BUSINESS TERMS AND CONDITIONS OF ČSOB, A.S. FOR THIRD-PARTY APPLICATIONS

1. These Business Terms and Conditions ("Terms and Conditions") of Československá obchodná banka a.s. ("Bank" or "ČSOB") regulate the use of third-party applications installed on a Device to execute payment transactions with Mastercard and VISA payment cards subject to rights and obligations arising from the contractual relationship between the holder of a payment card ("Cardholder") and the Bank ("Applications"). These Terms and Conditions supplement the Bank's Business Terms and Conditions for the Issuance and Use of Debit Payment Cards, the Issuance and Use of ČSOB Credit Cards and the Issuance and Use of Corporate Cards ("PC T&C"). A Cardholder who wishes to use the services of a Provider must note that in addition to these Terms and Conditions, they are also obliged to comply with the Provider's terms and conditions, under which the Provider has the right to change the functionality, technical conditions or characteristics of the Device or Application. Rights and obligations in the relationship between the Cardholder and the Bank not specified herein are regulated by the PC T&C.

2. DEFINITION OF TERMS:

DPAN or Token means the digital equivalent of a physical payment card in an Application, which is created when a Card is registered in the Application.

NFC payment on a mobile device (Near Field Communication) means a contactless payment executed using a mobile Device and a POS terminal or a withdrawal from a contactless ATM.

The Bank's mobile application is the ČSOB SmartBanking application, which can downloaded to a mobile device from the App Store or Google Play ("ČSOB SmartBanking application").

Business Terms and Conditions means the Terms and Conditions for the Issuance and Use of Debit Cards, the Terms and Conditions for the Issuance and Use of Corporate Cards and the Terms and Conditions for the Issuance and Use of ČSOB Credit Cards.

Provider means the third party that owns the copyright and other intellectual property rights related to an Application.

Verification code means a unique six-character verification code generated by the card company.

Device or Mobile Device means a mobile device, tablet, computer or smartwatch. The Devices or Mobile Devices supported for applications are determined by the Service Provider.

3. APPLICATION

3.1. For the purposes of these Terms and Conditions, Application means a mobile application that is used to register a payment card ("Card") in a supported device using a mobile phone or the ČSOB SmartBanking application. An Application is provided by the Provider that owns the copyright and other intellectual property rights to the Application ("Provider") and is obtained from the appropriate store for the type of application e.g. the Apple App Store or Google Play.

3.2. Application use is permitted to Cardholders aged 15 years or older. Application use is free of charge for clients of the Bank.

3.3. Descriptions of Applications and the technical conditions for their use can be found on the web page **https://www.csob.sk/individualni-klienti.**

4. TECHNICAL REQUIREMENTS FOR APPLICATION INSTALLATION

a) issuance and activation of a ČSOB Card with the Mastercard/VISA logo

b) the Cardholder should register their current mobile phone number with the Bank

c) consent for the Terms and Conditions and consent for the provision of data to the Provider

d) a Cardholder can use an Application on a device with Near Field Communication ("NFC") functionality that permits the installation and use of the Application, mainly a mobile phone, smartwatch etc. ("Device").

e) an Application can hold multiple digitised Cards, except for cards of the type Visa Classic Junior, VISA Electron Baby, whose digitisation is not supported. when a Card is entered, its Token is automatically set as the default and when multiple cards are entered, the Cardholder must select the default Token,

f) the Card's registration in the device has the same validity period as the Card itself: up to 3 years, 4 years or 5 years depending on the type of card issued.

g) The protection of Clients' personal data and its processing in the Bank is regulated by the Memorandum on Personal Data Protection, which is available on the Bank's website: **https://www.csob.sk/pravne-informacie#memorandum-ochrany-osobnych-udajov**.

5. APPLICATION ACTIVATION

5.1. The Application must first be downloaded from the store and installed in the Device. In some cases, the Device may need to be paired to another Device.

5.2. A Card can be registered in the Application from the ČSOB SmartBanking application.

5.3. Cardholders must familiarise themselves with the Provider's terms and conditions and these Terms and Conditions. Cardholders cannot use an Application without agreeing to its Terms and Conditions. The Cardholder must set up security features on the Device to ensure it is secure. If a Card is registered manually or through the ČSOB SmartBanking application, sensitive information must be provided such as:

- the whole Payment Card number
- the expiry date of the Payment Card
- the forename and surname of the Cardholder
- CVC2 / CVV2
- the Cardholder's address.

The sensitive information is sent in an encrypted form to the Application Provider or the card company.

5.4. If the Application requires Card verification, an SMS will be sent to the telephone number of the Device with a 6-character verification code to confirm the Cardholder's registration in the Application. The Bank reserves the right for registration to proceed without the use of a verification code. After the verification code is entered in the Application, a virtual number ("Token") is linked to the Card.

6. APPLICATION USE

6.1. The purpose of the Applications is to enable non-cash payments to be made by holding the device in proximity to a POS Terminal at the point of sale of a Merchant displaying the Mastercard and VISA logos, to enable withdrawals from contactless ATMs and to use selected Internet stores that support this form of payment.

6.2. Making a non-cash payment using the Application requires the Cardholder to light up or unlock the device and hold it close to the POS Terminal. When making the first payment with a Device other than a Mobile Device, e.g., with a smartwatch, the Cardholder must enter a 4-digit code that is not the Card PIN and hold the smartwatch close the POS terminal. For subsequent payments, this code is not required as long as a transaction was carried out in this way in the last 24 hours and detection of the Cardholder's heart rate has not been interrupted.

6.3. Non-cash transactions at POS terminals do not require entry of the Card PIN because the transaction is confirmed by the Device's security elements. The Card PIN is always required when using a contactless ATM.

6.4. The Cardholder can review the history and number of payments made using the Token in the extent supported by the Application's capabilities and settings.

7. TOKEN REMOVAL, CARD BLOCKING

7.1. The Cardholder may delete a Token created in an Application at any time and add it to the Device again. Such actions do not affect the functionality of the physical Card.

7.2. In the event of the theft, loss or unauthorised use of a Device on which an Application is installed with a Token, the Bank will ensure that the Token is deleted when the Cardholder reports the issue to the Bank. If the Card is lost or stolen, the Cardholder will receive a new Card with a new number, expiry date and CVC2/CVV2 and this Card will require a new registration to be used in the Application.

7.3. If a Card is blocked, the Bank will always delete all Tokens associated with the Card. To block a Card, the Cardholder must follow the appropriate steps laid down in the PC T&C.

7.4. When a Card expires, the Token is also suspended and only reactivated if a new Card is activated.

7.5. When transferring to a new device, it is recommended that you delete the Card from the old Device and the Application.

8. RIGHTS, OBLIGATIONS AND RESPONSIBILITIES OF THE CARDHOLDER AND THE BANK

8.1. The Cardholder must protect the Device against misuse by unauthorised persons including members of their own family and against loss or theft; they must also secure the Device containing the Application and Token against misuse in the event of loss or theft.

8.2. The Cardholder must not share the Card with other persons, including family members. The Card is non-transferable and third parties must not be allowed to register it in an Application.

8.3. Cards issued to another Cardholder must not be registered in an Application.

8.4. The Cardholder must have the Device continuously under their control and take measures to prevent third parties having access to the Device (e.g., locking the device with biometric data or an access code comprising a relatively complex sequence of letters and numbers).

8.5. The Cardholder must continuously monitor payments on the Card account when executing transactions using an Application and immediately report all discrepancies and deficiencies to the Bank.

8.6. In the event of the loss, theft, misuse or unauthorised use of the Device with the Application, or the disclosure of the Device's security elements, the Cardholder must report it without delay (immediately on becoming aware of it) by calling +421 2 5966 8230 or by visiting any branch of the Bank. This telephone number is also shown on the reverse of the Card, and the Bank will inform the Cardholder of any change in the number.

8.7. The Bank will not be liable for the functionality of the Application in the following cases:
- failure to satisfy the technical conditions necessary for use of the Application on the side of the Cardholder,
- non-functionality of electronic devices needed for the use of the Application,
- non-functionality, closure, hanging, or errors of the Application that are the fault of the Provider,
- non-functionality, closure, hanging or errors that are the fault of the card company
- outages of the data network or data service that the Device uses.

8.8. In the event of the loss, theft or misuse of data necessary for the use of the Application, or in the event of unauthorised use of the Application, the Bank will not issue a replacement Card or emergency cash. The Bank is entitled to unilaterally terminate the possibility to execute transactions and create Tokens if it suspects the misuse of card data, suspects fraud on the part of the Cardholder or suspects that a card is being used for unauthorised transactions.

8.9. The Cardholder must install on the Device only software from trustworthy and recommended sources, such as the Google Play Store and the App Store, they must pay attention to the requirements of the installed application, and they must use only data connections provided by their mobile operator or a secure Wi-Fi network.

8.10. The Bank reserves the right not to register an issued payment card.

8.11. The Bank reserves the right to unilaterally terminate its contract with a Provider though it must inform the Cardholder by publication in the Terms and Conditions with advance notice as required by law.

8.12. The Cardholder is fully liable for any losses that occur as a result of a breach of their obligations laid down in the Article "Rights, Obligations and Responsibilities of the Cardholder and the Bank".

9. FINAL PROVISIONS

9.1. Use of an Application is also regulated by the Terms and Conditions for the Issuance and Use of Debit Payment Cards, the Terms and Conditions for the Issuance and Use of Corporate Cards and the Terms and Conditions Governing the Issuance and Use of ČSOB Credit Cards published on the Bank's website **https://www.csob.sk** and the General Business Conditions of ČSOB as part of the contractual relationship between the account owner, the Cardholder and the Bank.

9.2. The Bank is entitled to amend the Terms and Conditions at any time. The Bank will inform the User of amendments via the Bank's website **https://www.csob.sk** two months before the date

when the change enters force. If the User does not reject the proposal to amend the Terms and Conditions at the latest on the working day before the entry into force of the amendment, they are deemed to have accepted the amendment. If the User wishes to reject the amendment before the date when the amendment enters force, they may terminate the contractual relationship that includes use of the Application with no charge and with immediate effect. If the Cardholder rejects the amendment before the date when it enters force but does not terminate the contractual relationship, the Bank has the right to permit use of the Application only in accordance with the amended Terms and Conditions for technical reasons.

9.3. The Bank is entitled to amend the Terms and Conditions for use of the Application with immediate effect if they do not affect the rights and obligations of the Cardholder. Such amendments include amendments of the Terms and Conditions relating to the introduction of additional functionality, increased security, technological developments and changes required by law. Cardholders will be informed of such amendments via the Bank's website **https://www.csob.sk.**

These Terms and Conditions enter force on 15/05/2022.