Chapter 8. ELECTRONIC WALLET SERVICE

TO THE UNIVERSAL AGREEMENT OF BANKING SERVICE OF CLIENTS - INDIVIDUALS IN

JSC BANK CREDIT DNEPR

8.1. Prior to receiving a notice from the Client (Payment Card Holder) prohibiting tokenization, providing services therefore UDBO, it is assumed that the Client (account holder) does not prohibit tokenization of cards / additional cards issued on his account. The Client may apply for a ban on tokenization of all or some cards / additional cards issued on his account (s) by contacting the Contact Center with identification. The Client may cancel the previously submitted application for prohibition of tokenization in the same way as the application was submitted.
8.2. Tokenization and transactions using the E-wallet Service are performed only on valid cards / additional cards of the payment vehicle if there is a technical possibility in the Bank.
8.3. To make payments using the E-wallet Service, it is necessary to register cards in it, providing the relevant details of such cards in the mobile application.
8.4. The e-wallet service is connected to the mobile device using the tips of the mobile application.
8.5. The Bank verifies the details of the payment card entered in the mobile application (card number, card validity period, CVC2 / CVV2 code) and, if necessary, conducts the Authentication of the Holder. The card must be valid.
8.6. Authentication of the Holder is performed by the Bank in one of the ways (at the choice of the Holder or in case another method of authentication is unsuccessful):
8.6.1.Using a one-time digital password (OTP password) sent to the Cardholder in an SMS / Push message.
8.6.2. By the Cardholder passing the verification procedure through the Contact Center in accordance with the procedure established by the Bank.
8.7. After successful registration of the Card in the mobile application, a token is formed and stored in the secure storage of the mobile device. The token allows you to uniquely identify the Card used when making payments using the E-wallet Service.
8.8. The E-Wallet Service records the last ten transactions for each Card registered in the E-Wallet Service (transaction history).
8.9. If there are several cards registered in the E-Wallet Service, the Cardholder may select the Card with which the default payments will be made in the E-Wallet Service.
8.10. The holder using the E-wallet Service using the appropriate mobile device can:
- make payments through a POS terminal equipped with NFC technology;
- make payments in mobile applications on a mobile device and on sites that support payments through the E-wallet Service.
8.11. The Cardholder, when making a payment using the E-Wallet Service, registers the Card in the mobile application, using a one-time digital password / fingerprint, confirming the occurrence and use of an analogue of a handwritten signature. The Cardholder acknowledges that the formation of an electronic document for payment using the Electronic Wallet Service is analogous to the handwritten signature of documents on paper.
8.12. Deleting a connected card from the E-Wallet Service is done by removing the token from the mobile application.
8.13. The holder is obliged to remove the token from the mobile application and delete the mobile application for mobile devices in the following cases:
- in cases of hacking of the mobile device to the Holder or suspicion of hacking;
- access by third parties to access to or suspicion of a mobile device or other breach of security and access to a mobile device and / or mobile application and the like;
- before the destruction of the mobile device or transfer to the use of another person and other disposal of the mobile device from the possession of the Holder, which occurs at his will by expression, or without such expression of will.
8.14. The token may be deleted by the Bank in case the Holder applies to the Contact Center, identifies it and receives a notification from the Holder about the signs of token compromise.
8.15. The Holder understands and agrees that:
- not all legal entities and natural persons-entrepreneurs who sell goods, perform works, provide services, as well as not all institutions that provide financial services, can provide the ability to pay with the help of the Service of electronic wallets;
- payment systems, institutions providing financial services may impose restrictions, in particular, on the amounts of transactions using the E-Wallet Service and set their fees for such transactions;
- the implementation of operations using the E-wallet Service may be limited by the functionality of the software of the mobile device, including the mobile application;
- access, use and ability to perform operations using the E-wallet Service depends on the state of the wireless communication networks used by the Internet provider;
- on any issues related to the technical support of the mobile device, software and hardware requirements, the Cardholder must contact the service center of the manufacturer of such mobile device;
- the procedure for receiving and processing any information received by the Internet provider in the process of using the Electronic Wallet Service Card Holder is regulated by the agreement between the Holder and the Internet provider;
- Internet provider, mobile operator used by the Holder, other persons involved in ensuring the operation of the E-Wallet Service have their own terms of service and privacy policy. By transmitting his personal data to the specified persons, using the services or visiting the sites on the Internet of the specified persons, the Holder accepts their conditions.
services and privacy policies.
8.16. The Holder is aware of the increased risk and understands that when using the E-Wallet Service, access to the Holder's mobile device directly affects the possibility of unauthorized Card / Additional Card transactions, and, therefore, the Holder is solely responsible for:
- confidentiality of one-time passwords, PINs and other means of access of the Holder to the mobile device, mobile application, card / additional card;
- the presence of restrictions on access to the mobile device (systematic blocking, etc.) and the reliability and sufficiency of the means chosen by the Holder to restrict access to the mobile device (passwords, biometric identifiers, time intervals, etc.), for the presence and timely update of antivirus programs installed on it mobile

application;
- operations carried out with the help of the Electronic Wallet Service, in the presence of the Bank's technical capabilities to provide such a service, on the Holder's mobile device;
- timely notification of the Bank on the need to block the token, including, but not limited to: in cases of hacking of the Holder's mobile device by third parties, loss / theft or damage of the mobile device, access by third parties to the mobile device or suspicion of a security breach and access to a mobile device and / or mobile application and the like;
- deleting the token from the mobile application before deleting the mobile application for mobile devices;
- removal of the mobile application before the transfer of the mobile device for processing, before destruction, transfer for use or ownership to a third party and other disposal of the mobile device from the possession of the Holder, which occurs with or without his will;
- compliance with instructions and rules for working with the mobile application.
8.17. The bank is responsible for:
- saving funds on the Cardholder's account and performing operations on the account provided that the Cardholder complies with the terms of this UDBO, tariffs;
- non-fulfillment of its obligations to the Cardholder in accordance with the current legislation.
8.18 The Bank is not responsible for:
- work of the Electronic Wallet Service;
- inability of the Cardholder to perform operations with the help of the E-wallet Service;
- any blocking, suspension, cancellation or termination of the use of the Card / additional card using the E-wallet Service;
- confidentiality of information stored on the mobile device in the mobile application;
- support for the operating system of the mobile device;
- actions of the provider or any third party are carried out within the limits of service of the mobile application, Service of electronic wallets;
- any circumstances that may interrupt, interfere with or otherwise affect the operation of the mobile application, E-wallet Service (inadmissibility of the network of the mobile operator, restrictions on the coverage area of the mobile network, interruptions in the supply or interruption of the wireless connection)
- maintenance of wireless communication networks, system of disconnection / interruption of wireless connection.
8.19. The Bank does not guarantee the confidentiality and security of electronic transmission of the Cardholder's data through third-party connections that are not under the Bank's control. Confidentiality and security of data transfer are ensured in accordance with the Company's regulations, which provide the E-wallet Service.