Appendix 26
to the Regulations on issuing and servicing
payment cards for the individuals

The Payment Card Use Rules

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. Overdue Payment cards and cards that have not yet expired are not subject to card transactions.

1.2. The procedure and terms for using the Payment Card shall be governed by the laws of the Republic of Kazakhstan, the Comprehensive Agreement, the operating rules of the international payment systems Visa International, MasterCard Worldwid, and the Bank's internal rules, including these Rules for Using a Payment Card (the "Rules").

1.3. The client may be denied a card transaction that is contrary to the requirements of the laws of the Republic of Kazakhstan, in cases provided for by these Rules, the Comprehensive Agreement, and the operating rules of the international payment systems Visa International, MasterCard Worldwide.

1.4. The Holder shall keep the Payment Card and take measures against its loss or theft. Loss or theft of the Payment Card (if the Holder does not take the necessary measures against the loss or theft of the Payment Card) may be considered by the Bank as a violation of the Comprehensive Agreement terms by the Holder.

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

1.5.1. payment Card bank account (the "Account") - a current account using a Payment Card, opened by the Bank to the holder of the main card based on an accession application to the Comprehensive Agreement and an application for issuing a Payment Card, for card transactions, settlements and money storage;

1.5.2. statement - a document containing information on payments and (or) transfers and other transactions, including those carried out using a Payment Card;

1.5.3. Payment Card Holder or Holder – an individual entitled to use the Payment Card in line with the Bank's Comprehensive Agreement. The Cardholder who is the Account holder is the Client;

1.5.4. Client - an individual who does engaged in entrepreneurial, advocacy, private notary activities and execution of judicial acts (private judicial executors) activities, professional mediator activities, who has concluded a CD with the Bank and is the owner of the Account and / or a person entitled to use the Payment Card on the terms determined by the Bank, or an individual - a potential Client of the Bank;

1.5.5. Comprehensive Agreement for Banking Services for Individuals (the "Comprehensive Agreement") is an agreement concluded between the Bank and an individual, on the basis of which a Payment Card is issued.

1.5.6. Mobile application - software installed and running on a mobile device (smartphone, tablet, etc.) that provides access to Electronic Banking Services;

1.5.7. PIN code – personal identification number, a secret code assigned to the Payment Card and intended for Client identification;

1.5.8. Payment card - an electronic payment instrument that contains information allowing the Client to make payments and (or) money transfers or receive cash or execute currency exchange and other operations determined by the payment card issuer and on its terms via electronic terminals or other communication channels;

1.5.9. Entrepreneur - a legal entity, and an individual engaged in entrepreneurial activities without forming a legal entity, accepting Payment Cards to make a non-cash payment to pay for the goods and / or services they supply;

1.5.10. trade and service enterprise (the "TSE") - an individual entrepreneur or a legal entity that accepts Payment Cards to make a non-cash payment for goods and / or services supplied to them. TSE may impose restrictions on the payment cards types accepted for payment and the transactions amounts;

1.5.11. stop list - a list of payment card numbers prohibited for use and subject to withdrawal when they are presented for service. The stop list is formed by the IPS based on online (in electronic mode) or written requests from issuers;

1.5.12. 3D Secure (Visa International/MasterCard International technology) – developed by international payment systems Visa International, MasterCard Worldwide technology for additional Cardholder identification by entering a secret password in the process of card transaction online via the Internet in order to reduce the unauthorized card transactions risk and ensure the card transactions security on the Internet;

1.5.13. CVV2 or CVC2 ("CVV2" - an abbreviation of the English phrase "Card Verification Value 2", "CVC2" – "Card Validation Code 2") - a three-digit identification code (CVV2 - for Visa cards, CVC2 - for MasterCard cards), designed to identify the Payment Card holder when paying for goods and services on the Internet. CVV2 or CVC2 shall be applied to the Payment Card surface or displayed in the mobile application of the Bank.

2. Procedure for issuing and storing a Payment Card

2.1. The Bank shall issue the made Payment Card directly to the Holder or to his attorney acting on the basis of the power of attorney issued by the Payment Card Holder. Upon receipt of the Payment Card, the Holder shall sign in the field specially provided for this on the reverse side of the Payment Card.

2.2. The Payment Card Transfer to other persons for use or as a pledge shall be prohibited. A payment card presented by an unauthorized person shall be seized.

2.3. On the front side of the Payment Card there may be a microprocessor (chip) with information encoded on it. The microprocessor (chip) shall not be exposed to electromagnetic fields and atmospheric influences, but mechanical damage (scratches, dirt, creases, etc.) shall

not be allowed, which can lead to damage to the chip, as a result, the impossibility of carrying out Card transactions.
2.4. On the reverse side of the Payment Card there is a magnetic strip with information encoded on it, and an identification three-digit code CVV2/CVC2, designed to identify the Payment Card when paying for goods and services on the Internet, except for certain card products, for which CVV2/CVC2 is displayed in the mobile application of the Bank (in case of issuing a virtual payment card used only for Card transactions on the Internet, the three-digit code CVV2/CVC2 shall be issued separately). Exposure to adverse factors shall not be allowed: electromagnetic fields (proximity to displays, magnetized or containing magnets, such as keys, magnetic locks on bags), mechanical damage (scratches, pollution, overheating, for example, sunlight), etc., which may damage the record on the magnetic strip and lead to the impossibility of carrying out Card transactions.
2.5. Certain rules shall be followed to ensure the secrecy of the CVV2 / CVC2 code:

- if the CVV2/CVC2 code is recorded somewhere by the Payment Card Holder, then the Payment Card and the record shall be kept separately;
- shall not allow anyone to spy on the CVV2 / CVC2 code numbers combination typed on the computer in order to avoid unauthorized payments on the Internet.

3. PIN code
3.1. The PIN-code for the Payment Card Holders shall be requested by Temporary Code means or by Mobile Application means. It is recommended to store the PIN-code separately from the Payment Card in order to avoid unauthorized use of the Payment Card.
3.2 The PIN code shall be known only to the Cardholder. No one has the right to require the Payment Card Holder to provide a PIN code.
3.3. To activate the Payment Card, shall carry out the first operation by entering the PIN code using an ATM or POS-terminal, or when contacting the retail business client service department, or using the Bank's Mobile Application.
3.4. When selecting to set a PIN code via the Bank's ATM, the Cardholder shall send an SMS message from the mobile phone number registered with the Bank to the short number 7711 with the text: "epin space XXXX" (where XXXX is the last 4 digits of the payment card number).
3.5. The response SMS shall contain the Temporary code.
3.6. The temporary code can only be used for setting the PIN-code to the Payment Card at the Bank's ATM within 30 calendar days from the receipt date.
3.7. Next, you shall come up with and set a permanent PIN code for the Payment Card.
3.8. Together with the permanent PIN-code installation, the Payment card automatic activation shall be carried out.
3.9. For security reasons, it is recommended not to use too simple combinations of numbers to set the PIN code, such as 1111, 1234, 9090, etc.
3.10. When selecting to set a PIN code via the Bank's Mobile Application, the Cardholder shall download the application from the App Store/Play Market to their mobile device and then follow the instructions in the Mobile Application.
3.11. Certain rules shall be followed to ensure the secrecy of the PIN code:

- if the PIN-code is recorded somewhere, then the Payment Card and the record shall be kept separately;
- exclude access of third parties when typing a PIN-code numbers combination on the keyboard of an electronic device.

3.12. When entering a PIN code, the electronic devices displays numbers shall not be specially highlighted, but are replaced by a conventional sign. It is important not to make errors when typing. If three times in a row (with any time interval, using one or different electronic devices) an incorrect PIN code was entered, then, in case of the fourth mistake in a row, the Payment Card shall be blocked by the Bank, and it shall be detained at an ATM or may be withdrawn from service point until the circumstances are clarified.
3.13. Card transactions confirmed by a set of PIN-code or a signature on a receipt shall be recognized as executed by the Payment Card Holder.
3.14. If the Payment Card Holder has forgotten the PIN code, then the Payment Card shall be handed over to the Bank for reissuance, as it shall become impossible to carry out Card transactions.

4. Using a Payment Card
4.1. The Bank shall ensure servicing the Payment Card, the uninterrupted operation of systems and electronic devices over which it has direct control, and take all possible measures to restore the service in case of its suspension due to reasons beyond the Bank's control.
4.2. All Payment Card service points shall be equipped with International payment systems logos to inform Payment Card Holders on possibility of servicing with a Payment Card at this point.
4.3. The Bank may impose restrictions both on the types of transactions and on the Payment Card service area.
4.4. The Bank may send advertising and/or informational messages to the Payment Card Holder (including for the purpose of preventing unauthorized card transactions, improving the service quality) via the communication channels provided by the Bank (including in the form of SMS messages, Push notifications, etc.). Payment for providing such messages from the Payment Card Holder shall not be charged.
4.5. To carry out Card transactions, the Payment Card Holder shall present the Payment Card to the cashier of the service point (TSE or the Bank), or shall act with an ATM in self-service mode.
4.6. When conducting card transactions, QR-code technology can be used. Scanning a QR code in the Bank's mobile application is an indication of the Holder to make a payment.
4.7. During a regular (contact) operation, the cashier shall insert the Payment Card into the reader of the terminal, enter the operation amount on the keyboard and offer the Payment Card Holder to confirm the operation by entering a PIN code on a special keyboard. The

request shall be sent to the Bank via communication channels. When the correct PIN code is entered and there is enough money in the bank account, a check shall be printed in two copies, confirming the transaction. The cashier shall hand over to the Payment Card Holder one copy of the receipt. The Payment Card Holder shall check the data receipts correctness. Depending on the transaction, the printed check can be certified by the signatures of the Payment Card Holder and the cashier. In case of a contactless transaction, the Holder can independently attach the Payment Card to the reader of the terminal to carry out the transaction. Transactions made in a contactless way can be carried out without entering a PIN-code or signature of the Payment Card Holder on the check if the transaction amount does not exceed the limit set in the TSE.

4.8. The cashier may demand from the bearer of the Payment Card a document proving his identity. The absence of an identity document may serve as a basis for the cashier to refuse to carry out a Card transaction to the Payment Card bearer.

4.9. The cashier may withdraw the Payment Card until the circumstances are clarified in line with the terms of clause 8 of these Rules.

4.10. Payment for goods and services on the Internet or by telephone mail orders using a Payment Card shall be made in line with the procedure applicable to the Entrepreneur. The Entrepreneur may request the following information: Card number, surname, name of its Holder, CVV2-code or CVC2-code, 3-D Secure.

5. Using a Payment Card to receive cash

5.1. Cash withdrawal using a Payment Card shall be made at cash points or using ATMs of banks - International payment systems members.

5.2. As a rule, cash shall be issued with a Payment Card in the host country currency. In some countries, the frequency and maximum amount of withdrawal of cash using a Payment Card may be limited by the laws of the respective residence country or the internal rules of the servicing Bank.

5.3. Upon receipt of cash at cash points, the cashier shall issue to the Payment Card Holder the requested amount of cash and a transaction receipt.

5.4. After the Card transaction completion at the ATM and withdrawal of banknotes from the ATM, a receipt shall be printed at the Payment Card Holder request.

5.5. A card transaction to withdraw cash from an ATM for a valid Payment card, if the correct PIN code shall be entered and there is money in the account, may be rejected for the following reasons:

- the requested amount cannot be dispensed with the banknotes available in the ATM cassettes. You shall request an amount that is a multiple of the minimum denomination of banknotes specified in this ATM instructions;
- the requested amount shall exceed the limit for a single withdrawal. Shall divide the requested amount into parts and repeat the operation several times;
- the requested amount shall exceed the available money amount to the Payment Card Holder. Shall take into account the commission fee amount provided for in the Bank's tariffs for this operation type.

5.6. When working with an ATM, shall remember that money or a Payment Card may be delayed by the ATM if it is not received by the Payment Card Holder within 10-30 seconds. In such cases, the Payment Card return to its Holder can be made by the bank servicing this ATM only after finding out the reasons for the Payment Card detention and consulting with the Bank issuing the Payment Card. The Payment Card Holder can apply to the Bank for support in negotiations with the bank servicing this ATM.

5.7. To receive cash from an ATM without using a card, the service shall be initiated independently via the Mobile Application.

Cash withdrawal shall be carried out only in KZT. When carrying out a debit transaction on an account in a currency other than the account currency, the Bank shall convert the withdrawn amount at the current rate of non-cash purchase / sale of currency established at the operation time.

6. **Using a Payment Card to pay for goods and services of TSE**

6.1. Pursuant to the International Payment Systems Rules, TSE shall not overestimate the cost of goods and services when accepting a Payment Card for payment in comparison with cash payment. The Payment Card Holder shall notify the Bank in such cases.

6.2. The Payment Card Holder may return a purchase paid for with a Payment Card or refuse a service prepaid with a Payment Card, for example, return a purchased air ticket. To do this, at the Payment Card Holder shall request and with the TSE consent, the cashier shall execute the operation “return of the purchase” with the obligatory execution of a check signed by the cashier. The cardholder shall keep a receipt for the return of the purchase. Cash purchases shall not be refunded.

6.3. The Client shall be responsible for all Card transactions carried out using the Payment Card when paying for goods and/or services at Trade and Service Enterprises, on the Internet, via postal and/or telephone orders, and when withdrawing cash at cash points or ATMs.

6.4. In order to ensure safe transactions on the Internet, Cardholders shall be recommended to pay for goods/services on sites using 3-D Secure technology (availability of the Verified by Visa/MasterCard SecureCode logo). 3-D Secure technology shall allow to identify the Cardholder using a special password, which is known only to the Cardholder.

6.5. Bonuses can be accumulated on the Cards. All terms for the accrual and spending of bonuses shall be posted in the Bonus Program Rules for individuals posted on the Bank's website at www.jusan.kz.

7. Blocking of the Payment card

7.1. In case of loss, theft or unauthorized use of the Payment Card, shall immediately contact the Bank with an oral or written request to Block the Payment Card.

7.2. Phone numbers of the Contact Center: 7711 - for calls from mobile phones, the call is free, 58 77 11 - for 16 cities of Kazakhstan (with six-digit numbering), 258 77 11 - for Almaty, 8 800 080 2525 - free line within Kazakhstan (phones open 24/7, on weekends and holidays).

7.3. Blocking of the Payment Card shall be carried out immediately after registration of a written request for blocking by the Bank's branch. When contacting by phone, the Payment Card shall be blocked immediately, which shall be reported to the applied person.
7.4. The Client shall bear the risk and liability for the consequences, including damage, related to the partial blocking of lost/blocked Payment Cards. Partial blocking shall be understood as the refusal of the Client/Payment Card Holder to enter the details of the lost/stolen Payment cards in the stop list.
7.5. Upon detection of a Payment Card previously declared lost, the Payment Card Holder shall immediately inform the Bank about it and then return the Payment Card to the Bank. In case of subsequent use of the Payment Card, previously declared as lost, the Holder shall assume all risks related to the use of the Payment Card, and also reimburse the Bank for any additional costs that the Bank may incur in connection with the Payment Card withdrawal.
7.6. If the Payment Card contains restrictions on its use by types of transactions and/or service area, the Payment Card Holder may apply to the Bank with an oral/written application to remove the restriction. At the same time, the Bank shall not be responsible for the consequences that occurred in connection with the restrictions removal on the application of the Payment Card Holder.
7.7. The Bank has the right to block the Payment Card in line with the Comprehensive Agreement terms until the disputes that have arisen are settled.

8. Payment Card Withdrawal by third parties

8.1. Payment card Withdrawal at the service point shall be carried out if:

- the payment card is blocked;
- the Payment Card bearer is not its Holder;
- the Payment Card Holder forgot the Payment Card at the service point after the Card transaction;
- three times in a row (with any interval in time, when using one or more electronic devices) an incorrect PIN code was dialed.

8.2. Payment Card Withdrawal shall be carried out by an ATM, a cashier at a service point, an authorized employee of the Bank. Upon withdrawal of the Payment Card (except for cases of its detention by an ATM), an appropriate act shall be drawn up.
8.3. The Payment Card withdrawn return shall be made by the Bank (if delivery of the delayed Payment Card to the Bank) directly to the Payment Card Holder upon a written application of the Payment Card Holder.

9. Validity period of the Payment card, suspension and termination of the use of the Payment card

9.1. The Payment Card shall indicate its expiry date (month and year). The payment card shall be valid until the end of the last day of the month indicated on it.
9.2. In case of refusal to use the Payment Card Holder shall apply to the Bank with an appropriate written application and return the Payment Card.
9.3. The Bank shall inform the Payment Card Holder about his Payment Card expiration at least ten calendar days before its expiration date in the manner prescribed by the payment card issuance agreement.

10. Payment Card Reissue

10.1. Payment Card Reissue shall be carried out on the basis of a written application of the Payment Card Holder submitted to the Bank.
10.2. The payment card shall be reissued on the following grounds:

- expiration;
- risk area service;
- Bank's initiative (technical defects, etc.));
- loss/theft;
- PIN code forgotten/CVV2/CVC2/PIN code declassified/CVV2/CVC2;
- Payment Card Holder initiative/;
- Payment card compromise;
- damage/degaussing.

10.3. The reissued Payment Card shall be returned to the Bank. In case of non-return of the Payment Card by the Client/Payment Card Holder, as established by this clause, the Client shall assume all risks that may arise in case of non-return, and also reimburse the Bank for any additional costs that the Bank may incur in connection with the Payment Card withdrawal.

11. Payment Card Services

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

- cash withdrawal;
- balance inquiry;
- service providers payment (mobile communications, utilities, etc.);
- money transfers Visa Direct/MasterCard Money Send;
- activation/deactivation of the SMS-informing service;
- change of PIN-code;
- other services (as the card business develops, the Bank's services may be supplemented).

11.2. SMS-informing service activation shall allow the Payment Card Holder to receive information about all transactions made with the Payment Card
11.3. Bank account statements shall be sent to the Payment Card Holder by e-mail based on his written application submitted to the Bank.

12. Dispute Resolution

12.1. The Cardholder shall keep receipts to record the spending of money on the Account and resolve possible disputes.
12.2. Submission by the Bank to the Cardholder of a statement, and other documents copies, including those confirming the correctness of the money withdrawal from the Account, shall

be carried out in the manner and within the time limits established by the laws of the Republic of Kazakhstan and the Bank internal rules, upon request, including the Tariffs.
12.3. For all disputes, the Cardholder shall submit a written request to the Bank, which, if the claim is accepted, acts before the Payment Card System on behalf of the Cardholder. If the claim for unauthorized transaction is justified, the Bank shall restore the Card transaction amount on the Account. For unfounded claims (when it is impossible to prove the transaction unauthorizedness), the Payment Card System shall establish penalties that may exceed the disputed Card transaction amount. The Bank has the right, without additional consent of the Cardholder (in an unconditional and indisputable manner), to withdraw from the Account of its direct debit the amount of the fine imposed by the Payment Card System. The Bank, within 15 (fifteen) calendar days from the written application acceptance date of the Cardholder, shall inform the Cardholder about the preliminary investigation results. Upon completion of the investigation, the Bank, in case of making a decision to reimburse the Cardholder, shall make a refund to the Cardholder's Account or send a notice of refusal to refund the unauthorized transaction, indicating the reason. If additional examination is necessary by obtaining information from third parties or an audit, the Bank shall consider the application of the Cardholder and make a decision on it within thirty calendar days for transactions within the Republic of Kazakhstan or sixty calendar days for transactions executed abroad.
12.4. On detected transactions, qualified by the Bank as unauthorized, or when the Client applies for unauthorized transactions, the Bank shall reserve the right to take measures to challenge card transactions in line with the operational rules of international payment systems Visa International/MasterCard Worldwide, including in the absence of a Client's written application.
12.5. All Client claims, expressed in writing, regarding receiving money transactions via the Bank's ATMs, replenishing the Account via the Bank's self-service devices, shall be considered by the Bank in the manner and within the time limits established by the Bank's internal documents, also in line with the current laws of the Republic of Kazakhstan. The answer to the Client can be provided both in person and by e-mail or other available communication channel.

13. Security measures
13.1. When using the Payment Card, the Payment Card Holder shall observe the following security measures:
13.1.1. not disclose or transfer to third parties, including Bank employees, the following information:
- PIN code;
- CVV/CVC-code;
- password/login to the Mobile application;
- password 3-D Secure;
- SMS confirmation with one-time password.
13.1.2. shall not write down the above data on a piece of paper;
13.1.3. shall control all messages (SMS, e-mail, Push-notifications) from the Bank about incoming and outgoing transactions on the Account. Shall immediately inform the Bank on cases of unauthorized crediting or debiting of money;
13.1.4. shall control access to the mobile phone to which the Bank sends SMS messages with a confirming one-time password, or to which the Mobile Application is installed. Shall not leave it without personal supervision, use the mechanisms of blocking and protection from unauthorized persons built into the operating system of the mobile phone;
13.1.5. If losing your phone, to which the Bank sends SMS messages with a confirmation one-time password for account transactions, or if the SIM card suddenly stops working, shall contact mobile operator and block the SIM card;
13.1.6. shall not send personal data and passwords to anyone when receiving messages with a request to transfer a login, password, one-time password, follow the specified link. Remember, the Bank never, under any circumstances, shall send out e-mails with such requests, and also shall not distribute programs and their updates by e-mail.;
13.1.8. upon detection of fraudulent transactions made with the Payment Card, it shall be immediately blocked:
- by calling the Contact Center;
- using the mobile application.
13.2. Recommendations for transactions:
13.2.1. via ATM:
Shall not use an ATM if its appearance does not inspire confidence:
different color of the card reader (reading information device from the Payment card), excessively protruding keyboard, exposed wires, foreign objects in the ATM service area, traces of glue or adhesive tape on the front panel of the ATM. All suspicious cases must be reported to the Bank's Contact Center;
13.2.2. for Entrepreneurs:
shall not use the Payment Card in trade and service organizations that are not credible;
shall demand that transactions with the Payment Card be executed only in the Payment Card Holder presence. This is necessary in order to reduce the risk of illegal receipt of personal data indicated on the Payment Card;
shall always dial the PIN yourself;
13.2.3. via the Internet:
make purchases only from your computer in order to maintain the confidentiality of personal data and information about the Payment Card;
if the purchase is made using someone else's computer, shall not save your data on it, and after completing all operations, shall make sure that personal data and other information are not saved;
shall complete the procedure for Payment card registering for the 3-D Secure service.