the execution of Card Transactions.
2.5. Certain rules must be followed to ensure the confidentiality of the CVV2/CVC2 code:

- If the Cardholder writes down the CVV2/CVC2 code anywhere, the Payment Card and the record should be stored separately.
- The Cardholder must not allow anyone to observe the entry of the CVV2/CVC2 code on a computer to prevent unauthorized online payments.

3. PIN Code
3.1. The PIN code for Payment Cardholders is issued upon request via a Temporary Code or through the Bank’s Mobile Application. To prevent unauthorized use, it is strongly recommended that the PIN code be stored separately from the Payment Card.
3.2. The PIN code is strictly confidential and known only to the Cardholder. No individual or entity is authorized to request disclosure of the PIN code from the Cardholder.
3.3. To activate the Payment Card, the Cardholder must conduct an initial transaction by entering the PIN code at an ATM, a POS terminal, a retail banking service branch, or through the Bank’s Mobile Application.
3.4. If the Cardholder opts to set the PIN code via the Bank’s ATM, they must send an SMS from their registered mobile number in the Bank’s system to the short number 7711 with the following text: “epin XXXX” (where XXXX represents the last four digits of the Payment Card number).
3.5. The Cardholder will receive a Temporary Code via an SMS response.
3.6. The Temporary Code is valid exclusively for setting the PIN code at a Bank ATM and must be used within 30 calendar days from the date of issuance.
3.7. The Cardholder must subsequently create and establish a permanent PIN code for the Payment Card.
3.8. The Payment Card will be automatically activated upon the successful establishment of a permanent PIN code.
3.9. For security purposes, it is strongly advised against using easily predictable numerical combinations, such as 1111, 1234, or 9090, when setting the PIN code.
3.10. If the Cardholder opts to establish the PIN code via the Bank’s Mobile Application, they must download the application from the App Store or Play Market onto their mobile device and follow the on-screen instructions.
3.11. To ensure the confidentiality of the PIN code, the following security measures must be observed:

- if the PIN code is recorded in writing, the Payment Card and the record must be stored separately.
- third-party access must be strictly prevented when entering the PIN code on any electronic device.

3.12. When entering the PIN code, numerical values will not be displayed on electronic device screens but will be replaced with placeholder symbols. The Cardholder must exercise caution to avoid errors when entering the PIN code. If an incorrect PIN code is entered three consecutive times (regardless of the time interval or device used), the Payment Card will be blocked by the Bank upon a fourth incorrect attempt. The card may be retained by the ATM or confiscated at a service point until the circumstances are clarified.
3.13. Any transaction authorized via PIN code entry or a signature on a receipt shall be deemed as performed by the Cardholder.
3.14. In the event that the Cardholder forgets the PIN code, the Payment Card must be returned to the Bank for reissuance, as further transactions will not be possible.

4. Use of the Payment Card
4.1. The Bank ensures the servicing of the Payment Card, the uninterrupted operation of systems and electronic devices under its direct control, and takes all possible measures to restore service in the event of interruptions caused by circumstances beyond the Bank’s control.
4.2. All Payment Card service points are equipped with logos of International Payment Systems to inform Cardholders about the possibility of using the Payment Card at a given location.
4.3. The Bank may impose restrictions on the types of transactions and the geographical area in which the Payment Card can be used.
4.4. The Bank may send promotional and/or informational messages to the Payment Cardholder (including for the purpose of preventing unauthorized card transactions and improving service quality) through communication channels established by the Bank (such as SMS messages, push notifications, etc.). No fees are charged to the Cardholder for receiving such messages.

4.5. To conduct Card Transactions, the Payment Cardholder must either present the Payment Card to the cashier at a service point (a Merchant or the Bank) or interact with an ATM in self-service mode.
4.6. QR code technology may be used for card transactions. Scanning a QR code in the Bank's Mobile Application constitutes the Cardholder's authorization of the payment.
4.7. In a standard (contact) transaction, the cashier inserts the Payment Card into the terminal's card reader, enters the transaction amount on the keypad, and asks the Cardholder to confirm the transaction by entering the PIN code on a dedicated keypad. The request is transmitted to the Bank via communication channels. If the correct PIN code is entered and sufficient funds are available in the Cardholder's account, a receipt confirming the transaction is printed in two copies. The cashier hands one copy of the receipt to the Cardholder, who must verify the accuracy of the details. Depending on the type of transaction, the printed receipt may require the signatures of both the Cardholder and the cashier.
For contactless transactions, the Cardholder may independently tap the Payment Card against the terminal's reader to complete the transaction. Transactions conducted via contactless payment may not require PIN code entry or the Cardholder's signature on the receipt, provided the transaction amount does not exceed the limit set at the service point.
4.8. The cashier may request an identification document from the person presenting the Payment Card (as obtained from government information systems). The absence of such an identification document may be grounds for the cashier to refuse to process the Card Transaction.
4.9. An employee of the Bank or a branch may confiscate the Payment Card for further investigation in accordance with the provisions of Section 8 of these Rules.
4.10. Payment for goods and services via the Internet or through mail/telephone orders using the Payment Card shall be carried out in accordance with the procedures established by the Merchant. The Merchant may request the following information: the Card number, the Cardholder's surname and first name, the CVV2 or CVC2 code, and 3D Secure authentication.

5. Use of the Payment Card for Cash Withdrawals
5.1. Cash withdrawals using the Payment Card are carried out at cash withdrawal points or via ATMs of banks that are members of International Payment Systems.
5.2. As a general rule, cash is dispensed in the currency of the country in which the transaction is conducted. In certain countries, the frequency and maximum amount of cash withdrawals using the Payment Card may be subject to restrictions imposed by local legislation or internal regulations of the servicing bank.
5.3. When withdrawing cash at cash withdrawal points, the cashier provides the Payment Cardholder with the requested amount in cash along with a transaction receipt.
5.4. Upon completion of a Card Transaction at an ATM and retrieval of the dispensed banknotes, a receipt is printed upon request of the Payment Cardholder.
5.5. A cash withdrawal transaction at an ATM for an active Payment Card, even if the correct PIN code is entered and sufficient funds are available in the account, may be declined for the following reasons:

- The requested amount cannot be dispensed due to the denomination of banknotes available in the ATM's cassettes. The Cardholder should request an amount that is a multiple of the minimum banknote denomination specified in the ATM's instructions.
- The requested amount exceeds the single transaction withdrawal limit. The Cardholder should divide the requested amount into smaller portions and conduct multiple transactions.
- The requested amount exceeds the available balance of the Payment Cardholder. The Cardholder must also consider any applicable transaction fees as outlined in the Bank's tariff schedule for this type of operation.

5.6. When using an ATM, the Cardholder should be aware that cash or the Payment Card itself may be retained by the ATM if not collected within 10-30 seconds. In such cases, the return of the Payment Card to its Holder may be carried out only by the bank servicing the respective ATM, after determining the reasons for retention and consulting with the issuing bank of the Payment Card. The Cardholder may contact the Bank for assistance in coordinating with the bank servicing the ATM.
5.7. To withdraw cash via an ATM without using the Payment Card, the Cardholder must initiate the transaction independently through the Mobile Application.
Cash withdrawals are conducted exclusively in KZT (Kazakhstani Tenge). If the transaction is performed in a currency different from the account's base currency, the Bank will execute a currency conversion at the prevailing non-cash exchange rate for buying/selling foreign currency at the time of the transaction.

6. Use of the Payment Card for Payment of Goods and Services at Merchants
6.1. In accordance with the rules of International Payment Systems, merchants are not permitted to increase the price of goods and services when accepting the Payment Card as a means of payment compared to cash transactions. The Payment Cardholder should notify the Bank of any such incidents.
6.2. The Payment Cardholder has the right to return a purchase paid for with the Payment Card or cancel a prepaid service, such as returning an airline ticket. In such cases, upon request of the Payment Cardholder and with the merchant's consent, the cashier shall process a "purchase refund" transaction, accompanied by the issuance of a receipt signed by the cashier. The Payment Cardholder must retain the refund receipt. Cash refunds are not permitted.

6.3. The Client is responsible for all Card Transactions conducted using the Payment Card, including payments for goods and/or services at Merchants, online transactions, mail and/or telephone orders, as well as cash withdrawals at cash withdrawal points or ATMs.
6.4. To ensure the security of online transactions, it is recommended that Payment Cardholders make payments only on websites that use 3D Secure technology (indicated by the Verified by Visa or MasterCard SecureCode logo). This technology enables the Payment Cardholder to be authenticated using a special password known only to the Cardholder.
6.5. The Payment Card may be eligible for a bonus accrual program. The terms and conditions for earning and redeeming bonuses are outlined in the Bonus Program Rules for individuals, available on the Bank's website at www.jusan.kz.

7. Blocking of the Payment Card
7.1. In the event of loss, theft, or unauthorized use of the Payment Card, the Cardholder must immediately contact the Bank with an oral or written request to block the Payment Card.
7.2. Contact Center telephone numbers:

- 7711 – toll-free for mobile calls
- 58 77 11 – for 16 cities in Kazakhstan (with six-digit numbering)
- 258 77 11 – for Almaty
- 8 800 080 2525 – toll-free nationwide in Kazakhstan
- (All numbers operate 24/7, including weekends and public holidays.)

7.3. Blocking of the Payment Card is carried out immediately upon registration of a written request by the Bank's branch. When requesting a block via telephone, the Payment Card is blocked instantly, and the caller is notified accordingly.
7.4. The Client assumes all risks and liabilities for consequences, including financial losses, arising from partial blocking of lost or stolen Payment Cards. Partial blocking refers to the Client's/Cardholder's refusal to have the lost/stolen Payment Card details added to the stop-list.
7.5. If a previously reported lost Payment Card is found, the Cardholder must immediately inform the Bank and return the Payment Card. Should the Cardholder use a Payment Card previously reported as lost, they assume full responsibility for any associated risks and must reimburse the Bank for any additional costs incurred in connection with the retrieval of the Payment Card.
7.6. If the Payment Card has operational or geographical restrictions, the Payment Cardholder may submit an oral or written request to the Bank for the removal of such restrictions. The Bank is not liable for any consequences resulting from the removal of restrictions at the Cardholder's request.
7.7. The Bank reserves the right to block the Payment Card in accordance with the terms of the Comprehensive Agreement until any disputed issues are resolved.

8. Withdrawal of the Payment Card by Third Parties
8.1. The Payment Card may be withdrawn at a service point in the following cases:

- The Payment Card has been blocked;
- The presenter of the Payment Card is not its rightful Cardholder;
- The Cardholder forgets the Payment Card at the service point after completing a Card Transaction;
- An incorrect PIN-code is entered three consecutive times (regardless of the time interval and whether different electronic devices were used).

8.2. The Payment Card may be withdrawn by an ATM, a merchant's employee, a branch employee, or an authorized Bank representative. In cases where the Payment Card is withdrawn (except for ATM retention), an official report is prepared.
8.3. The return of a withdrawn Payment Card is performed by the Bank (if the retained Payment Card is delivered to the Bank) directly to the Cardholder upon submission of a written request by the Cardholder.

9. Card Validity, Suspension, and Termination of Use
9.1. The expiration date of the Payment Card (month and year) is indicated on the card. The Payment Card remains valid until the end of the last day of the specified month.
9.2. If the Cardholder wishes to discontinue the use of the Payment Card, they must submit a written request to the Bank and return the Payment Card.
9.3. The Bank notifies the Cardholder about the expiration of their Payment Card at least ten calendar days before the expiration date, in accordance with the terms specified in the card issuance agreement.

10. Reissuance of the Payment Card
10.1. The reissuance of a Payment Card is carried out based on a written request from the Cardholder submitted to the Bank.
10.2. A Payment Card may be reissued under the following circumstances:

- Expiration of the card's validity period;

- Usage in a high-risk area;
- Bank's initiative (e.g., technical defect, etc.);
- Loss or theft;
- Forgotten PIN-code/CVV2/CVC2 or disclosure of PIN-code/CVV2/CVC2;
- Cardholder's initiative;
- Card compromise;
- Damage or demagnetization.

10.3. The old Payment Card must be returned to the Bank upon reissuance. If the Client/Cardholder fails to return the previous Payment Card as required, the Client assumes all associated risks and reimburses the Bank for any additional expenses incurred due to card retrieval.

11. Payment Card Services

11.1. The following services are available to the Payment Cardholder via ATM:

- Cash withdrawal;
- Balance inquiry;
- Payment for service providers (mobile operators, utilities, etc.);
- Money transfers via Visa Direct/MasterCard Money Send;
- Activation/deactivation of SMS notification services;
- PIN-code change;
- Other services (as the Bank expands its card service offerings).

11.2. Activating the SMS notification service allows the Payment Cardholder to receive real-time information about all transactions conducted using the Payment Card.

11.3. Bank account statements are sent to the Payment Cardholder via email upon submission of a written request to the Bank.

12. Dispute resolution

12.1. The Cardholder is advised to keep transaction receipts for tracking account expenditures and resolving potential disputes.

12.2. The Bank provides the Cardholder with account statements and copies of other relevant documents, including those confirming the accuracy of debits from the Account, in accordance with the laws of the Republic of Kazakhstan and the Bank's internal regulations. These documents are provided upon request and may be subject to applicable Fees.

12.3. For any disputes, the Cardholder must submit a written request to the Bank. If the claim is accepted, the Bank represents the Cardholder before the Payment Card System. If the dispute is found to be valid and the transaction is determined to be unauthorized, the Bank restores the disputed transaction amount to the Account. However, if the claim is deemed unfounded (i.e., if unauthorized use cannot be proven), the Payment Card System may impose penalty fees, which may exceed the amount of the disputed transaction. The Bank has the right to debit the Account for such penalties without additional consent from the Cardholder. The Bank informs the Cardholder of the preliminary results of the investigation within fifteen (15) calendar days from the date of the written request. If the claim is deemed valid, the Bank reimburses the disputed amount to the Cardholder's Account. If reimbursement is denied, the Bank provides a written explanation stating the reasons for rejection. If additional information from third parties or further investigation is required, the Bank reviews the claim within thirty (30) calendar days for transactions conducted within Kazakhstan and within sixty (60) calendar days for transactions made abroad.

12.4. If the Bank identifies transactions as unauthorized or if the Client reports unauthorized transactions, the Bank reserves the right to dispute such transactions in accordance with the operational rules of international payment systems (Visa International/MasterCard Worldwide), even if no formal written request is submitted by the Client.

12.5. Any written claims related to cash withdrawals from the Bank's ATMs or account deposits via the Bank's self-service terminals are reviewed by the Bank in accordance with internal policies and the applicable laws of the Republic of Kazakhstan. The Bank may provide a response in person, via email, or through other available communication channels.

13. Security measures

13.1. The Cardholder must observe the following security measures when using the Payment Card:

13.1.1. Do not disclose or share the following information with third parties, including Bank employees:

- PIN code;
- CVC code;
- Login/password for the Mobile Application;
- 3D Secure password;
- SMS confirmations with one-time passwords.

13.1.2. Do not write down the above data on paper.

13.1.3. Monitor all messages (SMS, email, push notifications) from the Bank regarding incoming and outgoing transactions on the Account. Immediately inform the Bank of any unauthorized credits or debits.

13.1.4. Control access to the mobile phone that receives SMS messages with one-time passwords from the Bank or has the Mobile Application installed. Do not leave it unattended and use built-in phone security features such as lock mechanisms.
13.1.5. If the mobile phone receiving SMS confirmations for transactions is lost or the SIM card unexpectedly stops working, contact your mobile operator and block the SIM card.
13.1.6. Do not send personal data or passwords in response to messages requesting login credentials, passwords, one-time passwords, or links to be clicked. Remember, the Bank never sends emails requesting such information or distributes software and updates via email.
13.1.8. If fraudulent transactions are detected on the Payment Card, it must be blocked immediately:
- by calling the Contact Center;
- using the Mobile Application.
13.2. Recommendations for transactions:
13.2.1. When using ATMs:
- do not use an ATM if its appearance is suspicious: different card reader color, excessively protruding keypad, exposed wires, foreign objects near the ATM service area, traces of glue or tape on the ATM panel. Report any suspicious cases to the Bank's Contact Center.
13.2.2. When using the card at merchants:
- do not use the Payment Card at retail and service locations that do not inspire trust.
- always request transactions to be conducted in the presence of the Cardholder to minimize the risk of unauthorized access to the card’s personal data.
- always enter the PIN code personally.
13.2.3. When making purchases online:
- make purchases only from your personal computer to maintain confidentiality of personal data and Payment Card information.
- if using a public or third-party computer, avoid saving your data, and ensure no personal information remains stored after completing transactions.
- register the Payment Card for the 3D Secure service.