

Terms and Conditions for usage and adding Cards In the System

1. General Provisions

1.1. This document sets out the terms and conditions (hereinafter referred to as the **Terms**) for the usage of services of the System and the registration of the bank cards into the system by the clients of JSC Basisbank (address: 0103, 1, St. Queen Ketevan Ave., Tbilisi, Georgia. Registration code 203841833. hereinafter referred to as the **Bank**). This document also constitutes an addition to the Agreement on banking services provided to natural person (hereinafter referred to as the **contract**).

1.2. Prior to registering/adding a card into the device and using the service, the customer is required to be thoroughly familiar with these terms and conditions and to ensure that they are fully and properly implemented throughout the service period.

1.3. In any case, by registering/adding a card and/or additional card into the device the client and/or additional card holder express their consent to the present terms and confirmation and agree on their fulfillment.

1.4. By adding a card and/or additional card to the device, the additional client / additional card holder agrees to the terms of use of the System.

1.5. Given terms and conditions set out the rules for accessing the System and using a customer card only within the relationship between the bank and the customer. Mobile Communications Operator, Service and other service providers (including websites) that are integrated into the payment service system) are authorized to set their own rules and regulations (including terms and conditions of the System) and privacy policies.

2. Definitions of terms

2.1. For the purposes of present Terms and Conditions The following terms have the following meanings:

- **Device** - a device which can be used to register a card to pay in The System;
- **System** - A mobile/digital payment system/service that allows users to make payments using device and cards registered/added this devices;
- **Vendor of The System** – Apple Pay or Google Pay, as case may be.
- **Authentication data** - Customer password for authorization on The System (including client biometric data (Touch ID), face image (Face ID)) or other new technology provided by The System, installed in accordance with the rules of the System. PIN code, as well as other data used to log in to the system. Authentication Data is the analog to client's personal signature;
- **Payment service** - service(s) that are envisaged in its terms and conditions, and intended to pay for goods and services using digital cards;
- **Card** – a Visa or MasterCard bank card issued in the name of the client or additional card holder in accordance with the agreement;
- **Additional card holder** - the client and/or other individual /named by the client to whom the bank has issued the card;
- **Virtual image** - electronic image of digital card;
- **Touch ID** - A fingerprint recognition function to verify actions, including payment operations. This feature can be activated, modified or disabled using the access code on the device;
- **Client** – an individual who has signed a contract;
- **Wireless Communication Operator** - a customer service provider that provides telephone/ internet connection to the mobile network for the operation of the mobile terminal;
- **Contactless Payment** - Payment made using a contactless reader and digital card;
- **Digital card** - a card selected and registered/added by the client for use in the System.

3. Registering/Adding a Card to Device

3.1. The client is entitled to register their card, and the additional card holder is in turn authorized to register/add an additional card to their device, provided that:

3.1.1. The client and/or the additional card holder will be identified by the bank in accordance with the rules established by the bank;

3.1.2. The appropriate card or card account will not specify the conditions by the bank that limit the ability to add a card to the device.

3.2. Adding a card/additional card to the System and/or deleting the added card/additional card can be done by the client or the additional card holder of the relevant additional card, according to the rules set by the System, taking into account the present terms and conditions.

3.3. The client registers the card in The System by entering the card data in the device. In case of successful verification of the card, the System creates a digital card and forms its virtual image in the System.

3.4. While adding a card to the device, in order to use service, the client may be required to go through the verification process. Verification can be done with a single code, which is sent to the contact number registered by the client with the bank or through the bank call center, following the identification process established by the bank. In addition, the client allows the bank to communicate with the client by telephone and/or other means of communication to complete the client's verification process and/or to remind the client to finalize the incomplete verification .

3.5. Once the client/additional cardholder registers/adds the card to the System, they will be entitled to make authorized transactions with their card account via the System. To make the payment, the client confirms the payment by selecting the

desired digital card in the system and placing the device near the contactless terminal or reading device located in the store, by entering the authentication data.

3.6. Multiple cards can be added to the System, as well as one card may be added to multiple devices.

4. Security and Responsibility

4.1. The client acknowledges that any person who has the ability to unlock and use the device will also be able to use the added/registered card/additional card in the System.

4.2. After adding the card /additional card to the System, the client/additional card holder is obliged to ensure that:

4.2.1. devices may only be used by cardholder's authentication methods;

4.2.2. e-wallet is only accessible by the cardholder;

4.2.3. The device passcode are stored following the same security standards and rules as the access codes, including:

- It shall not be shared with a third party;
- It shall not be stored in such a way that it is in any form available to a third party;
- Shall not be used an easily comprehensible or computable passcode (for example: client's name, date of birth, etc.);
- The clients shall not show carelessness/negligence while storing the passcode.

4.2.4. Shall protect the security of the device, including not leaving the device unattended in an unlocked state, shall install the latest version of the antivirus on it, etc.

4.2.5. Shall ensure deletion of the card/additional card from the system before transferring the device to a third party.

4.3. The client/additional cardholder acknowledges that if they use a third-person fingerprint or facial recognition system to unblock the device, or share the device passcode to the third party, that means authorizing the third party to dispose the card/additional card in the System. This means that the transaction initiated by the relevant third party will be considered authorized and the terms and conditions established for unauthorized/unsanctioned transaction will not be applied to it.

4.4. The client/additional cardholder is authorized to remove the card/additional card from The System at any time or to suspend its operation. Herewith, the client acknowledges that they are not exempt from the liability of paying amount of transactions and of related fees and liabilities, which were carried out before removing the card from the System and/or suspending its validity.

4.5. The client/additional cardholder is obliged to immediately notify the bank, if:

4.4.1. Their device was lost or stolen;

4.4.2. An unexpected interruption occurred in the service of the device, which may indicate that the data is being ported;

4.4.3. It is suspected that his/her device was used illegally or that an unauthorized person has accessed the access codes of the card.

4.5. Based on the information provided, the bank will ensure that the use of the card /additional card is suspended. This in turn will help the client/additional cardholder to protect themselves from unauthorized use of accounts.

4.6. In the contract:

4.6.1. Each reference to access codes also implies a reference to the System authentication methods.

4.6.2. Each instruction on protecting the security of the card/additional card includes an instruction on the System and device security. Each instruction regarding lost/stolen cards includes an instruction on the loss/theft of the device.

5. Costs and fees

5.1. The fees and expenses for the transactions carried out from the account are published on the bank's website. The bank does not charge additional fees for registering a card in and using the System.

5.2. Customer understands that the agreements and other arrangements concluded with third parties may envisage such taxes, limitations or restrictions, which can be reflected on any digital card use (for example, the use of data, or text messaging fees, imposed on a client by wireless communication operator), for which the bank is not responsible. The client is solely responsible for paying such taxes and for adhering all restrictions and prohibitions.

6. Termination or/and Suspension of the Use of the System

6.1. The Bank reserves the right to terminate the service or support of any digital card and participation in the system on any grounds (on the basis of notification). The bank is authorized to block the card/additional card registered in the System and/or suspend or terminate the validity of the card/additional card issued by the bank in the System, in case: the bank has a reasonable suspicion of fraud; the card/additional card is blocked; the terms of the account related to the card were violated; upon the terms of the System and/or international payment system; in case of termination of the contract between the bank and the Vendor of the System; in cases prescribed by law.

6.2. The Vendor of the System reserves the right to block, restrict, suspend or discontinue the use of a digital card by the client/additional card holder and/or modify the functions of the system without notice to the bank. Customer/cardholder understands that in such case the bank is not liable towards the customer/additional cardholder or third party.

6.3. After elimination of the grounds of a temporary blocking of a digital card or the suspension of a card, the client/additional cardholder will be able to continue using services of the System after receiving the appropriate notification.

6.4. The client is authorized to remove the digital card from the system after completing the relevant procedure on the device or by contacting the bank.

7. Delay in the Provision of Payment Services

7.1. Access to a digital card, its usage and service depends on the volume of services of the System and the wireless communication operator network. Taking into consideration that the bank is not an operator of services of the System or wireless communication network and does not control their operation, the bank is not responsible to client/additional cardholder for any circumstances that may suspend, restrict or otherwise affect the function of any digital card, including limited accessibility of services or wireless connectivity, network blockage, wireless coverage restrictions, service-related flaws the wireless connection fail.

7.2. The use of a digital card involves the electronic transmission of personal information via a third party network. Due to the fact that the bank does not operate or control such networks, it is not responsible for the confidentiality and security of such information.

8. Limitation of Liability

8.1. The client/additional card holder acknowledges and agrees that the System and digital card functions can be updated automatically, without additional notifications sent to them. The Bank shall, at any time, have the right to decide to expand, reduce or suspend the types and/or volume of operations specified for the digital card or change the registration procedure.

8.2. After returning all the cards to the bank and closing the account, the client is not exempt from the amount of the transactions; and the obligations to paying commissions related thereto; and from the liabilities that the client carried out during the period before returning the card and closing the account

9. Making amendments to given Terms and Conditions

9.1. The Bank reserves the right to revise these Terms and Conditions. The Bank shall notify the client of any changes in these Terms and Conditions via any communication channel specified in these Terms and Conditions as defined in the contract. If the client does not agree with any of the changes made to Terms, they may remove the digital card from the system. Herewith, the client allows the bank to continue processing/completing the tasks related to this type of digital card, which could not be completed by the time the card was deleted.

9.2. After the bank establishes new Terms and conditions, the completion of the payment operation through the digital card will be considered as the client's consent to their use.

10. Communication

10.1. By registering/adding the card/additional card in the system, the client/additional card holder agrees to the given Terms and Conditions as they are.

10.2. The client /additional card holder agrees to receive information and other messages sent by the bank regarding the system services and for which the following communication channels are used:

10.2.1. Email (the same email address as specified in the account opening application);

10.2.2. SMS message (mobile phone number of the wireless communication operator, indicated in the application for opening the account).

11. Data Collection and Security

11.1.1. The client/additional cardholder is aware and agrees that the bank is authorized to collect, process and use technical information, personal data and related information, including, but not limited to, the information available at client's/additional cardholder's mobile terminal, to ensure:

11.1.1.1. Updating and improving the bank's products and services;

11.1.1.2. Improving the security level of the services provided;

11.1.1.3. Prevent fraud.

11.1.2. The client acknowledges and agrees that the bank shall not be liable for the confidentiality of information transmitted through communication channels, SMS messages, USSD services and/or other channels.

11.1.3. The client/additional cardholder acknowledges and agrees that the Bank shall not be liable if third parties get hold of the client's account information (all cards through which the transactions are completed on the account) when such information is passed on to the client via remote channels and the bank used details submitted to the bank by the client/client representative (mobile phone numbers, email addresses, passwords or secret words, etc.).

11.1.5. The client/additional card holder agrees to transfer their personal data to the Vendor of the system, and/or affiliated parties.

12. Other Conditions

12.1 The Vendor of the relevant system ensures the smooth operation of the system and the device. The bank's involvement is limited to providing information only, so that cardholders can make full use of services provided by the System.

12.2 By using the System, the client/additional cardholder fully agrees to the terms and conditions of the System.

12.3 Given Terms and Conditions are regulated by the legislation of Georgia. The client/additional cardholder agrees that the common courts of Georgia will have exclusive jurisdiction over any case or dispute that may arise in connection with these terms and conditions.