Slovenská sporiteľňa, a.s.
Tomášikova 48
832 37 Bratislava
www.slsp.sk

Client Centre
0850 111 888
info@slsp.sk

ID. No.: 00151653
Tax No.: 2020411536
VAT No.: SK7020000262

Commercial Register: Municipal Court Bratislava III, Section: Sa, File No.: 601/B

Publication effective from 1 January 2026

PUBLICATION ON DEBIT PAYMENT CARDS
(natural person – sole trader, legal entity, public and non-profit sector)

PAYMENT CARDS ISSUED BY THE BANK FOR BUSINESS ACCOUNTS

Visa Business electronic, Visa Business, Visa Business Platinum, Deposit Business Card

PAYMENT CARD LIMITS

Unless the Bank and the Client agree otherwise, the Client's Payment Card has the following defined Card Limits:

Type of Payment Card	Daily Cash Limit	Daily Non-Cash Limit*	Daily Limit for Online Payments and Ordering Goods*	Daily Total Limit*
Visa Business electronic	€ 3,000	€ 3,000	€ 3,000	€ 6,000
Deposit Business Card	€ 0	€ 0	€ 0	€ 0
Visa Business	€ 5,000	€ 6,000	€ 6,000	€ 11,000
Visa Business Platinum	€ 10,000	€10,000	€ 10,000	€ 20,000

SLOVENSKÁ sporiteľňa

MAXIMUM PAYMENT CARD LIMITS

Type of Payment Card	Maximum Daily Cash Limit	Maximum Daily Non-Cash Limit	Maximum Daily Limit for Online Payments and Ordering Goods	Maximum Daily Total Limit*	Maximum Daily Cash Limit for ATM Deposits**
Visa Business electronic	€ 3,000	€ 10,000	€ 10,000	€ 15,000	€ 20,000
Deposit Business Card	€ 0	€ 0	€ 0	€ 0	€ 20,000
Visa Business	€ 5,000	€ 20,000	€ 20,000	€ 30,000	€ 20,000
Visa Business Platinum	€ 10,000	€ 50,000	€ 50,000	€ 60,000	€ 20,000

* Does not include the Maximum Daily Cash Limit for ATM deposits
** Not included in the Maximum Daily Total Limit

PERMITTED TRANSACTIONS PERFORMED WITH A PAYMENT CARD

Unless otherwise agreed between the Bank and the Client, the Bank shall issue the Client with a Payment Card with the following permitted operations for the use of the Payment Card:

a) ATM withdrawal
cash withdrawal from ATM in Slovakia or abroad;
b) POS withdrawal
cash withdrawal via POS at banks;
c) payment
cashless payment for goods and services at Merchants in Slovakia or abroad via POS (for embossed cards also via imprinter);
d) contactless payment
cashless payment for goods and services at Merchants in Slovakia or abroad using contactless functionality;
e) balance
information about the available balance on the Account via the Bank's ATM;
f) turnover
information about Account turnover via the Bank's ATM;
g) payment for telecommunications services
cashless top-up of mobile operator credit;
h) online payments and ordering goods
online payments and orders by telephone or post (MO/TO);
***i)* ATM deposit;**
cash deposits via the Bank's ATM with deposit function (the only type of transaction permitted on the Deposit Business Card); cash will be credited to the account to which the Payment Card is issued.

INFORMATION ON THE PAYMENT CARD

The Payment Card shows the Payment Card number, its expiry date and the name of the Card Holder, or other details depending on the type of Payment Card. Payment Card details (number

and expiry date of the Payment Card and CVV2 Code) are also displayed to the Card Holder in the George mobile application of the Internetbanking Electronic Service.
Payment Card that can be used for Contactless Transactions is also marked with the payWave logo or the contactless payment symbol .
The validity of the Payment Card is also indicated on the Payment Card. The validity of the card expires on the last day of the month indicated on the Payment Card. The validity of the card also expires on the date specified by the Bank as the last day of provision of the specified type of Payment Card by the Bank.

SECURITY FEATURES ON THE PAYMENT CARD

The Payment Card is secured by security features such as a hologram and card company logo, magnetic strip, chip and CVV2 Code. Some Payment Cards may also include a signature strip with the Card Holder's signature.

An embossed Payment Card has raised lettering and can be used in an electronic environment as well as for mechanical scanning of personalisation data from the Payment Card (e.g. withdrawal or payment via an imprinter). An electronic (non-embossed) Payment Card does not have embossed lettering and can only be used in an electronic environment (e.g. at an ATM, POS terminal, for online payments, etc.).

STRONG CLIENT AUTHENTICATION

Strong Authentication is a procedure for verifying the identity of the Card Holder when making payments with a Payment Card via the internet, which is intended to contribute to greater payment security by verifying the Card Holder on the basis of two or more different characteristics of the Card Holder, characterised as knowledge, possession or inherence. The Bank uses Strong Client Authentication for all types of cards.

George ID

When Strong Authentication is applied by the Bank for remote payment by Payment Card without its physical presentation, after the Card Holder enters the card information (card number, expiry date and CVV2 Code) during the purchase, a notification will be sent to the Card Holder in the George application; if the Card Holder has not activated or deactivated notifications in the George application, the Card Holder will have the Payment Card information available in the George application. After clicking on this notification or logging into the George application on a device owned by the Card Holder, the Card Holder will be shown summary information about the online payment they have initiated and the Card Holder will be asked to confirm it and complete the authentication by entering a second characteristic element, which will be the agreed PIN number, fingerprint or facial scan of the Card Holder (depending on which element the Card Holder has selected in the George application settings). Correct entry of the agreed second characteristic element will confirm the payment and complete the Card Holder's Strong Authentication.

Activating George ID will cancel the SMS key or mToken for authorising (signing) payment Instructions using a Payment Card on an online retailer's website.

If the Client has both George ID and ePIN activated, when paying by Payment Card, the Client will first be asked to confirm and complete authentication via George ID in the George application.
The Card Holder can activate and deactivate George ID and activate and change ePIN in the George version of the Internetbanking Electronic Service in the manner and under the conditions specified in the Disclosure on Electronic Services.

mToken

When the Bank applies Strong Authentication for remote Payment Card payments without physical presentation of the card, after the Card Holder enters the card information (card number, expiry date and CVV2 Code) during the purchase, a notification will be sent to the Card Holder in the mToken application. After clicking on this notification on the device owned by the Card Holder, the Card Holder will be shown summary information about the internet payment they have initiated and the Card Holder will be asked to

confirm it and complete the authentication by entering a second characteristic element, which will be an agreed 6-digit PIN number, fingerprint or facial scan of the Card Holder (depending on which element the Card Holder has selected in the mToken application settings). Correct entry of the agreed second characteristic element will confirm the payment and complete the Card Holder's Strong Authentication.

ePIN

The ePIN is used to apply Strong Authentication by the Bank when making a remote payment with a Payment Card without physically presenting it. If the Card Holder has multiple Payment Cards issued, the ePIN applies to all of the Client's Payment Cards.
When making a purchase online, the Card Holder enters their Payment Card details (card number, expiry date and CVV2 Code), enters their ePIN and 3D Secure Code (if supported by the online merchant). Correct entry of the agreed additional characteristic element, which is the ePIN, will confirm the payment and complete the Card Holder's Strong Authentication.

If the Client has both mToken and ePIN activated, when paying with a Payment Card, the Client will first be asked to confirm and complete authentication by entering mToken. The Card Holder can activate and deactivate mToken and activate and change ePIN in the George or Business24 Internetbanking Electronic Service in the manner and under the conditions specified in the Disclosure on Electronic Services.

3D SECURE

If the Internet Merchant supports 3D Secure, the Card Holder may be asked to enter card information (card number, expiry date and CVV2 Code) when making a purchase. The Card Holder will then be asked to confirm the payment with an authorisation SMS code, which will be sent in an SMS message to the Card Holder's mobile phone number provided to the Bank as a contact number. For successful verification of the Card Holder's identity, the Card Holder must meet the technical requirements, provide the Bank with a mobile phone number as a contact number, and set the Payment Card Limit for online and MO/TO payments to an amount greater than zero (0) EUR. The Card Holder acknowledges that if they have provided the Bank with an incomplete or incorrect mobile phone number or have not notified the Bank of any change to that number, this may result in payment made with the Payment Card not being successfully processed or being processed by an unauthorised person.

DELIVERY OF PAYMENT CARDS

If the Bank and the Client do not agree on the method of delivery of the Payment Card, the Payment Card will be delivered to the Client by post to the Client's address. The estimated delivery time is 10 working days from the date of submission of the application and, in the case of Express Delivery (not applicable to the Own Card service), 3 working days.

The Payment Card is delivered by regular post. The above-mentioned deadlines are for information purposes only.
Unless the Bank agrees with the Client on another method of PIN number delivery, the PIN number is delivered to the Client via the Electronic Service.

If the Bank learns in a credible manner of the death of the Card Holder, or if the Card Holder does not collect and activate the Payment Card delivered to the Branch within 90 days of the date of its production, the Bank shall cancel the Payment Card and the Contract on the basis of which this Payment Card was issued shall terminate in respect of the Payment Card issued to the Card Holder.

DAMAGED SHIPMENT

If the shipment containing the Payment Card or PIN number is damaged, or if the Client does not receive

this shipment, the Client shall immediately inform the Bank thereof. The Bank shall then arrange for the production of a Replacement Card and the issuance of a new PIN number for the Client.

ACTIVATION OF THE PAYMENT CARD

The Client activates the Payment Card by entering the PIN number correctly for the first time when using the card, or via the George version of the Internetbanking Electronic Service, Business24 version or by telephone via the Client Centre by providing the Payment Card number and confidential data if agreed in the Payment Card Contract, or by providing another Authentication Code.

Activation of the Renewed Card does not result in deactivation of the previous Payment Card. The validity of the previous Payment Card will expire on the last day of the month indicated on the previous Payment Card, but the Client may deactivate it earlier via the Internetbanking Electronic Service, Business24 version or by telephone via the Client Centre by providing the Payment Card number and the confidential data agreed in the Payment Card Contract, or by providing another Authentication Code.
The Card Holder is entitled to change the PIN number issued for the Payment Card via an ATM of the Bank or another bank, provided that the ATM in question allows this service to be provided.

CONFIDENTIAL DATA

If the Bank agrees with the Client in the Payment Card Contract on a confidential data, this serves to identify the Client in remote communication with the Bank. The confidential data agreed for the Payment Card in a later concluded agreement on the issuance and use of the Payment Card replaces all previously agreed confidential data for Payment Cards issued by the Bank to the Client.
In justified cases, the Bank may also accept confidential data for a Payment Card that was not agreed with the Client as the last one.

RESTRICTIONS ON THE ISSUANCE OF A RENEWED CARD

A Renewed Card is usually issued two months before the expiry date of the original Payment Card. The Client is entitled to cancel the issuance of a Renewed Card in advance via the George Internetbanking Electronic Service. The Bank will issue the Client a Renewed Card with the same Payment Card number, and the PIN number for the original Payment Card will remain valid for the Renewed Card.
For security or technical reasons, the Bank may change the Payment Card number when issuing a Renewed Card, or may also change the PIN number for the Renewed Card.
For technical reasons, it is not possible to make certain changes to the Payment Card or change the terms and conditions of its use during the 8-week period prior to the expiry of the Payment Card until the expiry of the Payment Card.
If the Client changes the PIN number on the original Payment Card via an ATM during the period of 8 weeks prior to the expiry of the original Payment Card until the expiry of this Payment Card, the PIN number will only be changed on the original Payment Card, but not on the Renewed Card. If the Client changes the PIN number on the Renewed Card during this period, the PIN number will only be changed on the Renewed Card, while the PIN number for the original Payment Card will not be changed.
The Bank is not obliged to allow the Client to change the PIN number via an ATM on this Payment Card during the period of 8 weeks before the expiry of the original Payment Card until the expiry of this Payment Card.

BLOCKING THE CONTACTLESS FUNCTIONALITY ON THE PAYMENT CARD

The Client may request the Bank to block and subsequently unblock the contactless functionality on the Payment Card. Blocking and subsequent unblocking of the contactless functionality on the Payment Card is subject to a fee in accordance with the valid Service Charge List.
In the event of unauthorised overdraft of the Account to which the Payment Card is issued, the Bank may temporarily block the contactless functionality on the Payment Card. The contactless functionality will be automatically unblocked by the Bank upon simultaneous fulfilment of the following conditions:

a) the unauthorised overdraft is settled and
b) the available balance on the Account to which the Payment Card is issued is at least EUR 60

c) once the conditions specified in points a) and b) have been met, a transaction will be made using the Payment Card, which will be authorised by entering the PIN number or by signing the Sales Receipt with a signature matching the signature on the back of the Payment Card.

PAYMENT CARD BLOCKING

The Client may request the blocking of the Payment Card via the George Internetbanking Electronic Service, the Business24 Electronic Service, by telephone via the Client Centre service or in person at any Branch.

In the case of a telephone request, the Bank will block the Payment Card after identifying the Client and after the correct entry of the confidential data or another Authentication Code. In justified cases, the Bank will block the Payment Card even without the disclosure of the confidential data or another Authentication Code. In such cases, the Bank may require the Client to provide additional identification and other verification data necessary for the purposes of his/her identification. The Client shall never disclose the PIN number.

Through the George Internetbanking Electronic Service, the Card Holder may request the Bank to block the Payment Card of which he/she is the holder due to loss, theft or misappropriation. The Card Holder hereby also requests the Bank to issue a Replacement Card. If the Card Holder is not interested in having a Replacement Card issued, the Payment Card will be temporarily blocked.

The account holder may request the blocking of any Payment Card issued to the Account. The Card Holder may only request the blocking of the Payment Card of which he/she is the holder. In exceptional cases, the Bank may also block a Payment Card at the request of a third party, provided that such party proves the credibility of the request.

In order to prevent or minimise damage in the event of reasonable suspicion of possible misuse of a Payment Card, as well as in cases where such an obligation arises for the Bank under applicable law, the Bank may block a Payment Card on its own initiative, even without a request from the Client. For the same reasons, the Bank is also entitled to take and implement other security measures to protect the Client, their funds, the Payment Card and the Bank. For these reasons, the Bank may issue a Replacement Card to the Client without the Client's request. The Bank shall inform the Client of the blocking of the Payment Card and the reason for the blocking without undue delay in an appropriate manner. Once the reason for the blocking has ceased to exist, the Bank is entitled, but not obliged, to cancel the blocking of the Payment Card, taking into account the security of further use of the Payment Card in its decision. The Bank shall inform the Client of the cancellation of the blocking in an appropriate manner.

After blocking the Payment Card, the Bank is not obliged to issue a Replacement Card to the Client.

The Client may request the Bank to unblock the Payment Card at any time. If the reason for which the Payment Card was blocked still persists, the Bank is not obliged to comply with this request. In the event of a Payment Card being blocked for reasons other than at the Client’s request, the Bank may lift the block if the reasons for such block have ceased to exist.

TEMPORARY BLOCKING OF THE PAYMENT CARD

The Client may request a temporary blocking of the Payment Card via the George Internetbanking Electronic Service. The Client may lift the temporary block of the Payment Card at any time via the George Internetbanking Electronic Service.

During the temporary blocking, it is not possible to perform authorised transactions with the Payment Card. The Bank does not investigate the Client's reasons for temporarily blocking or unblocking the Payment Card.

CANCELLATION OF A PAYMENT CARD VIA THE GEORGE INTERNETBANKING ELECTRONIC SERVICE

The account holder may request the cancellation of any Payment Card issued for the Account via the

George Electronic Service. The Card Holder may only request the cancellation of a Payment Card of which they are the holder via the George Electronic Service. The cancellation of a Payment Card shall be deemed a termination of the Contract under which the Payment Card was issued.

ISSUANCE OF A REPLACEMENT CARD

The Bank shall issue a Replacement Card to the Client after the Client reports its loss, theft, damage, non-delivery or change of details (first name and surname) stated on the card to the Bank.
If the Client requests the Bank to issue a Replacement Card due to damage to the Payment Card, the Payment Card will be automatically blocked until the Replacement Card is activated.
The Bank shall issue a Replacement Card also at the Client's request; in justified cases, the Bank may issue a Replacement Card automatically. The Bank may refuse to issue a Replacement Card in justified cases. The Bank shall issue a Replacement Card with a new card validity period. When issuing a Replacement Card, the Bank may, for security or technical reasons, change the Payment Card number and PIN number associated with that card.

AUTHORISATION FOR THE CARD HOLDER

By entering into an agreement for the issuance of a Payment Card for the Card Holder in respect their Account, the account holder authorises the Card Holder to request the Bank at any time during the term of the Payment Card contract in relation to the Payment Card issued in the name of the Card Holder, to request the Bank to:

a) activate the Payment Card issued in the name of the Card Holder,
b) request the reissuance of the PIN number for such Payment Card,
c) cancel such Payment Card,
d) temporarily block and unblock such Payment Card.

The account holder authorises the Card Holder to enter into, amend and if necessary, terminate the travel insurance contract for the Payment Card issued to the Card Holder at any time during the term of the Payment Card Agreement. The Bank is entitled to debit the account holder's Account with the amount corresponding to the annual insurance premium in accordance with the travel insurance contract for the Payment Card, if the Card Holder has concluded such an insurance contract, and to transfer this amount to the insurer's account even without a payment order, even if there are insufficient funds in the Client's Account, in which case the Bank is entitled to debit this amount from the Client's Account, even into unauthorised overdraft.
The account holder may authorise the Card Holder via the Electronic Services to perform further actions to the extent permitted by the relevant Electronic Service.

PAYMENT CARDS THAT NEED TO BE RETURNED TO THE BANK AFTER THE EXPIRATION OF THEIR VALIDITY OR AFTER THE EXPIRY OF THE PAYMENT CARD

All embossed Visa Business, Visa Business Platinum

SECURITY WHEN USING A PAYMENT CARD

When using a Payment Card, it is necessary to comply with the security principles in its use and take all necessary measures to prevent misuse of the Payment Card, in particular:

a) store the Payment Card in a safe place out of the uncontrolled reach of third parties, in particular separately from personal documents and identity documents, and take extra care to protect it from loss and misuse;
b) upon receipt of the Payment Card, take all reasonable steps to ensure the protection of the Payment Card's security features of the and the data on the Payment Card used in the execution and authorisation of payment transactions;
c) upon receipt of the Payment Card, if it contains a signature strip, immediately sign it by hand on the signature strip;
d) not to allow the use of the Payment Card by a third party; not to disclose Payment Card details – number, expiry date and CVV2 Code (e.g. via social networks)
e) when using the Payment Card to make a payment at a Merchant, do not allow the Merchant to take the Payment Card out of the Client's sight;
f) when making payments via the internet and in MO/TO transactions, do not use the Payment Card for payments on unverified websites of unreliable Merchants;
g) when making online payments and MO/TO transactions, to carefully read the details of SMS codes or payment information in George via George ID or in the mToken application.
h) when making online payments, do not provide SMS codes to strangers or confirm transactions via George using your George ID or mToken at the instruction of another person.
i) upon receipt of the PIN number for the Payment Card, ensure its confidentiality, prevent its disclosure to any third party, not to record the PIN number in any form or store it in any form, in particular do not store it together with the Payment Card;
j) protect the PIN number and other data used for the authorisation of payment transactions made with the Payment Card from being observed by third parties;
k) not to use a cancelled Payment Card, a Payment Card after its expiry date, or a blocked Payment Card;
l) after the expiry of the validity period, as well as after any reissue of the Payment Card, destroy the old Payment Card in such a way that the data used for the authorisation of payment transactions cannot be retrieved;
m) in the event of loss, theft or suspicion of possible misuse of the Payment Card by a third party, inform the Bank of this fact without undue delay and request the blocking of the Payment Card, by contacting the Client Centre's 24-hour service or any Branch, and at the same time report this fact to the local police.

Given the need to comply with security principles when using the Payment Card, a breach of the obligations set out in this Article shall be deemed to constitute gross negligence and a material breach of the Payment Card Contract and the terms and conditions of use of the Payment Card.

The Payment Card must be protected against damage and magnetic fields. If the Payment Card is damaged, the Client shall notify the Bank of this fact and return the damaged Payment Card to the Bank. The Bank may retain the damaged Payment Card at any time for security reasons. The Bank may also retain a cancelled, invalid or blocked Payment Card, as well as a Payment Card whose authenticity is in doubt.

For security reasons, in order to protect the Client's funds against misuse, in cases of speculative behaviour on the part of the Client, as well as in the event of repeated complaints from the Client relating to misuse of the Payment Card, the Bank may suspend, modify, restrict or cancel individual authorisations to perform permitted transactions using the Payment Card, as well as block the Payment Card.

SLOVENSKÁ sporiteľňa

TELEPHONE NUMBERS FOR REPORTING LOSS, THEFT OR SUSPECTED MISUSE OF A PAYMENT CARD
In the event of loss or theft of a Payment Card or suspected misuse of a Payment Card, the Client shall be obliged to report this immediately **to the Client Centre's 24-hour telephone line: 0850 111 888, 0910 111 888, or *0900 from abroad 00421 2 58268 111**, or **at any Branch of Slovenská sporiteľňa, a.s.**

ADDITIONAL SERVICES FOR PAYMENT CARDS

Business Insurance

The Bank provides this service automatically for all Visa Business and Visa Business Platinum Payment Cards. The service is included in the Payment Card fee.

The Bank has agreed as the policyholder with the insurer, INTER PARTNER ASSISTANCE, S.A., a member of the AXA Group, ID No.: 0415591055, registered in the Commercial Register maintained by the Greffe de Tribunal de commerce de Bruxelles under registration number 0415591055, in favour of:

a) the card holder as the insured party insurance for medical expenses and assistance services
b) the account holder to whom the above-mentioned types of business Payment Cards are issued as the insured party insurance against loss caused by the use of the Payment Card. The scope, parameters and conditions of the insurance are set out in Group Insurance Contract No. 10233/80142 concluded between the insurer and the Bank as the policyholder and in the General Insurance Conditions for Travel Insurance for Business Payment Cards (VPPCP-KK) and the General Insurance Conditions for Business Payment Card Misuse (VPP PZ-KK) issued by the insurer.

The Card Holder, as well as the account holder to whom the Payment Card is issued, as the insured person, agrees in accordance with the provisions of Section 50 and Section 794 of the Civil Code, to insurance based on a Group Insurance Contract concluded between the insurer and the Bank as the policyholder.
Legal relations related to insurance are governed by the relevant provisions of the Group Insurance Contract, the General Insurance Conditions for Travel Insurance for Business Payment Cards and the General Insurance Conditions for Business Payment Card Misuse issued by the insurer, which are available at the Bank's Branches and on the Bank's website, and the provisions of the Civil Code and other related legal regulations, in that order.

Insurance conditions, scope and parameters:

Insurance against loss caused by the use of a payment card by the holder	
Coverage of the insured's financial loss incurred as a result of the holder of the Payment Card issued to the insured's Account uses it contrary to the insured's instructions or contrary to the contract on the basis of which the Payment Card was issued to him/her, either intentionally or as a result of negligence, when the holder is unable to properly charge the use of the Payment Card to the insured. The insurance also covers financial losses resulting from loss/theft of the Payment Card.	up to € 15,000/holder/year up to € 500,000/company/year
Medical expenses insurance (MEI)	€ 25,000
Repatriation (return to home country and transport)	actual costs up to the MEI limit
Transport of human remains	€ 4,500
Visit by a family member (accommodation + transport)	€ 75/night (max. 10 nights) + actual transport costs
Accompanying person (accommodation + transport)	€ 75/night (max. 10 nights) + actual transport costs
Accompanying person for minors from abroad (accommodation + transport)	€ 75/night (max. 3 nights) + actual transport costs

Dental treatment	€ 250
Deductible	€ 100
Assistance services insurance (ASI)	
Tourist information	Related costs
Medical information	
Emergency telephone assistance	
Interpreting and translations	

Further terms and conditions and more detailed information are available on the Bank's website.

ATM Deposit Service

The ATM Deposit Service is a service provided by the Bank that allows the Card Holder to make cash deposits using their Payment Card at the Bank's ATMs with a deposit function. The Card Holder may deposit a maximum of 200 banknotes per deposit. The service may be used by holders of all types of Payment Cards issued by the Bank. The Client may agree with the Bank to cancel the service by concluding an amendment to the contract.

The Bank may request information and documents from the Client to prove the origin of the funds deposited through the ATM Deposit Service, regardless of the amount of funds deposited and even after such a cash deposit has been made. If the Client fails to provide the requested information and documents within the period specified by the Bank, the Bank shall be entitled to refuse to allow the Card Holder to make cash deposits via the ATM Deposit Service until the origin of the disputed funds has been duly proven.

Payment by Payment Card via a Third-Party Application

Card Holder with a Payment Card registered in the application:
Google Pay, operated by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, and/or
Apple Pay, operated by Apple Distribution International, with its registered office at Hollyhill Industrial Estate, Cork, Ireland, and/or
Garmin Pay, operated by Garmin Ltd., with its registered office at 5650 El Camino Real, Suite 205, Carlsbad, USA, and/or
Xiaomi Pay, operated by Beijing Xiaomi Payment Technology Co. Ltd., and/or
SwatchPay, operated by Swatch Group (UK) Limited, Building 1000, 2nd Floor East Wing, The Royals Business Park, Dockside Road, London E16 2QU, UK,
(hereinafter also referred to as the "Third-Party Application"),
has the option to make cashless payments on the internet and order goods or services from Merchants in the Slovak Republic and abroad via POS and cash withdrawals from selected ATMs that offer this service.

The technical prerequisite for performing payment transactions via the Third-Party Application is that the Card Holder is a user of a device (e.g. smartphone, tablet or watch) with functionality (e.g. NFC) and the appropriate operating system required by the operator of the Third-Party Application (hereinafter referred to as the "device"). The Card Holder acknowledges that when using the Third-Party Application, the Card Holder is bound by the terms and conditions of the Third-Party Application of the company that operates this service. The costs of internet connection or data services from the provider or mobile operator shall be borne by the Card Holder.

In order to use the Payment Card for payments via a Third-Party Application, the Card Holder shall meet the following conditions:

The Card Holder shall install the Third-Party Application on their device, in which the Card Holder register in accordance with the Third-Party Application operator instructions, and, if necessary, verify their identity using a one-time SMS code or the Client Centre.

If the Card Holder's phone number is not current or complete, the Card Holder is required to update their mobile phone number through the Client Centre service. The Card Holder may register multiple Payment Cards in the Third-Party Application, but payment transactions will only be executed from the Payment Card that the client places first in the Third-Party Application (default card).

For newly issued Payment Cards, the Card Holder may also register the Payment Card in the Google Pay and Apple Pay applications via the George mobile Internetbanking application (hereinafter referred to as the "George Application") from the moment the information about the new Payment Card is displayed in the Card Holder's George Application. The Card Holder may successfully register such a newly issued Payment Card via the George Application in Google Pay and Apple Pay and subsequently make payments via Google Pay and Apple Pay even before the plastic version of the Payment Card is delivered and activated.
Each payment transaction made by the Card Holder via a Third-Party Application is considered a Payment Card payment. Payment transactions made with a Payment Card via a Third-Party Application are debited by the Bank to the Account to which it is issued.
In the case of a payment at a POS terminal in the amount of up to EUR 50 via the Google Pay application for goods and services at Merchants marked with the contactless payment logo, the Card Holder shall make the payment by placing a locked device with the display lit on the POS terminal. Payments over EUR 50 for goods and services at Merchants marked with the Third-Party Application logo are usually made by the Card Holder entering a numeric password, fingerprint, face scan or pattern into the device, thereby unlocking their device. For security reasons, when making payments over EUR 50 for goods and services at Merchants, the Card Holder may be asked to place their unlocked device on the POS terminal. The Card Holder confirms online payments and online orders of goods of any value by touching the Third-Party Application logo.
When making payments via the Apple Pay application, each transaction, regardless of its amount, is verified by a numeric password, fingerprint or facial image, which the Card Holder has chosen as their access PIN on their device. When making payments via the Swatch Pay application, each transaction, regardless of its amount, is verified by entering the PIN number issued for the Payment Card.
When activating the Garmin Pay service, the Card Holder chooses their access PIN for the purpose of verifying their identity. The Card Holder enters the access PIN when making their first payment using a watch that uses the Garmin Pay service, regardless of the amount. After successfully entering the access PIN, the Card Holder no longer needs to verify subsequent payments by entering the access PIN and makes the payment by opening the relevant application on the watch and placing the watch on the POS terminal. The access PIN must be re-entered for payments of any amount whenever the Card Holder puts the watch back on their wrist or 24 hours after the last successful entry of the access PIN.
When withdrawing cash from an ATM that supports the functionality of withdrawals via a Third-Party Application, the client shall, after placing the device with the Third-Party Application on the ATM, verify their PIN number issued for the debit card they have registered in the Third-Party Application.
The Third-Party Application contains a history of payments made by the Card Holder using the Payment Card in the Third-Party Application for informational purposes.
After issuing a Renewed or Replacement Card, the Bank will update the Card Holder's card details in the Third-Party Application. It is not necessary to activate the plastic version of such a Renewed or Replacement Card in order to use the payment functionality via the Third-Party Application. The Third-Party Application will also be updated when the Payment Card is cancelled.
If the Payment Card is blocked or temporarily blocked, it cannot be used to perform payment transactions with it via the Third-Party Application.
If the Payment Card is deregistered from the Third-Party Application and is not cancelled, the Card Holder may use the Payment Card and perform other payment transactions. The Card Holder shall be obliged to uninstall the Payment Card details from the Third-Party Application when replacing the device, or repairing it, or making other changes that could compromise the security of the Payment Card.

AirRefund
The Bank provides a service for Visa Business and Visa Business Platinum Payment Cards.
AirRefund is a programme operated by Air Refund, S.A., registered under number CH-660.0.717.014-3, with its registered office at 3 bis chemin de la Marbrerie, 1227 Carouge, Geneva (Switzerland) (hereinafter "AirRefund"). Card Holders can use AirRefund to file claims if their flight has been cancelled, delayed, or if the Card Holder has been denied boarding due to "overbooking".
Visa Business and Visa Business Platinum Card Holders who paid the full amount of the ticket with this card are entitled to a 10% discount on the fee for a successfully processed claim if AirRefund mediates

the refund of compensation from the airline. The fee is charged by AirRefund and, after taking the discount into account, is deducted from the amount that the airline will refund to the Card Holder through AirRefund.
Card Holders can submit their claims at: https://visa.airrefund.com/en/SLSP.
AirRefund reserves the right to change the discount amount and other terms and conditions. Detailed terms and conditions for applying the discount can be found at AirRefund | Slovenská sporiteľňa

Displaying PIN number in George
PIN number display is a service provided by the Bank, enabling the Card Holder to display their PIN number for their Payment Card via the George or Business24 Internetbanking Electronic Service or in the George Internetbanking mobile application (hereinafter referred to as the "George app"). The Card Holder can find the option to view the PIN number in the relevant version of Internetbanking in the details of the Payment Card linked to their Account. After successful authorisation of the transaction by the Card Holder via George ID or mToken, the PIN number will be displayed to the Card Holder for 10 seconds in Internetbanking version George or Business 24 and in the case of displaying the PIN number in the George app, while holding their finger on the marked field in the app. The Card Holder shall be obliged to ensure that when using the Displaying PIN number service, the PIN number is not made available to third parties. The Card Holder may use the PIN number Display service a maximum of 5 times per day.

Access to airport lounges
The Bank provides this service for the Visa Business Platinum Payment Card.
The Visa Business Platinum Payment Card Holder is entitled to an unlimited number of free entries to airport lounges in Vienna, together with one accompanying person.
The service applies to the following airport lounges:

Schwechat Flughafen Wien AG Airport
Lounges: Vienna Lounge (Terminal 1)
Sky Lounge (Terminal 3)

Visa Business Platinum Card Holders are entitled to 4 complimentary visits and use of airport lounge services with one accompanying person between 1 January and 31 December of the calendar year:

Liszt Ferenc International Airport Budapest
Lounge: SkyCourt Lounge

The decisive period for counting the number of visits to the airport lounge is the calendar year. Each visit by the Card Holder in excess of the number of free visits guaranteed per year is charged according to the price list of the respective airport lounge.

Visa Benefit Programme
Provided for Visa Business and Visa Business Platinum cards
Card Holders of these card types can enjoy the benefits of the programme, which is a set of benefits, rewards and other services and advantages provided by Visa and its contractual partners.
The programme also includes access to airport lounges worldwide via the Visa Airport Companion Europe application at a discounted price.
Detailed information about the programme can be found at www.visa.sk/visabenefit
The card company reserves the right to change the list of benefits. Benefits cannot be exchanged for cash.

Purchasing access to airport lounges with the Airport Companion Europe application
The Bank provides this service for Visa Business and Visa Business Platinum Payment Cards.
Card Holder of Visa Business or Visa Business Platinum Payment Cards issued by Slovenská sporiteľňa can register free of charge with the Airport Companion Europe application, which is operated by DragonPass International Limited, based at 173A Ashley Road, Hale, Cheshire WA15 9SD.
The Client is granted, via the Airport Companion Europe application, the option to purchase access to

more than 1,000 airport lounges for themselves and their guests, allowing them to use the services offered there.
The Card Holder acknowledges that when using the services provided through the Airport Companion Europe application, the Card Holder is bound by the terms and conditions of this app from DragonPass International Limited. Any costs for internet connection or data services from a mobile operator shall be borne by the Card Holder.

Updating card details in the Visa system (VAU)

In accordance with the requirements of card companies, the Bank ensures that Payment Card data is updated in Visa's Visa Account Updater system, known as VAU.

Thanks to automatically updated Payment Card data, the VAU platform allows the Card Holder's invalid Payment Card to be paired with a reissued Payment Card with a new card number, or with a new expiry date, allowing the Card Holder to continue making regular recurring payments on the internet (e.g. subscriptions for services provided by merchants) without having to enter new Payment Card details to the merchant. Recurring payments will only continue if the merchant also supports this service. If the Card Holder does not wish to automatically continue making regular recurring payments on the internet when a new Payment Card is reissued, they are obliged to notify the Bank of this. In such a case, the Bank shall ensure that the Card Holder's Payment Card is not linked to their previous Payment Card in the VAU system.

Partial authorisation

Partial authorisation is a service provided by Visa, on the basis of which the Bank is entitled to settle a cashless payment by Payment Card even partially, up to the permitted Payment Card Limit, up to the maximum amount of the available balance on the Account and provided that the partial authorisation service is supported by the Merchant. The initial value of the minimum amount of a cashless payment by Payment Card must be EUR 5, and after it is settled by the Bank, the available balance on the Account will be EUR 2.