Last updated: 31/03/2026

PAYMENT (DEBIT) CARD SERVICE TERMS AND CONDITIONS FOR INDIVIDUALS

These Payment (Debit) Card Service Terms and Conditions for Individuals (hereinafter the **"Terms and Conditions"**) constitute an annex to the General Agreement for the Provision of Services to Individuals (hereinafter the **"General Agreement"**) concluded between **JSC "Paysera Bank Georgia"** (identification number 402204841) and the **Client**. The consolidated version of the General Agreement is available at the following website. These Terms and Conditions shall enter into force upon the Client's confirmation of the card order application and shall remain in effect for the duration of the Client's use of either the physical and digital card

1. Definitions

Terms used in these Terms and Conditions shall have the following meanings:

One - Time Password (OTP) — a combination of randomly generated digits used to perform transactions when receiving remote banking services.

PIN — the cardholder's Personal Identification Number, which constitutes one of the authentication elements of the cardholder.

Card Account — the client's multi-currency current account to which the card is linked and on which transactions performed with the debit card are reflected.

Unauthorised Overdraft — a negative monetary balance on the client's card account resulting from: (a)an offline transaction; and/or (b) the settlement of the Client's outstanding liabilities to the Bank.

Offline Transaction — a transaction that is authorised or declined without establishing communication with the bank.

Card — a payment instrument issued by the bank by means of which the cardholder may initiate a card transaction.

Primary Card — where several cards are linked to the client's card account, the card that was linked to the card account first.

Supplementary Card — where several cards are linked to the client's card account, each card linked after the primary card is considered a supplementary card.

Debit Card — a card that enables the cardholder to dispose of the available funds in the card account on the basis of and in accordance with the agreement concluded with the bank.

Digital Card — a virtual card issued by the bank comprising a set of card credentials (including, but not limited to, the card number, expiry date, and security code), by means of which the cardholder may make payments subject to the applicable authentication measures.

Cardholder — an individual who is a client of the bank and/or a third party designated by the client to use the card.

Supplementary Cardholder — a person designated by the client to whom a supplementary card is issued.

Card Credentials — the card number; card expiry date; cardholder's name and surname; card security code (CVC2 or CVV2 — a security/authentication element).

Application — a document in a form and content pre - established by the bank through which the client's request for banking services is recorded.

Cash Withdrawal Transaction — a transaction involving the withdrawal of funds from the card account by means of the card.

Remote Communication Channels — ATM s , self - service payment terminals , mobile phone s , mail, e - mail, mobile banking, internet banking, or other means designated by the bank as an available communication channel.

Authorisation — the confirmation of a transaction through channels permitted by the bank, using the PIN and/or the security code on the reverse side of the card (CVV, CVC, etc.) and/or a 3D Secure code and/or a combination of such credentials and/or another mechanism establi shed by the bank, transmitted directly to the client/cardholder.

Terms not defined in this section shall be interpreted in accordance with the General Agreement and Georgian legislation.

2. General Terms of Card Services

2.1. Within the scope of the card services, the bank ensures the execution of card transactions and the corresponding adjustment of the card account balance by means of the VISA plastic/digital card issued by the bank (hereinafter the "Card").

2.2. The digital card may be used through remote banking service channel(s). In addition, the digital card may be:

2.2.1. added to the Apple Pay digital wallet;

2.2.2. added to the Google Pay digital wallet;

2.2.3. used to make payments at POS terminals through a digital wallet.

2.3. Under and in accordance with these Terms and Conditions, the client may use one or several debit cards, hold several card accounts, or have several cards linked to a single card account. The validity period of each physical card is indicated on the card surface, and in the case of a digital card — in the channel(s) designated for the use of the digital card (including internet banking/Paysera Super App). A card becomes invalid after the last day of the month indicated on the card.

2.4. The terms and conditions of use of both physical and digital cards are set out in detail in these Terms and Conditions, the General Agreement, and the informational materials published on the bank's website relating to the card, including:

2.4.1. Card Information and Frequently Asked Questions (FAQ) Web Page.

2.4.2. Card Security Requirements Information Web Page.

2.4.3. Card Service Fees and Limits Information Web Page.

2.4.4. Information on conversion schemes — available on the bank's website.

2.4.5. Detailed information on the VISA card and international payment systems is available on the following Web Page.

2.5. To use the card, the client is required to pay the bank a service fee in accordance with the tariffs established by the bank. Information on the tariffs established by the bank and the frequency of payment is available on the following Web Page .

2.6. The client is entitled to use multiple cards linked to a single card account (primary and supplementary cards). In this case, the card linked first to the card account is considered the primary card, while the card subsequently issued to the client and/or to a third party designated by the client is considered a supplementary card. The limit of supplementary cards per account is 20 cards in total, including embossed, digital, and physical cards.

3. Card Order and Activation Procedure

3.1. To obtain a physical or digital card (whether primary or supplementary), the Client must complete and confirm the relevant application through the mobile banking application (Paysera Super App) and/or internet banking. Upon confirmation of the application for the issuance of a physical card, the card issuance fee will be debited from the Client's existing current account.

3.2. The client is entitled to request the production of a supplementary card both for personal use and for use by a third party designated by the client (the cardholder).

3.3 Delivery of a physical card to the cardholder is carried out at the bank's service centre or, at the client's instruction, by postal service, following deduction of the applicable fee and within the timeframe agreed between the bank and the client at the time of the card order. In each case, the physical card is transferred on the basis of a handover and acceptance act signed between the cardholder and the bank. Prior to signing the handover and acceptance act, the cardholder must verify that the physical card delivered corresponds to the request recorded in the application, that the card shows no visible damage, and that the special envelope containing the card is sealed and undamaged. Confirmation of card receipt is made through internet banking or mobile banking (Paysera Super App) by pressing the "I have received the card" button.

3.4. Following receipt of the physical card, the client must activate the card. Activation is carried out through internet banking or mobile banking by entering the card's CVV code in the card activation tab. The physical card cannot be used without completing the activation procedure. The client must take delivery of the physical card within 3 (three) months of its production. If the client fails to comply with the three-month period, the card will be automatically blocked upon expiry of the specified period. A digital card is activated immediately upon confirmation of the card order.

3.5. To activate the contactless payment function of the card, the client must perform a transaction using the card’s chip by inserting it into a POS terminal or an ATM. It is recommended that the Client changes the temporary PIN immediately after receiving the card.

3.6. Following card activation, the PIN can be viewed by the client Client through the designated section in internet banking and/or the mobile application.The PIN may be changed at any ATM globally that is part of the Visa network.

3.7. If the client fails collect the physical card within the specified delivery period or if the Cardholder otherwise fails to take delivery of the card, the Bank shall be entitled to destroy the card without prior notice. In such instances, the card issuance fee and any postal service charges paid by the Client shall be non-refundable.

3.8. Following activation of the digital card, the digital card credentials are accessible to the client through the channel(s) designated for the use of the digital card — internet banking or mobile banking.

3.9. The card and card credentials including the PIN, CVV/CVC code, one-time OTP code, and any other identification or security credentials related to the card, constitute confidential information.

4. Card Usage Rules

4.1. Following card activation, the client shall be entitled, in accordance with these Terms and Conditions, to manage the funds available in the card account(s).

4.2. Throughout the entire period of card use, the client must ensure that the card account holds sufficient funds for the deduction of fees established by the bank.

4.3. The bank is entitled to set maximum transaction limits for the use of funds through the card within a specified period, to establish transaction limits, and/or to restrict specific transactions. Restrictions on card payments at high-risk merchants/service providers (including gambling establishments and other high-risk categories designated by the National Bank of Georgia) constitute a client protection mechanism and are imposed in accordance with Georgian legislation.

4.4. The client is entitled to manage funds in the currencies available within the card account. Where funds are used in a currency other than the card account currency, a conversion will be applied when debiting funds from the client's account, in accordance with the commercial exchange rate established by the bank at the time of the transaction. Detailed information on conversion schemes is available on the bank's website.

4.5. Currency priority is determined by the bank. Information regarding the Card Account balance is displayed in the priority currency, based on the Bank's commercial exchange rate for that day. The Base Currency (primary currency) of the Card is the Georgian Lari (GEL). Additional available currencies include: EUR, USD, DKK, PLN, NOK, GBP, SEK, CZK, AUD, CHF, JPY, CAD, HUF, RON, NZD, HKD, INR, MXN, SGD, and ALL./p>

4.6. Card transactions are initially recorded in the currency in which the transaction was performed. If the Client does not hold sufficient funds in the transaction currency within the corresponding Card Account, the settlement of such transaction shall be carried out in the national currency (GEL).

4.7. The client shall receive push notifications for card transactions through the mobile banking application (Paysera Super App). The client may also activate the SMS notification service. If, following Card activation, the Client chooses to use only internet banking, the Client must activate the SMS notification service to ensure they receive transaction alerts. Failure to do so shall exempt the Bank from any responsibility regarding the Client's failure to receive notifications

4.8. The digital card becomes active upon issuance, independently of the physical card. In the event that the physical card is destroyed or deactivated, the Digital Card remains active until it is cancelled by the Client or until the Card’s expiry date.

4.9. Card issuance, cancellation, and all other card-related operations performed by the Client shall be confirmed via internet banking and/or the mobile application.

4.10. ¿Upon the Client's performance of a Card transaction, the Bank shall be entitled, upon receipt of the payment order, to block (hold) an amount on the Client's Card Account sufficient to execute the authorized transaction (including any applicable Bank fees). Where currency conversion is required for the execution of the transaction, such conversion shall be performed at the commercial exchange rate established by the Bank (see the following website).

4.11. The timeframes for executing card transactions and their reflection on the account may differ —the settlement period depends on the processing timeframes of the international payment system. Payments made via the internet and/or transactions carried out through the network of another bank are reflected on the account after processing by the relevant payment system; the maximum processing period for such transactions generally does not exceed 30 calendar days.

4.12. Information on transactions performed by the client is accessible through internet banking and mobile banking.

4.13. At the clearing (settlement) stage, transaction amounts are debited as follows:

4.13.1. If the blocked (held) amount corresponds exactly to the final settlement amount of the transaction, the debit is made directly from the account of the corresponding currency. If the balance of that account is insufficient, the bank shall collect the remaining funds from the Client's other currency account(s) based on available balances, utilizing the commercial exchange rate established by the Bank at the time of settlement.

4.13.2. If the blocked (held) amount does not correspond to the final settlement amount, an unauthorised overdraft may arise on the account of the corresponding currency. In such an event: the negative balance shall first be covered by funds from the Priority Currency Account (GEL). If the Priority Currency Account holds insufficient funds, the coverage shall continue from other currency account(s) based on available balances. Currency conversion shall be performed at the commercial exchange rate established by the Bank at the time of settlement. This conversion process shall continue until the total transaction amount is fully settled.

5. 3D Secure Service

5.1. The bank provides the cardholder with the 3D Secure service (Verified by Visa) for the protection of online transactions. The service is enabled automatically and is provided free of charge.

5.2. Under the 3D Secure service, when performing an online transaction, a one-time password (OTP) is sent to the cardholder's mobile banking application. The Cardholder is strictly obliged to maintain the confidentiality of the OTP and must not disclose it to any third parties.

5.3. The terms of the service, exceptions (including cases involving saved cards and recurring transactions), and the procedure for updating the service are set out in the 3D Secure service description published on the bank's official website, accessible on the following website. This description forms an integral part of these Terms and Conditions.

6. Unauthorised Overdraft

6.1. In the event of an Unauthorized Overdraft, the Client's Card Account shall be debited accordingly, and the Client/Cardholder shall be notified of the overdraft via a push notification in the mobile application. The Client is also entitled to activate the SMS notification service to receive such alerts.

6.2. In the event of an unauthorised overdraft, the client must immediately, and in any case no later than upon receipt of the notification, replenish the Card Account with an amount at least sufficient to restore the balance to zero.

6.3. Interest shall accrue on the amount of the Unauthorized Overdraft utilized by the Client at an annual rate determined by the Bank's tariffs applicable at the time the overdraft arises. This interest is calculated on the basis of a 365 (three hundred sixty-five) day year. Interest shall accrue on the Unauthorized Overdraft from the date it originates until the date of full and final repayment (actual settlement).

6.4. In the case of a multi-currency Card Account, if an Unauthorized Overdraft exists on any currency subaccount, any funds deposited or credited to the Card in any currency shall be automatically converted and applied to cover the Unauthorized Overdraft. Such conversion shall be performed at the Bank’s commercial exchange rate applicable on the date of the transaction. For the purpose of settling any Unauthorized Overdraft, the Bank is entitled to debit the required amount from any other account held by the Client with the Bank without the Client’s further consent (Direct Debit). Where the Client’s liability is denominated in a currency other than the national currency, the equivalent amount shall be determined based on the Bank’s commercial exchange rate at the time of the debit.

6.5. In the event that a collection order or attachment (legal lien) is placed on any account of the Client/Cardholder, any existing overdraft facility shall be deemed automatically cancelled. Upon the execution, withdrawal, or cancellation of the collection order, or upon the lifting of the attachment, the Bank reserves the right to unilaterally reinstate the overdraft.

7. Unauthorised Card Transactions

7.1. An unauthorised transaction is a transaction that has not been performed on the basis of consent (authorisation) given by the client.

7.2. If the client/cardholder considers that an unauthorised and/or incorrectly executed transaction has been performed on the account, the client/cardholder must block the card through internet banking or the mobile application (Paysera Super App) and notify the bank immediately upon discovery of the transaction, without undue delay, using the communication channels provided for in the General Agreement.

7.3. Upon receipt of a notification from the cardholder of loss, theft, misappropriation, or an unauthorised transaction, the bank is obliged to ensure that further use of the card is restricted (card blocking).

7.4. If the client claims that a transaction is unauthorised, the client/cardholder must ,during the investigation conducted by the bank, provide the bank with all necessary evidence, including, upon the bank's request, any information in their possession or accessible to them regarding the circumstances of the transaction, in order to determine whether the transaction was authenticated and/or correctly executed.

7.5. The client/cardholder bears full liability for losses arising from unauthorised payment transactions caused by the client's fraudulent conduct and/or intentional or grossly negligent failure to comply with obligations stipulated by the General Agreement, these Terms and Conditions, and other related terms and conditions and/or applicable legislation.

8. Card Blocking and Cancellation

8.1. The client is entitled to block the card through the relevant tab in internet banking and/or mobile banking (Paysera Super App) following authentication. A card blocked by the client may be unblocked by the client through the bank's application and/or by contacting the bank.

8.2. In the event of loss or theft of the card, the cardholder is also entitled to request that the card be placed on the international stop list, which ensures complete blocking of the card at the international level. Placement of the card on the international stop list is subject to the tariffs established by VISA and requires the availability of sufficient funds in the client's account to cover the applicable fee.

8.3. For security purposes, the card is automatically blocked in the following circumstances:

8.3.1. three consecutive incorrect PIN entries at an ATM;

8.3.2. three consecutive incorrect CVV code entries when making an online purchase;

8.3.3. in cases of attachment, collection, or other circumstances provided for by law;

8.3.4. automatically by the processing centre, where the processing centre's software has detected any attempt at fraud.

8.3.5. In addition to automatic blocking, the card may be blocked at the client's request and/or by a decision of the bank, as set out in these Terms and Conditions.

8.4. The card operation will be suspended following the client's/cardholder's expression of intent to block the card vis-à-vis the bank.

8.5. The bank is entitled to immediately block the card and/or prevent its further use if there are reasonable grounds to suspect that the payment instrument is being used or may be used for unauthorised transactions, including fraudulent and/or unauthorised use, if security standards are being violated, and/or such blocking is

appropriate for other reasons, and/or if the cardholder is in breach of the General Agreement, the card services terms, and/or has an overdue liability to the bank. In such case, the cardholder will be immediately notified of the action taken through a communication channel permitted under the General Agreement.

8.6. In the event that the cardholder breaches any of the terms set out in these Terms and Conditions or in the card usage rules, the bank may at any time block or cancel the card.

8.7. The bank is entitled to close the card and/or the card account in the following cases:

8.7.1. upon termination of the agreement between the bank and VISA, on the basis of a notification sent to the client regarding the closure of the card account;

8.7.2. upon the client's written request — within 30 (thirty) calendar days of the client's application;

8.7.3. upon expiry of the card's validity period — automatically;

8.7.4. in the event of a material breach by the client of the obligations assumed under the agreement or these Terms and Conditions — on the basis of a notification sent to the client no less than 5 (five) business days in advance.

8.8. Following the closure of the Card or Card Account, the Client must, within 10 (ten) calendar days, return the Card to the Bank or provide proof of its destruction. The failure to return the Card shall not release the Client from any outstanding obligations or liabilities assumed under these Terms and Conditions.

8.9. The closure of the Card or Card Account shall not result in the automatic closure of the Client's other accounts or banking products, unless such closure is explicitly required by the Agreement or by applicable legislation.

9. Rights, Obligations, and Liabilities of the Parties

9.1. The client/cardholder is obliged to:

9.1.1. Retain all documents confirming card transactions and submit them to the bank in the event of a dispute;

9.1.2. Maintain the confidentiality of the card, card data (including PIN, CVV/CVC, OTP), mobile device, and any other identification information related to the card, and not transfer or disclose such information to third parties. The client bears full liability for all transactions performed using the client's access credentials.

9.1.3. At the end of each calendar month, review all transactions carried out via the card to verify their accuracy and, where necessary, notify the bank in writing of any discrepancy or disputed transaction within the period established by these Terms and Conditions and the applicable legislation.

9.1.4. Immediately, without undue delay, notify the bank via the 24/7 hotline: (+995 32) 2 22 55 22 or through the internet/mobile banking notification service of any loss, theft, misappropriation of the card, card data, mobile device, or card-related accessories, or of the occurrence of an unauthorised transaction, or of any suspicion thereof.

9.1.5. In the event of disputed card transactions, if the client has notified the bank without undue delay upon discovery of an unauthorised or incorrectly executed transaction , the client is entitled to submit a written request to the bank for corrective action in respect of the unauthorised or incorrectly executed transaction

within 13 (thirteen) monthsom the date the transaction was debited to the account. Such written application in the case of an international transaction must be submitted without undue delay, but no later than 75 days from the date of the debit.

9.1.6. Reimburse the bank for any expenses related to additional paid services provided by VISA in respect of the card, where applicable.

9.1.7. The client must ensure that the contact details registered with the bank (mobile phone number, e-mail address) are accurate and up to date. The mobile number registered with the bank is the sole channel for receiving OTP codes under the 3D Secure service. If the mobile number is incorrect or outdated, the client will not be able to use the 3D Secure service. The bank will not be liable for consequences arising from the client's failure to update contact details.

9.1.8. If the client suspects that the client's access credentials (password, PIN, OTP) or card data have become known to a third party, or that the client's account has been placed at real risk, the client must immediately:

9.1.8.1. change passwords in the bank's mobile/internet banking; and

9.1.8.2. notify the bank on the 24/7 hotline: (+995 32) 2 XX XX XX or through the mobile/internet banking notification service to block the card.

9.1.8.3. The bank will not be liable for consequences arising from failure to notify and/or disclosure of passwords.

9.1.8.4. The client/cardholder must immediately update their contact details in the event of any change, in accordance with the procedure established by the bank. The bank shall not be liable for failure to provide information to the client if the client has changed contact details without notifying the bank.

9.2. The client is entitled to:

9.2.1. Request a supplementary card, the opening of additional card account(s), the cancellation, blocking, or unblocking of a supplementary card;

9.2.2. Request the cancellation of the card and/or the closure of the card account;

9.2.3. Change the PIN of both the primary and supplementary card;

9.2.4. At any time and on multiple occasions,to apply to the bank in accordance with the procedure established by the bank, requesting the activation or re-blocking of payments at high-risk merchants/service providers. The client acknowledges that such activation is carried out at the client's own risk, and the bank will not be liable for any loss resulting from activated payments.

9.2.5. Submit a claim to the bank regarding transactions performed by means of the card (both digital and physical), either orally or in writing (electronically to: claims@paysera.ge; tel: +995 32 2 22 55 22). The client's application must be submitted without undue delay from the time the transaction was recorded. The procedure and conditions for submitting a complaint and for its examination by the bank are available at the following website.

9.3. Liability of the Client

9.3.1 The client is liable for losses arising from unauthorised transactions resulting from the loss, theft, or misappropriation of the payment instrument, or from its unauthorised use, up to a maximum of GEL 100, unless one of the following conditions is met:

9.3.2 discovery by the user of the loss, theft, or misappropriation of the payment instrument was not possible prior to the execution of the transaction;

9.3.3 the loss was caused by the act or omission of the bank, its agent, or an outsourcing company.

9.3.4 The client bears full liability for losses arising from unauthorised payment transactions caused by the client's fraudulent conduct, as well as by the client's intentional or grossly negligent non-compliance with one or more obligations stipulated by the General Agreement, these Terms and Conditions, and/or applicable legislation. In such case, the maximum liability amount set out in clause 9.3.1 of these Terms and Conditions does not apply.

9.4. The bank is liable for:

9.4.1. Taking immediate and appropriate action upon receipt of a notification from the Cardholder regarding the loss or theft of the Card, and assuming liability for any consequences resulting from a failure to take such action.

9.5. The bank will not be liable for:

9.5.1. Card transactions performed using a lost and/or stolen card, if the cardholder failed to ensure the timely blocking of the lost/stolen card and/or to notify the bank accordingly;

9.5.2. Offline card transactions executed in accordance with the rules of the international payment system in real time without the bank's authorisation;

9.5.3. Any card transaction caused by the client's disclosure of confidential data (PIN, CVV, OTP);

9.5.4. Delayed, incorrect, or unexecuted transactions caused by the international payment system or other technical reasons beyond the bank's control;

9.5.5. If the client has lost the client's profile password or another password, or it has become known to a third party without fault/cause on the part of the client or Paysera, or if a real risk has arisen or may arise to the client's profile, the client undertakes to immediately change the passwords, or, if this is not possible, to immediately notify Paysera through the means specified in Article 10 of the General agreement. Paysera will not be liable for consequences arising from failure to notify.

9.5.6. The bank will not be liable for transactions carried out by the client using the card on the internet or at merchants/service providers, and for the consequences and risks arising therefrom.

9.5.7. In the event of a disputed transaction with a merchant/service provider, the bank will act in accordance with the rules and procedures of Visa International — the bank does not guarantee the refund of a disputed amount if the matter is not resolved in the client's favour by the international payment system.

9.5.8. The bank is not obliged to reimburse the amount of an unauthorised transaction if there are reasonable grounds to suspect that the client has engaged in fraudulent conduct and/or has intentionally or with gross negligence breached an obligation under applicable legislation, the agreement, or these Terms and Conditions. In such case, the established limit of GEL 100 will not apply.

10. Final Provisions

10.1. The client's consent to these Terms and Conditions granted through remote banking services will be equivalent to the client's handwritten signature and will have equal legal force.

10.2.By confirming these Terms and Conditions, the client also confirms having read and agreed to the bank's Personal Data Protection Policy, and grants consent for the bank, without the client's prior or additional consent, to process/transfer the client's personal/confidential data to payment card schemes (Visa), payment systems, and intermediary/acquiring banks for the purpose of providing services.

10.3.The supervisory authority of JSC "Paysera Bank Georgia" is the National Bank of Georgia (address: 1 Zviad Gamsakhurdia Embankment, Tbilisi 0114; website: https://www.nbg.gov.ge). The supervisory authority is not liable for Paysera's improper performance of its obligations.

10.4.For useful information for consumers, visit the National Bank of Georgia's website at www.nbg.gov.ge/cp or call the hotline: 032 2 406 406.