Regulations of OJSC Bank Respublika on Usage and Servicing of Banking Cards

1. General provisions

1.1. These Regulations identify rules and procedures for usage and servicing of banking cards (hereinafter – cards) issued by OJSC Bank Respublika (hereinafter – the Bank) to individuals.

1.2. Cards are Bank's property and shall be returned to the Bank at the end of expiry date.

1.3. The Bank shall service cards in line with card emission and usage tariffs.

1.4. The Bank shall service cards solely on its own devices in line with the work schedule set up by the Bank. The work schedule is subject to changes.

1.5. The Bank can perform following operations through cards:

- Receive cash and non-cash payments on card account, including from third parties;
- Issue cash funds equal to the account balance;
- Non-cash payment settlements for goods and services;
- Transfer funds from card accounts to other accounts.

1.6. Card accounts can be increased by cash through following:

- "Cash in" ATMs.When using this method, the funds are immediately activated on the account.
- Bank Respublika branches and divisions;
- MilliÖnterminals;
- E-Manatterminals.

Funds credited on the account are active for use for the following periods:

Crediting times through Bank's branches, MilliÖn, e-Manatterminals	**Funds activated for use**
Until 12:00	After 12:00
Until 15:00	After 15:00
Until 17:45	After 17:45
After 17:45	After 12:00 of the following business day
Non-business day	After 12:00 of the following business day

1.7. During transactions through third bank terminals the amount of card transaction performed by the card user can be blocked until confirmation is received from the acquirer bank (bank servicing relevant terminal). After receipt of approval from acquirer-bank the transaction amount is written off from the card account. In the event if the acquirer bank's confirmation is not received within 33 days, the transaction amount is unblocked and available for use to the Card user.

1.8. While operating with bank card, first of all, the amount of card transaction gets blocked. If the currency of the card account and operation differ, the amount gets blocked according to the currency rate of that day. However, the amount is actually written off within 33 days after the operation according to the currency rate of current day and is transferred to Payment Systems. In this case writing off more amount than was blocked is considered to be the risk of card holder.

1.9. Personal Identification Number (hereinafter- PIN code) – is a confidential number code used to identify the card user during card transactions. Depending ont he card type, it is either personally assigned and set by the card user when receiving the card or provided to the card user in a sealed envelope. Card user is personally responsible for ensuring confidentiality of the PIN code.

1.10. In the event when operations are performed through POS terminals, these operations should be approved by Card user inputting the PIN code.

1.11. The Bank shall not bear responsibility for rejection of enterprise, including other credit organizations in servicing the card, as well as failure of technical equipment beyond Bank's property and other cases beyond Bank's control.

1.12. Cardholder can use the main card issued to his\her name, as well as supplementary card ordered for other trusted persons. In such case the cardholder is responsible for all transactions performed through those cards.

1.13. Bank shall not bear responsibility for any damage incurred by the Card user as a result of transfer of the card to third parties.

2. Cards in circulation

2.1. Card order applications can be submitted through the Bank branches, as well as online through customer's personal "Internet Division" and bank's official webpage at www.bankrespublika.az.

2.2. The Card shall be effective until the last of the month and year embossed on it.

2.3. The signature strip on the back of the card should be signed by the cardholder. Card user shall be responsible for any issues related to card signing.

2.4. In addition to the main card the card account holder can order a supplementary card with access to the same card account. The supplementary card can be issued to the cardholder's name, or any other individual's name under cardholder's responsibility.

2.5. Supplementary card can be ordered for:

2.5.1. Any person having reached age of maturity;

2.5.2. Persons between ages of 14-18 (fourteen – eighteen) can receive a supplementary card ordered by their parents or legal representatives.

2.5.3. Persons with supplementary cards ordered to their names shall also receive a unique PIN code.

2.6. Main card holder shall inform the supplementary card holders of these Regulations and applicable tariffs.

3.Re-issuing the card

3.1. In the event of a written application requesting prolongation of the card usage period, the Bank shall re-issue the card for a new period.

3.2. In absence of any written application from customer requesting prolongation of card, the Bank does not extend the term of the card.

3.3. In case of change in the first or last name of the customer, the Cardholder shall submit a written application to the Bank requesting re-issue of the card and submit all the necessary documents verifying change in personal information.

3.4. Supplementary card's maturity can be prolonged only by the main cardholder.

3.5. In the event if the card suspended (received) by Bank Respublika ATM belongs to the Bank, the card status and expiry date and returned to the Card user.

3.6. In the event if a card suspended (received) by another bank's ATM, the Card user shall immediately apply to the Bank to block the card and issue a new card.

4. Closing the card account

4.1 In order to close the card account the Cardholder shall apply in writing to Bank's branch which issued the card and shall return the card, including all the attached supplementary cards, if any.

4.2 In the event of failure to return the card to the Bank, the card shall be considered as lost. Bank shall apply relevant commission fee for loss of the card.

4.3. In order to deactivate the supplementary card, card account holder the shall address the Bank in writing and return the supplementary card.

4.4. When closing a customer's card account, attached supplementary cards issued to another individual(s)'s name are also deactivated.

4.5. When closing a card account, the residual funds in the account are returned to the Card holder after all the blocked but not charge-off amounts are charged off.

5. Conducting card transactions

5.1. When using the card to pay for goods and services, the Cardholder should verify the amount and date of the transaction, before signing the POS terminal receipt. By signing this receipt, the Cardholder confirms accuracy of the amount and authorizes the Bank to charge this amount off the card account. Copy of the official receipt is presented to the Cardholder.

5.2. Entities accepting card payments for goods and services may request from the cardholder to provide their identification documents.

5.3. Card holder should keep the receipts and slips evidencing operations performed using the card until such transactions are reflected in the monthly report. In the event if the goods are returned, or information is not received in sufficient detail, the representative of the merchandize\service entity will refund the funds to the account. Cardholder may not request cash refund of the value of goods purchased by card. The amount is subject only to non-cash refund by transfer of funds by the merchandize\service entity to the card account.

5.4. Bank shall provide the Cardholders with card transaction report from the card account. The report can be provided upon customer request, as well as regularly via email (if indicated in application).

5.5. Any objections on account charge-offs shall be submitted to the Bank within 45 days following the write-off. The Bank considers the objection and provides the customers with review results within 45 days following the customer's application.

6. Limits

=

6.1. Cardholder shall set the daily limit for internet card transactions not on the 3D secure service. Otherwise, the limit shall be set by the Bank as 5 transactions per day, overall amount of 150 USD equivalent.

6.2. Limits for all cash and non-cash transactions can be set and changed by the Cardholder after written application to the Bank.

6.3. For security reasons the Bank or payment systems may set certain restrictions on cash and non-cash transactions performed with cards.

7. Security

7.1. CVV2/CVC2 — is the special security code for Visa/Mastercardcards. This is a 3 (three) digit code is embossed on the back of the card, above or near signature strip. If a card does not have such code on it, it is not possible to perform online transactions using such cards. This code can be used not only to perform online transactions, but also when the card's magnet strip cannot be read (e.g. through payments over the phone).

7.2. If the PIN code is entered incorrectly 3 (three) times, the card is blocked. In this case, the customer needs to apply the Bank to unblock the card. The customer can change the PIN code by visiting the Bank or through ATM.

7.3. Code word –is a password (word, number or combination of both) used to identify the customer in telephone communications.

7.4. The account statements, as well as account information sent by the Bank to the customer is encrypted. To be able to read the information, the customer needs to enter code word in capital letters.

7.5. Customer can receive information on all of his\her accounts using the code word.

7.6. Code word is assigned exclusively by the customer.

7.7. Bank shall not be held responsible for any damage incurred as a result of disclosure to third parties.

8. Remote account management

8.1. **Mobile Banking.** The customer can use this service to perform following account transactions in real time regime (from any location and at any time) through a mobile phone:

- Utility payments;
- Mobile operator payments;
- Internet provider payments;
- Card-to-card transfers;
- Card blocking;
- Account statements;
- Card balance statement;
- Cash-by-code transaction.

8.2. To subscribe to service:

8.2.1. In ATM menu select "Services" section. Then in "Services" menu select "Mobile Banking registration" section and then the ATM will print out a receipt with serial number and components.

8.2.2. Formobile (smart) phones upload "Bank RespublikaMobilBank" from Play Market\App Store.

8.2.3. Serial number and components from the printed receipt are used to personalize the downloaded application.

8.3. **"Internet Office" service.** This service helps the customer to perform following transactions in real time regime any time of day from any location:

- **Loans.** Online loan application, pay loans online, monitor loan repayment schedule;
- **Cards.**Online card orders, card transaction receipts, increase card account balances.
- **Current accounts.** Receive current account statements;
- **Deposits.**Receive statements about deposit accounts;
- **Utilities payments etc.**

8.4. To subscribe to this service the customer may approach Bank's any office and fill out relevant application form. Service is personalized by the number of person's ID, login and password or AsanImza (Simple Signature) service.

8.5. **SMS Notification service.**This service immediately sends the customer SMS texts with information (transaction amount, currency, account currency) about conducted transactions. To subscribe to service: select in ATM Menu "service payment" - "service" – "other services" - "SMS Notification", and enter your mobile phone number.

8.6. **3D Security**. This service is the most advanced technology ensuring security and safety of online payments. This technology allows to unconditionally identify card user conducting transaction and at the same time limit the risk of unauthorized and fraudulent use of the card. When using such technology the Cardholder approves every transaction by entering a special code. "3D" password can be received in ATM Menu by going to "Internet Banking and list of single 3D passwords"section, printing the receipt with the list of passwords and registering on www.azericard.com/3d webpage.