1. Terms and Conditions of use of Bank cards in the mobile payment system

1.1. Terms and Definitions

Each term retains its meaning no matter where it is used in the Terms, and the words for the singular include the plural and vice versa.

* Service Provider – * Any company being the vendor of the Mobile terminal with whom the Client signed the agreement on providing Payment services.

* System - pre-installed software in the Mobile Terminal, exclusive rights to which belong to the Service Provider, and which is an application allowing Mobile terminals to provide Payment Services.

* Service Provider Terms - Software License Agreement and other Additional Service Provider Terms concluded by and between the Client and the Service Provider.

* Bank —JCS Credo Bank, #27 R. Tabukashvili str. 0108, Tbilisi, Georgia, ID: 205232238

* Contract - Terms of comprehensive banking services.

* Client - an individual who has entered into an Agreement with the Bank.

* Contactless payment - a payment made by using the Digital Card in a contactless reader.

* Authentication data - the Client's password for authorization in the Mobile Application (including but not limited to biometric data (fingerprint authorization) set in accordance with the Conditions of the Service Provider, PIN code, and other data used to access the System. Authentication data is equivalent to the Client's personal signature.

* Digital Card - A Card that the Client has selected and registered for use in the System.

* Card - Service with a plastic card implies performance of a banking operation through the plastic card Visa or Mastercard (hereinafter "Card") issued by the bank, except for business card, by the Client (hereinafter "Card Owner") or any person notified by them in a written form (hereinafter "Card Owner").

* Mobile terminal - a wireless payment device.

* Built-in application - the ability to make a purchase using a mobile application from merchants who provide payment services in their applications through the System.

* Supported devices - devices that support the Service Provider Systems.

* Contracts with a third party - the Service Provider, the wireless operator and any other third party services or sites embedded in the System, which provide their own terms and conditions (including the Terms and Conditions of the Service Provider) and privacy policy.

* Virtual representation - an electronic image of a digital card.

* Fingerprint input - fingerprint recognition function to certify actions in the System, including payment transactions. The function can be set, changed or disabled using the access code in the Mobile Terminal.

* Wireless Operator - means the Client's service provider that provides a telephone connection to the mobile network for the operation of the Mobile Terminal.

* Payment Services - Service Provider services for payment for goods and services using Digital Cards in accordance with the Service Provider Terms.

2. General Provisions

2.1. This document contains conditions governing the use of any Digital cards of the Bank in the System. These Terms are an addition to the Card Agreement.

2.2. If there are discrepancies between the provisions of these Terms and other Agreements, the provisions of this Agreement apply to Payment Services.

2.3. These Terms and Conditions establish the rules for access and use of the Client's Digital Card only between the Bank and the Client. The mobile operator, Service Provider and other third-party service providers or sites included in the Payment Services system may set their own terms and conditions (including the terms of the Service Provider) and privacy policy, and the Client must also comply with the terms of such Agreements with third parties when providing them with personal information, using the services or visiting the relevant sites.

2.4. The use of Payment Services by the Client for the purchase of goods and services using a Digital Card is governed by the Agreement in effect.

3. Working principle

3.1. Making payments

3.1.1. The system allows you to create a Virtual Card View on the Client's Mobile Terminal, so that the Client can perform:

* Contactless payments at contactless terminals at points of sale;

* Built-in application or other digital commercial payments to sellers connected to the system of Payment services.

3.1.2. The client registers the Card in the System by entering the Card details into the Mobile terminal. After successful verification of the Card, the System forms a Digital Card and creates its Virtual Representation in the System.

3.1.3. To make a payment with the Digital Card, the Client, by selecting the appropriate Virtual Representation of the Digital Card in the System and placing the Mobile Terminal next to the contactless payment terminal at the point of sale or a reader, the Client confirms the payment by entering Authentication data.

3.1.4. To make purchases with the Embedded application, the Client selects the appropriate Virtual Representation of the Digital Card in the System and confirms the payment by entering Authentication data.

3.2. Browsing the information and the payments

3.2.1. The system provides the Client with an access to the following information on the Digital Card:

3.2.1.1. card status: active, expired, blocked due to different reasons;

3.2.1.2. information on previous transactions performed by this Digital Card: date, amount of purchase, name of the seller. The System provides the ability to disable notification of purchase transactions for each Digital Card.

3.2.2. The system cannot provide information on transactions performed without using the System.

3.3. Rights and obligations of the Client

3.3.1. The Client is obliged to comply with the terms of the Service Provider.

3.3.2. Before registering in the System, the Client is obliged to ensure that only the Client's fingerprints (Touch ID), Face ID (secure authentication) or other new technology provided by the Service Provider are registered in the System. Usage of fingerprints (Touch ID), Face ID (secure authentication) or other new technology provided by the Service Provider will be considered as the confirmation of transactions on operations with the use of the Card. If fingerprints (or Authentication Data) of another person are used for the authorization in the Mobile terminal or for the Fingerprint Login (Touch ID), or for performing operations at the Client's Mobile Terminal, such fingerprints will be considered as the Client's fingerprints.

3.3.3. The client is obliged to ensure the storage of their Authentication data in a place inaccessible to third parties.

3.3.4. In the event of a compromise of the Authentication data and / or Digital Card data, the Client must immediately notify the Bank about such case.

3.3.5. In case the Client fails to timely notify the Bank by about the loss of the Authentication data and / or the compromise of the Digital Card details, the Bank shall not be liable for any losses of the Client.

3.3.6. Purchases or other transactions made by the Digital Card and Client Authentication data are considered Client operations.

3.3.7. The Client has the right to use any Card opened in the name of the Client that is not canceled or blocked, to create a Digital Card.

3.3.8. The Client has the right use one and the same Card in different Mobile terminals.

3.3.9. The Client has the right to refuse to use the Payment Services at any time by deleting the Digital Card from the System.

3.4. Rights and Obligations of the Bank

3.4.1. The Bank is authorized to refuse the Client to register the Card and create a Digital Card in the System.

3.4.2. The Bank is authorized to block the operation of the Digital Card or the possibility of its use in the System, to order a removal of the Card / Digital Card and take all necessary measures for this:

3.4.2.1. in case of non-fulfillment or improper fulfillment by the Client of the obligations stipulated by these Terms;

3.4.2.2. in case an unauthorized use of a Digital Card and / or Card is suspected.

3.4.3. The Bank is obliged to provide information support to the Client on the use of the Digital Card by phone: +995 32 2 42 42 42.

3.5. Agreements with third parties

3.5.1. These Terms apply only to the use of the Digital Card(s) by the Client. The service provider, wireless operator and other third-party sites or services connected to the System have their own Agreements with third parties, and the Client is obliged to comply with their conditions when providing personal information to specified persons, using the services provided by them or visiting relevant sites. The Bank is not responsible for the safety, accuracy, legality, suitability and other aspects of the content or operation of the products or services of the Service Provider or of a third party.

3.5.2. The Bank is not responsible and does not provide support or assistance in relation to any third party hardware or software, as well as their other products or services (including the System or the Mobile Terminal).

3.6. Service price

3.6.1. The bank does not charge for the use of the Digital Card.

3.6.2. The Client must consider that contracts and other agreements with third parties may include payments, restrictions and prohibitions that may affect the use of any Digital Card(s), for example, data usage or text messaging fees charged by the wireless operator. The client undertakes an obligation to bear sole responsibility for such payments and the observance of all restrictions or prohibitions.

3.7. Resolution of Disputes and the governing law

3.7.1. Any dispute and disagreement between the parties are to be resolved by negotiations. In case an agreement between the parties is not reached, such dispute shall be transferred to the Tbilisi City Court.

3.7.2. 3.7.2 This agreement is governed by Georgian law.

4. Privacy and security

4.1. Personal Information

4.1.1. The Client has read and agrees that the Bank is entitled to collect, process and use technical, personal data and related information, including but not limited to, the Client's Mobile Terminal, in order to ensure:

4.1.1.1. Improvement of the Bank's products and services for the benefit of the client;

4.1.1.2. improving safety of the services provided;

4.1.1.3. prevention of fraud and money laundering;

4.1.2. In the remaining cases, permission to use and transfer such information is governed by these Terms, the Law on personal data protection.

4.2. Information collected by other persons

4.2.1. The Bank is not responsible for the services of the System or another third-party Service Provider. Accordingly, any information, collected by the Service Provider when a Client uses a Digital Card or System, is governed by the contracts with the Service Provider and Third Parties.

4.3. Loss, theft or unauthorized use of the Client's Mobile Terminal

4.3.1. In case of loss or theft of the Mobile Terminal, use of the Card (Digital Card) or its details by a third party or use of the System without the Client's consent, the Client is obliged to notify the Bank immediately after the discovery of such facts.

4.3.2. In the event of a compromise or suspicion of compromising the Authentication data, the Client is obliged to immediately change the personal security information, Authentication data and make sure that only authorized fingerprints (Touch ID) are registered in the Mobile terminal in order to avoid any unauthorized use of the Digital card or personal information.

4.3.3. Upon receipt of the new Mobile Terminal, the Client is obliged to ensure that all Digital Cards, other personal information in the replaced mobile terminal are erased.

4.3.4. If needed, the client is obliged to assist the Bank in conducting any investigations and take measures to prevent fraud or other measures that may prevent unauthorized access to the Cards.

4.3.5. Certain functions and security measures may be used in the System and / or in the Mobile Terminal to ensure protection from unauthorized use of Digital Cards. Responsibility for such functions and procedures rests solely with the Service Provider. The Client undertakes not to disable such functions and use the specified functions and security measures to ensure the protection of all Digital Cards.

4.4. Protection of system, other authentication data and the Cards (which are selected to be used as digital cards).

4.4.1. The client is required to ensure the confidentiality of personal security information and authentication information. The Client is obliged to ensure their safety, as well as the safety of the Mobile Terminal in the same way that the safety of Bank Cards and other information, numbers and passwords confirming the Client's identity are ensured.

4.4.2. The Bank strongly recommends that the security information of the Digital Card be kept separately from the information used by the Client. Physical Bank Cards should not be stored with a Mobile Terminal, except for cases of Card registration in the System.

4.4.3. When you receive a text message, an e-mail stating that the Client has registered with the System, provided that the Client has not performed such registration, or if there are any operations that the Client did not recognize on the Mobile terminal or in the Card statement, immediately contact the Bank by phone: + 995 32 2 42 42 42.

5. Pausing, changing and cancellation of the functions

5.1. The Bank reserves the right to terminate the service or support of any Digital Card or participation in the System for any reason (on the basis of a notice). The Bank has the right to block, restrict, suspend or terminate the use of any Digital card by the Client in case of violation of these Terms, the Agreement, the Service Provider Terms and Conditions, as well as agreements with third parties, or if the Bank suspects fraudulent activity or abuse of the Digital Card.

5.2. The Service Provider reserves the right to block, restrict, suspend or terminate the use of the Digital Card by the Client and / or change the System functions without the consent of the Bank. The Client understands and agrees that in this case the Bank shall not be liable to the Client or a third party.

5.3. If the Bank detects fraud or any suspicious activity, the Bank has the right to take measures to block the Card, including the Digital Card, by notifying the client in different available ways: by a voice call, Push notification, SMS message or email.

5.4. After the temporary blocking or suspension of the Digital Card has been eliminated (for example, after carrying out a revision for fraud), the Client will be able to continue using the System services based on a corresponding notification.

5.5. The Client has the right to remove the Digital Card from the System by following the corresponding procedure in the System on the Mobile Terminal or contact the Bank by phone: 995 32 2 42 42 42 . In such circumstances, the client authorizes the Bank to continue processing of any non-fulfilled orders using the Digital Card.

6. Interruptions in the provision of Payment Services

6.1. Access, use and maintenance of a Digital Card depends on the scope of services of the System and the network of the wireless operator. The Bank is not the operator of the System or such network services and does not control their actions. The Bank shall not be liable to the Client for any circumstances that may interrupt, create obstacles or otherwise affect the operation of any Digital Card,

including unavailability of the System or wireless services, communications, network delays, wireless coverage restrictions, system interruptions or interruption of wireless communications.

6.2. The use of a Digital Card envisages electronic transfer of personal information through a third party connection. Since the Bank does not operate or control such connections, the Bank cannot guarantee the confidentiality or security of such data transmission.

7. Disclaimer

7.1. The Client agrees that the functions of the System and the Digital Card may be updated automatically without any additional notice. At any time, the Bank may decide to expand, reduce or suspend the types and / or volumes of operations provided by the Digital Card, or change the registration procedure. The right to update and modify the functions and functionality of the System does not include changes to the Agreement, which can be made only in accordance with the Agreement.

8. Changes to these Terms

8.1. The Bank reserves the right to unilaterally revise these Terms and Conditions in accordance with the Agreement. Any changes to these Terms and Conditions shall be communicated by the Bank to the Client via e-mail or using any other method of communication. The client has the opportunity to get acquainted with the revised Terms and Conditions on the mobile terminal. If the Client does not accept any changes made to these Terms, he is obliged to delete their Digital Card from the System by clicking on the “Delete Card” button in the System.

9. Communication

9.1. By registering the Card in the System, the Client automatically accepts Terms and Conditions stipulated by the Credo Bank.

9.2. The Client also agrees to receive notifications and other messages sent by the Bank regarding the status of the System services in the following ways:

9.2.1. Email

9.2.2. SMS messages;

9.2.3. Push Notifications;

10. Additional provisions

10.1. For any questions related to the support of Mobile terminals compatible with the System, the Client must contact the Service Provider directly.

10.2. For information about any restrictions or limits in relation to the System services, as well as minimum software and hardware requirements, the Client is obliged to contact the Service Provider directly.