Approved by
Appendix 1 of the resolution N 43/02-04.03.22 dated 04.03.2022
of the Executive Board of ARMECONOMBANK OJSC

INFORMATION BULLETIN ON THE TERMS (TERMS AND CONDITIONS) OF ISSUE OF DIGITAL PAYMENT CARDS OF ARMECONOMBANK OJSC AND TRANSACTIONS EXECUTED THEREWITH

1. Definitions and concepts:

"Bank": ARMECONOMBANK OJSC
"Card": payment card of Visa International payment system issued by the Bank for the Customer
"Identification: an obligatory process of verification and approval of the Customer's identity. While executing transactions at the Bank, the identification is verified on the basis of identification documents submitted by customers. When transactions are being executed on non-face-to-face communication basis (through electronic transactions), the customer is identified by the use of Customer Identifying data.
"Client identifying data": Client identifying data is envisaged to be applied in the electronic environment or during non-face-to-face communication, which can be PIN code (secret password), card's CVV code, parole, password or other means by the use of which the client will be deemed identified.
"**Trade and service outlet"** (hereinafter "TSO"): a partner of the Bank, for whom the Bank installed, activated POS/cash registers (POS) /Virtual POS terminals (hereinafter referred to as "Terminal").
"Digital card" (Token): The virtual representation of the card which the customer has activated in Mobile application and/or payment wallet to execute remote and/or contactless transactions. It's a unique digital code which has been generated by the payment system and is an additional requisite of the card.
"Card Tokenization": technology of replacement of the customer's secret data with special non-material equivalent
"Mobile application": a software (AEB Mobile, Apple Pay), which is installed on the mobile device and uses the service provider technology, the exclusive rights of which belong to the service provider. The functionality of the mobile app, the usage terms and the procedure on granting rights for the use of the mobile app are defined by the Provider of the given service.
"The provider": a company which on the bases of rules of the payment system and/or a separate agreement with the payment system provides necessary information and technology support to register, use and remove a digital card in the mobile app, the terms of which have been agreed with the Customer.
"NFC (Near field communication)": technology of wireless transfer of data between devices over a short distance (about 10 cm.)
"NFC payments": contactless payments which are executed through AEB Mobile app and/or other systems which are installed on the mobile device.
"Electronic image": image of the card electronically registered in the mobile device which contain the 4 digits of the Card, the logos of the Bank and the payment system
To read the General Terms and Conditions of the banking services rendered by **"ARMECONOMBANK OJSC"** visit the link: https://aeb.am/hy/sakagner/

2. Main principles of the transactions

2.1 Tokenization of the card, implementation of contactless and/or remote transactions through the Bank's system.

2.1.1 The tokenization is possible to implement with cards of VISA International payment system issued by the Bank.

2.1.2 The customer can simultaneously tokenize more than one card in the mobile device.

2.1.3 It is possible to make NFC payments via a mobile device, if the latter has one of the following unlocking security systems: fingerprint, FaceID, PIN.

2.1.4 The customer is granted with an opportunity to activate/register a digital card and an e-image corresponding thereto in the mobile application for which the Customer:

2.1.4.1 Enters the required information about the card into the mobile app following the instruction of the app interface.

2.1.4.2 Accepts the terms and conditions of the Provider of the service and other terms (if any) in accordance with the terms of mobile application.

2.1.4.3 Agrees with the terms on the issue of the digital payment card and transactions executed therewith.

2.1.4.4 After the successful verification of the card by the Bank, the mobile application offers the Customer to pass identification by entering the one-time password into the mobile app which has been received through an appropriate SMS or e-mail.

2.1.4.5 Confirms the Customer identifying method offered by the mobile app (e.g. entering a one-time password which has been sent as SMS message)

2.1.4.6 After the successful identification of the Customer, the mobile app informs about the activation/registration of the digital card and downloads the appropriate e-image.

2.1.5 The safety of the Customer's card data during the tokenization is guaranteed by Visa International payment system.

2.2 To implement contactless transactions through ATMs the customer shall perform the below mentioned activities:

2.2.1 Check the payment amount reflected on the screen of the POS terminal of the TSO

2.2.2 Enter the identification (biometric) data into the portable device to activate the mobile device

2.2.3 Select the appropriate e-image of the digital card through which he/she wants to make the payment, if necessary

2.2.4 Bring the mobile device nearer to the Pos terminal for the transfer of data.

2.2.5 In some cases to execute a transaction with the digital card the Customer may be required to confirm the transaction additionally entering the Card PIN through TSO's Pos terminal.

2.3 To perform a remote operation the Customer shall implement the below mentioned activities.

2.3.1 Choose the product or service which he/she wants to buy with the digital card registered in the mobile app through the apps of TSOs, the Provider or on the websites cooperating with the mobile app (web platforms).

2.3.2 Check the amount to be paid and other details

2.3.3 Select the e-image of the appropriate digital card in the mobile application through which the transaction will be executed.

2.3.4 Confirm the payment process with the digital card entering the identification data into the mobile device.

2.3.5 The confirmation of the customer's instruction of the execution of a transaction through the digital card is the entry of the identification data into the mobile device.

3. **Liabilities and rights of the Bank**

3.1 The Bank is obliged to:

3.1.1 Ensure the service of the digital card in accordance with the rules accepted by the payment and settlement systems and provide the Customer with round-the-clock support at 86 86 or +374-8000-8686 phone numbers.

3.1.2 Immediately block the card after the Customer warns about the loss of a mobile device, theft of identification data or the data of tokenized card or on access thereto by third parties.

3.1.3 In the order prescribed by the RA Legislation and the Agreement, keep the information regarding the Customer constituting bank secrecy that has been submitted to the bank.

3.2 The Bank is eligible to:

3.2.1 Unilaterally reject the tokenization of the card in case the card is blocked; there is suspicion of a fraud or in other cases.

3.2.2 Reject the implementation of transactions if the required amount exceeds the payment limit of the Card.

3.2.3 In the cases and order set forth by the RA Legislation, impose restrictions on the monetary funds available on the account based on the judicial acts, decisions of compulsory enforcement bodies and tax authorities

3.2.4 Without prior notice charge the fees set by the Tariffs, offset the receivables, loans and other monetary liabilities of the Customer to the Bank.

4. Liabilities and rights of the Customer:

4.1 The customer is obliged to :

4.1.1 Read the terms and conditions of the transactions made through payment cards and meet all the rules and requirements set forth by it prior to the tokenization of the card.

4.1.2 In case of loss of the mobile device, theft of the identification data or data of the tokenized card or the access thereto by the third parties immediately apply to the Bank to block the tokenized payment card/s/.

4.1.3 The Customer may have other terms and agreements with the Provider or the third party companies the fulfillment of the provisions set forth by them is obligatory for the Customer.

4.2 The customer is entitled with the right to:

4.2.1 Implement remote and/or contactless transactions in the Mobile app and /or payment wallet with the tokenized card

4.2.2 Tokenize more than one card

4.2.3 Dispute the transactions made through the card account in the order and terms set forth by the Agreement.

5. **Responsibility**

5.1 The Bank is not liable for the prohibited transactions transactions or attempts of transactions with the tokenized card for the services offered by the Provider or third parties.

5.2 Should the Customer fail to notify the Bank about the loss of the Mobile device, the theft of identification data or tokenized card data or about the access thereto by third parties the Bank is not liable for transactions with the tokenized card.

5.3 The Bank is not liable for interruptions, malfunctions or failures of the work of the third party companies.