Expobank

CONDITIONS
For the Issue and Use of Expobank CZ a.s. Payment Cards

1. GENERAL CONDITIONS

1.1. Expobank CZ a.s. (the "**Bank**") issues MasterCard contactless payment cards as an electronic payment means for personal and business current (payment) accounts denominated in Czech crowns, American dollars, and Euros. The current offer of payment cards and related supplementary services is published in information documents of the Bank. Legal matters relating to the issue and use of the Bank's payment cards are subject to the law of the Czech Republic.

1.2. The Conditions for the Issue and Use of the Bank's Payment Cards ("**Conditions**") constitute an integral part of every payment card agreement ("**Agreement**") between the Bank and the account holder (client). The Conditions are binding for both the Bank and the account holder as well as for any cardholder other than the account holder. By signing the Agreement and/or a payment card application, the account holder certifies to have thoroughly read, understood, and accepted the Conditions. The account holder may apply for the issue of supplementary cards for other persons (cardholders). In such a case, the account holder is fully liable for compliance with these Conditions by such cardholders. The account holder acknowledges that a failure to comply with duties to which cardholders are subject under the Conditions represents a breach of the Agreement. The account holder may also apply for the issue of cards through internet banking operated by the Bank.

1.3. In providing all banking services, the Bank is required to identify the account holder and a cardholder. In the case of a legal entity, the Bank must identify the controlling person and the beneficial owner. In particular, the Bank is required to carry out mandatory identification to the lawful extent in respect of transactions whose value exceeds the applicable legal limit. In case that the account holder or a cardholder refuses to undergo an identification check, the requested banking service will not be provided. The Bank is required to refuse to provide banking services if the identity of the account holder or a cardholder cannot be established.

1.4. The account holder must notify the Bank of any and all changes in data pertaining to payment cards issued for his accounts and to the holders of such cards, as specified in the Agreement or in the payment card application. The account holder is liable for any and all damage incurred as a result of a failure to comply with this requirement.

1.5. The account holder acknowledges that the Bank may inform other banks in the Czech Republic of any gross violation of the Conditions committed by the account holder or by a cardholder. Defining a gross violation of the Conditions is within the Bank's discretion. Furthermore, the account holder acknowledges that the Bank may provide information on payment cards issued for his account to the MasterCard Association.

1.6. The account holder must provide the Bank with complete and accurate information. The account holder is fully liable for any damage incurred by the same or by the Bank as a result of providing false or inaccurate information.

1.7. Payment cards are the property of the Bank. As a rule, a payment card is issued in the name of the cardholder and is not transferable to another person. A violation of this rule is considered a **gross violation** of these **Conditions** and of the **Agreement**.

1.8. There is no legal entitlement to the issue of a payment card. The Bank reserves the discretionary right to reject the account holder's payment card application. The Bank will inform the account holder in writing, through internet banking or by telephone if an application is rejected.

1.9. The Bank is entitled to debit fees and charges for services relating to card issue and card use by the cardholder and for the settlement of card transactions from the account holder's account, in accordance with the applicable current Table of Fees and Commissions referred to in the

Agreement. The card issue fee is charged upon the issue of a card, regardless of whether the cardholder takes possession of the card.

1.10. These Conditions are Special Conditions within the meaning of the Bank's General Business Conditions ("**GBC**"). In the event of differences, the provisions of these Conditions take precedence over the provisions of the GBC.

2. CARD ISSUE

2.1. A payment card application is made by the account holder at the Bank branch where the account holder's current account is maintained or through internet banking. The account holder must provide complete and accurate information. The account holder is fully liable for damage incurred by the Bank due to providing false or misleading information, including criminal prosecution.

2.2. Every cardholder may hold only one payment card of a particular type for one account or one combination of accounts denominated in different currencies.

2.3. The Agreement entered into between the Bank and the account holder is for a fixed term or open-ended. If entered into for a fixed term, the Agreement expires on the card expiration date. If the Agreement is open-ended, the Bank may issue to the account holder a new card automatically as of the expiration date of the original card, unless the account holder or the cardholder serves a written notice rejecting the issue of a new card **no later than six weeks prior to the expiration date** of the original card. The cardholder may apply for payment card renewal at an earlier date. If the card is not activated before the expiry date shown on the front side, the Bank has the right not to issue a renewal card. If the cardholder does not use the card for more than six months prior to the expiry date, the Bank has the right not to issue a renewal card.

2.4. A card is valid until the last day of the month and year indicated thereon. A card must not be used after the expiration date. A cardholder or an account holder is obliged to invalidate the card by cutting it over a magnetic tape and a chip, and to prevent access to the payment card data.

2.5. A cardholder must collect a payment card no later than **three (3) months** after making a payment card application. If not collected, the Bank can cancel and destroy the payment card. The account holder is not entitled to a refund of the monthly payment card maintenance fee and fees for supplementary services charged until the card is discarded.

2.6. The Agreement and/or a payment card application specify a maximum weekly transaction limits for every payment card. The limit restricts the maximum amount of payments made using a payment card in the course of one week. The account holder is informed of card parameters and limits upon signing the Agreement or submit a payment card application, or the cardholder is informed of its setting and its limits at the time of collecting the card. The cardholder may complete transactions using a card only up to the limit set by the account holder, where the cardholder must not overdraw the account in excess of the available balance within the meaning of the GBC. The cardholder may change card limits within the maximum weekly limits set by the account holder. The Bank may unilaterally reduce transaction limits due to security reasons, particularly in the event of a suspected unauthorized or fraudulent transaction. The Bank will inform the cardholder of such a reduction immediately.

2.7. An account holder is entitled to change payment card limits through internet banking, mobile application, call centre or by written request up to the maximum limit for a given type of transaction.

2.8. The account holder is liable for all transactions regardless of the limit and must compensate the Bank for damage incurred as a result of the incorrect use of a payment card or any unauthorized overdraft exceeding the available account balance.

2.9. By entering into the Agreement, the account holder authorizes the Bank to settle **all** payments and transactions completed using a cardholder's card to the debit of the account holder's account, following the cardholder's receipt of the payment card.

2.10. A non-activated payment card is delivered by mail to an address specified in the application for issue of a payment card. In exceptional cases, payment card may be collected by the cardholder in person at the Bank branch. Upon receipt, a payment card must be signed by the cardholder in the signature strip if there is a strip on the card. The Bank is not liable for any damage that may be incurred as a result of a failure to sign the card.

2.11. When delivered by the Bank to the future cardholder, a payment card is non-activated. The cardholder must only activate the payment card after its delivery. By activating the card, the cardholder confirms its actual delivery. The cardholder is prohibited from activating a card the cardholder does not have in his/her possession. The Bank is not liable for any damage that might be incurred by the account holder as a result of card activation carried out through electronic banking if the cardholder is not in actual possession of the card. The Bank may cancel a delivered card that is not activated within three months after the month of issue.

2.12. A payment card (application allowing ATM withdrawals and payments to merchants) is activated by the cardholder by any contact online ATM transaction completed using the correct PIN code (such as a balance inquiry or cash withdrawal) or through internet banking or a mobile application. The cardholder may also request activation upon collecting the card at the Bank branch.

3. Cardholder's personal security features - PIN code, ePIN code, 3D Secure, mobile application PIN codeb, biometric features (fingerprint, facial image)

3.1. The PIN code, ePIN code, and mobile application PIN code are together with biometric features (fingerprint, facial image) Are the personal security features of the cardholder, by which the cardholder consents to the payment transaction and with which the payment service provider verifies the cardholder. PIN code is a personal identification number disclosed solely to the cardholder and used exclusively for authorization of payment card transactions. The cardholder can set the PIN code using Internet banking and subsequently transfer it to the card by entering the card into ATM and carrying out a contact online transaction (ATM cash withdrawal or account balance inquiry), or sent to the cardholder by registered mail to the address specified in the Agreement or payment card application. ePIN code (if the Bank made it available to the cardholder) is a personal identification number disclosed solely to the cardholder and used exclusively for authorization of 3D Secure payment transactions made by payment card. ePIN code can be set up by the cardholder in Internet banking, or it can be sent via SMS to the cardholder to the mobile number registered for 3D Secure. The cardholder must contact the Expobank customer service center during business hours for sending ePIN code via SMS. Mobile application PIN code is a personal identification number used for logging in the mobile application unless the client uses biometric data to log in, and also used to authorize 3D Secure payment transactions made with a payment card in the event that for any reason it is not possible to authorize such payment using biometric features. Biometric features include a fingerprint or a facial image. A cardholder can choose to use these features when registering a mobile application.

3.2. If the PIN code is delivered by mail, the cardholder must ensure that the PIN envelope, particularly the security field containing the PIN code, is undamaged. If the PIN code envelope is damaged in any way whatsoever, the cardholder must request a damaged delivery confirmation from the Česká pošta, s.p. branch that delivered the envelope. In such a case, the Bank will issue a replacement payment card with a new PIN code free of charge. If the cardholder does not present a Česká pošta, s.p. confirmation, the Bank will charge a card replacement fee in accordance with the Table of Fees and Commissions.

3.3. The PIN code, ePIN code and mobile application PIN code is known to the cardholder only. It is prohibited to mark the PIN code on the card, to keep it together with the card, or to disclose it to any person, including family members. **Allowing the PIN code, ePIN code and mobile application PIN code to be disclosed to other persons is considered a gross violation of these Conditions and the Agreement**. The cardholder must protect the PIN code, ePIN code and mobile application PIN code from being disclosed when it is entered using a keyboard, for instance by covering the keyboard or using another suitable method. Any violation of this requirement, regardless of whether deliberate or due to fraudulent action or negligence is considered a gross

violation of the Agreement. The account holder bears full liability for any and all losses incurred as a result of any payment transaction completed using the PIN code, ePIN code and mobile application PIN code, not authorized by the cardholder, until such a transaction is reported to the Bank. The account holder must pay for all transactions completed using the correct PIN code, ePIN code and mobile application PIN code and compensate the Bank for any losses incurred as a result of the disclosure of the PIN code, ePIN code and mobile application PIN code.

3.4. The cardholder may change the PIN code. A PIN code change can only be made by making a contact online transaction at an ATM in the Czech Republic, through internet banking or mobile application, and then uploading a new PIN to the card via a contact online ATM transaction (ATM cash withdrawal or account balance inquiry). A PIN code change may only be made until six weeks prior to the card expiration date. ePIN code change can be made in the internet banking. In case the cardholder does not have an access to the internet banking, the cardholder can contact the Expobank customer service center during business hours and the new ePIN code will be sent the cardholder's mobile number registered for 3D Secure. Mobile application PIN code change can be made by the client in the mobile application.

3.5. For security reasons, the Bank advises cardholders not to use as the PIN code, ePIN code and mobile application PIN code a number that can be easily guessed or worked out, such as four identical digits, a consecutive series of digits, the birth date of the cardholder or his family members, or a fragment of the payment card number and not to set up the same digits for PIN code, ePIN code and mobile application PIN code.

3.6. If the PIN code is forgotten, the cardholder may change it in internet banking or mobile application and subsequently upload the new PIN to the card via a contact online ATM transaction (ATM cash withdrawal or account balance inquiry) or apply to the Bank for the issue of a new PIN code in the paper form. In such case, the Bank issues for the client an envelope with original PIN code valid upon the issue of the payment card, even if the PIN code has been changed by the client.

3.7. 3D Secure is a standardized security protocol used for online card payments at merchants marked with MasterCard ID Check logos. Payment transactions where the security protocol is used may also be authorized by a disposable code which is sent in the course of the payment in the form of SMS and by entering ePIN code, or through a mobile application using biometric data or using a mobile application PIN code. Mobile telephone number, which is used for receiving the security code, is provided by the cardholder to the Bank via internet banking by filling in the Agreement or Application as per article 1.2 of the Conditions, by filling in the form at the Bank branch or by sending respective form provided with officially verified signature of the cardholder via post to the respective the Bank branch. Cardholder must protect the disposable 3D Secure code in order to prevent any misuse of the card. Any violation of this requirement, regardless of whether deliberate or due to fraudulent action or negligence is considered a gross violation of the Agreement. The account holder bears full liability for any and all losses incurred as a result of any payment transaction completed using the disposable code, not authorized by the cardholder, until such a transaction is reported to the Bank. The account holder must pay for all transactions completed using the correct disposable code and compensate the Bank for any losses incurred as a result of the disclosure of the disposable code. **Allowing the disposable code to be disclosed to other persons is considered a gross violation of these Conditions and the Agreement.**

4. CARD USE

4.1. A payment card may be used by the cardholder in the Czech Republic and abroad for payments for goods and services purchased at retail and service outlets, for ATM cash withdrawals, for account balance inquiries, and for cash withdrawals at bank branches and currency exchange outlets identified by the MasterCard logo. A Client has an option of setting up an automatic rejection of transactions for which an additional fee is to be paid, the so-called surcharge fee, which is charged by some operators for the use of ATMs, within the electronic banking service, at the Bank's branch or via the Bank's mobile application (if this service is available in the application). A Client also has an option to deactivate the use of a magnetic stripe within the electronic banking service, at the Bank's branch or via the Bank's mobile application (if this service is available in the

application). If an attempt is made to perform a transaction using a magnetic stripe, it will be automatically rejected.

4.2. A contactless payment card may be used for contactless payments for goods and services at payment terminals that support the contactless technology. A payment is made by placing a payment card on the payment terminal. The limit for a contactless payment made without cardholder identification, such as the entry of the PIN code, for cards issued in the Czech Republic is CZK 500. The limit may be changed at any time. A payment terminal may refuse contactless payment at any time and, instead, request a standard payment (insertion of card into the payment terminal) with the entry of the PIN code. Contactless payment cards issued after 1.12.2017 can be used for contactless cash withdrawals or for account balance inquiries in bank machines supporting the contactless technology. The PIN code must be entered for all contactless cash withdrawals, regardless of the amount to be withdrawn. With some internet merchants the renewal or replacement card can working in case that the data of the original card are stored with such merchants.

4.3. Due to security reasons, particularly when an unauthorized or fraudulent transaction is suspected, the Bank reserves the right to refuse certain types of payment transactions, such as transactions where the card is not physically present, i.e. transactions by mail, telephone – so-called MO/TO transactions, Internet transactions, transactions originating in high-risk regions completed using the magnetic strip of a card, and the like, depending on the payment card type.

4.4. A payment card must not be used for a transaction that would be contrary to laws effective in the jurisdiction where such a transaction was to take place. The cardholder and/or the account holder bear full liability for any violation of this requirement, including liability for any losses and penalties. The Bank reserves the right not to allow selected payment transaction especially in accordance with law No. 186/2016 Coll., on gambling.

4.5. The Bank is not liable for the non-provision of services and damage incurred by cardholders directly or indirectly due to circumstances beyond the control of the Bank or its partners, including, without limitation, power outages, equipment failures, defects in data processing systems or transmission lines, work stoppages, and the like. Likewise, the Bank is not liable for a refusal to accept a card by a merchant or a branch of another bank.

4.6. The Bank is not liable for defects in goods or services paid for using a payment card.

4.7. A point of sale where a payment card is used may request an authorization for completing the requested transaction and only complete the transaction if it is authorized by the Bank or by an organization charged by the Bank.

4.8. The cardholder demonstrates an authorization to use a payment card for a transaction as follows: if the conditions for one of the exceptions provided by law are not met, the cardholder is always identified by a combination of two elements from different categories, which are “knowledge” (something the cardholder knows, e.g. PIN code, ePIN code, mobile application PIN code), “possession” (something the cardholder owns or otherwise holds as authorized possession, e.g. a mobile phone or other mobile device) and "inherence" (something what the cardholder is - this includes biometric elements, i.e. fingerprint or facial image):
Specifically, the cardholder is identified and the payment order is authorized:

- by entering the PIN code if the payment card is used at an ATM,
- by entering the PIN code during a cashless or cash transaction when using a payment terminal at a business establishment if a business establishment is equipped with a PIN code verification device
- by entering the payment card number, the expiration date, and the Card Verification Code (CVC) if the payment card is used for a card-not-present transaction, such as an online payment over the Internet.
- internet non-cash payments via secured 3D Secure protocol may be in addition to the authorization described in the previous article further authorized by a disposable SMS code and ePIN code (combination of "possession" and "knowledge" elements), or by means of a mobile application using biometric data (combination of "possession" and "inherence" elements) or a mobile application PIN code (combination of "possession" and "knowledge" elements). The Bank reserves the right not to allow completing online

payments when cardholder does not provide mobile telephone number for the service as per article 3.7 of these terms and conditions to the Bank. The Bank reserves the right not to allow completing online card payments by merchants who do not support 3D Secure. If 3D Secure security protocol is activated in the card, the Bank may authorize the online payment without using the 3D Secure security protocol. The Bank advises completing online purchases only in those e-shops (internet shops) which support 3D Secure authorization standard presented under the trademarks MasterCard ID Check.

4.9. No transaction authorized by the cardholder (for instance by entering the correct PIN code) may be cancelled.

4.10. If the account holder requests SMS notifications for authorized payment card transactions, the sum specified in an SMS notification sent for a transaction completed abroad is approximate only.

4.11. If the wrong PIN code is entered more than three times during a payment card transaction, the card is automatically temporarily blocked for security reasons. The card functionality will be renewed on the first day of the subsequent weekly transaction-limit period. A cardholder may request to unblock the card at the Bank branch, by contacting a call center or sending a message via Internet Banking. A cardholder can also unblock the card by himself in internet banking, where he can also view the number of remaining attempts to enter the PIN code before its possible temporary blocking.

4.12. If the incorrect PIN code is entered more than three times during an internet non-cash payment via 3D Secure protocol, the card is automatically temporarily blocked for internet payments due to security reasons. The card functionality will be renewed the following day.

4.13. The Bank may without prior notice cancel, in full or in part, the right to use a payment card by restricting, temporarily or permanently, its validity due to reasons including, without limitation, a violation of contractual conditions, account attachment (distrainment), unauthorized debit, suspicion of fraudulent action on the part of the cardholder or a third party, and security.

4.14. If the mobile phone number used for 3D Secure services is not under the control of the cardholder, particularly in the cases of loss or theft of the mobile phone with the respective number or change of the telephone number, cardholder must inform the Bank thereof immediately.

4.15. The Bank allows the cardholder to receive MasterCard MoneySend transactions. In providing these services, the Bank reserves the right to allow funds to be credited only to selected types of payment cards. The money transfer service can be used up to the limits set for MasterCard MoneySend services.

5. TERMS OF PAYMENT BY NEAR FIELD COMMUNICATION DEVICE (NFC)

5.1. The NFC Product Terms and Conditions for mobile or watch payments within the Google Pay service (hereinafter the "**Service**") contain a contractual agreement between the Client / Payment Card Holder and the Bank on the execution of payment operations by a payment card via a device with NFC functionality (hereinafter the "**NFC Device**") and via the Google Pay application (hereinafter the "**Application**").

- The application allows Clients to add the card to the NFC Device via a mobile phone or in internet banking or in a mobile application. It is possible to perform payment transactions via the Service by the NFC device. The copyright owner of the Application and the Service provider is: Google Ireland Limited, based in Ireland, Gordon House, Barrow Street, Dublin 4; (hereinafter the "**Provider**")

5.2. The Provider allows the cardholder to add the card and manage it in the Application. The Bank will enable the execution of payments using the Service through the Application installed in the NFC Device, which enables the execution of payments in stores that accept payment cards, up to the amount of limits set for individual cards.

5.3. The Application functionality, including the Provider's right to make changes, suspend or terminate it, is governed by the Provider's terms and conditions, which are set out in the terms of use of the Application, with which you must be acquainted before using the Application. The Bank has no influence on the wording of these terms and conditions and bears no responsibility for this wording.

5.4. The card registration in the NFC Device remains valid for as long as the card is valid, but does not exceed 3 years. After the expiration of the card registration in the NFC Device, it is necessary to register the card again.

5.5. The Cardholder acknowledges the degree of risk associated with the execution of contactless transactions and is obliged to:

- secure the NFC Device with a registered card by means of an antivirus program and ensure its regular update;
- secure the NFC Device with an access password, protect the access password and the one-time password for card registration, do not disclose or make them accessible to other people;
- disallow transactions to be carried out by another person;
- protect the NFC Device from software misuse and prevent its loss, theft or misuse;
- immediately report to the Bank the loss, theft or misuse of the NFC Device and immediately block the Card in the NFC Device via internet banking, mobile application or the Bank's call center;
- not to share the card data (card number, validity and CVC/CVV code) with a third party.

5.6. The Bank is entitled to unilaterally restrict or terminate the possibility to execute transactions using the NFC Device. The Bank is not liable for the loss caused by the restriction or termination of transactions using the NFC Device.

5.7. When cardholders use the Application for payment transactions, the Bank processes their personal data to the same extent as when they use the Card. In addition, data relating to the NFC Device may be processed for the purposes of providing customer support, resolving disputes and preventing fraud during the provision of the Service. More information on the processing of personal data is provided in the document “Information on the processing of personal data” which is available at www.expobank.cz/document/pravni-informace.

5.8 The Bank is entitled to provide data on transactions performed using the Application to the Provider. The Provider reserves the right to use this information for the purposes stated in the conditions of use of the Service and in accordance with the instructions on the processing of personal data.

6. TRANSACTION SETTLEMENT AND CLAIMS

6.1. Payment card transactions are debited from the account on a daily basis after they are processed by the clearing center. Upon authorization, Bank has the right to reserve the applicable transaction amount on the account holder's account. The reserved funds will be actually debited from the account holder's account only after the Bank receives all transaction information. The Bank does not review the grounds for orders submitted using a payment card. Until funds are debited from the account holder's account, the Bank is unable to review the grounds for a given reservation. If transaction details are not delivered to the Bank within the timeframe corresponding to the rules and customary practices of the MasterCard Association, the Bank cancels the applicable reservation. For selected merchant types, the reserved amount may be set as an estimate of costs expected to be incurred (hotel accommodation, car rental, etc.).

6.2. Settlement currency of the Bank for foreign currency transactions is EUR. Transactions in a currency other than the settlement currency (EUR) are converted by the MasterCard association from such currency to the settlement currency by official exchange rate of MasterCard association valid at the time of the transaction. Exchange rates used by MasterCard association may change during the day based on the development of rates of main currencies on the world currency markets. The bank is converting the settlement currency to the currency of the account to which transactions

are debited using foreign currency sale exchange rate of the Bank in effect at transaction processing time.

6.3. The account holder acknowledges the method used for the settlement of payment card transactions completed abroad. No claim may be made regarding exchange differences relating to the settlement of payment card transactions completed abroad. Exchange differences may be due to a difference between the transaction and settlement dates or to a payment converted to a settlement currency and subsequently to the account currency. As to a credit transaction submitted by a merchant or another bank for an already completed transaction, the Bank bears no liability for any difference in the value of converted amounts arising from a delay between the settlement of debit and credit transactions.

6.4. If a payment card is issued for several accounts denominated in different currencies, the account holder acknowledges that card transactions are charged to the applicable account based on the transaction currency. If technically feasible in view of the authorization conditions, a transaction may be charged to an account denominated in a different currency which has a sufficient balance for settling the transaction at settlement time. However, the Bank is under no obligation to carry out settlement using such another account.

6.5. The account holder and a cardholder must verify promptly and regularly the accuracy of the settlement of payment card transactions using account statements or the Internet banking system to allow, among other reasons, making claims in a timely manner.

6.6. If a cardholder opts to have a foreign payment card transaction settled in CZK or another currency that differs from the transaction currency (for instance at a payment terminal, ATM, etc. – the so-called DCC – Dynamic Currency Conversion), the transaction sum is always converted by the merchant using the merchant's exchange rate (the exchange rate and the converted sum are usually indicated on the receipt). The Client has an option of deactivating DCC within the electronic banking service, at the Bank's branch or, via the Bank's mobile application (if this service is available in the application). A transaction using DCC will be automatically rejected if DCC is deactivated.

6.7. Any discrepancy concerning a payment card transaction ascertained by the account holder or the cardholder must be reported in writing immediately (without delay after detection) at the Bank branch, together with a request for the rectification of such a discrepancy. Together with a claim, the account holder or the cardholder must enclose all available documents (copies of account statements, copies of receipts, a sworn statement of the cardholder or the account holder disproving a transaction). the Bank may ask the cardholder or the account holder to provide additional documents regarding a disputed transaction. The cardholder or the account holder must assist the Bank as necessary in the processing of a disputed transaction. Until the end of the next working day after the Bank was notified by the account holder of an unauthorized payment, the Bank (i) regularizes the account from which the sum was debited so that it corresponds with the state of the account before the unauthorized transaction was debited or (ii) returns sum of the transaction including paid remuneration and loss of interests to the payer if the procedure stated in point (i) of this sentence is not applicable. Procedure according to the previous sentence is not applied if the account holder bears a loss from unauthorized payment according to these Conditions.

6.8. The account holder or a cardholder must make a claim without unnecessary delay (immediately after detection) using the applicable the Bank form within 13 months after a claimed transaction is charged to the account holder's account, in accordance with the the Bank Complaint Guidelines.

6.9. The account holder and/or the cardholder must inform the Bank if a claimed sum is refunded by the merchant.

6.10. The account holder or a cardholder may submit a claim concerning an erroneous transaction or another discrepancy, which is made in accordance with these Conditions and is rejected by the Bank, to the financial arbitrator who settles disputes between payment card issuers and cardholders (consumers) regarding the issue and use of electronic payment means in accordance with the Financial Arbitrator Act (229/2002), as amended. The Financial Arbitrator is a non-judicial authority established by government competent to decide certain disputes at the financial market. For

additional information, visit www.finarbitr.cz. The cardholder or the account holder may also file a claim with the Czech National Bank, Na Příkopě 28, 115 03 Prague 1, www.cnb.cz, the supervisory authority in charge of overseeing banking services. The cardholder or the account holder can also file a complaint with a court of law.

7. CARD PROTECTION, LOSS/THEFT

7.1. The cardholder must keep the card in a safe place and prevent its misuse by unauthorized persons. The cardholder must refrain from allowing a third party to use the card. The cardholder must **prevent the disclosure of a PIN code, ePIN code or a mobile application PIN code, as well as disposable codes sent via 3D Secure to any third party**. The cardholder must not record the PIN code, ePIN code or a mobile application PIN code in any form which would allow their disclosure and **must not be kept together with the card**. Cards must be protected against mechanical damage and the effect of strong magnetic fields.

7.2. In the event of any doubt or suspicion of ATM fraud (such as stuck banknotes, presence of a scanning device allowing the copying of payment card data, or irregular cash disbursement) or in the event that suspicious persons are present near an ATM and attempt to intervene in a transaction, the cardholder must inform the Bank and the Police immediately.

7.3. The cardholder must report card loss or theft immediately by contacting the authorization center of Global Payments Europe, which is open 24 hours a day, at +420 267 197 197. It is also possible to block the payment card through internet banking or mobile application.

7.4. A "Payment Card Loss, Theft, Finding" report may be made by a third party. Such a third party must inform the Bank of all circumstances concerning the loss, theft, finding of the payment card.

7.5. If the reporting person does not know the card number, other details must be provided based on which the card can be identified (cardholder's name, Birth Registration Number, account number, card issuer, and card type). The reporting person must not disclose the PIN code, ePIN code or a mobile application PIN code to any responsible Bank employee.

7.6. The account holder is liable for all costs and any losses incurred due to using of lost or stolen card or a card misuse in an unauthorized transaction up to EUR 50 or equivalent. This limit on the account holder's liability only applies to cards issued for accounts of private individuals who are consumers, and only if (i) payment transaction was not caused by fraud, deliberately, or by negligent breach of any of the obligations stated in the Agreement or Conditions (ii) loss, theft misuse or unjustifiable use of the card have been reported to the Bank without undue delay. If the account holder not a private individual consumer, the account holder is fully liable and must bear the full amount of costs and losses incurred due to an unauthorized payment transaction arising from card misuse. The liability for the use of a lost or stolen card passes from the account holder to the Bank at the time a blocking request is made. If damage is incurred due to a gross violation of obligations committed by a cardholder, the account holder is liable for all related costs and losses with no limit.

7.7. As regards the calculation of losses arising from an unauthorized transaction, the reference date for claims made by the account holder is the date and time at which card loss, theft, or misuse report is made.

7.8. Following the receipt of a lost, stolen payment card report, the Bank will block the card or place it on the stop list. The card will remain blocked until the blocking request is revoked in writing by the person who made the request. The Bank is authorized to block a payment card at its discretion to ensure payment card security, for example if the Bank suspects unauthorized or fraudulent payment card use or in the event of unauthorized account overdraft where the risk exists that the balance due will not be repaid.

7.9. The Bank may debit the account holder's account for any and all expenses and losses it incurs as a result of a failure to comply with these Conditions by persons holding cards issued for the

account holder's account.

8. TERMINATION OF THE AGREEMENT, CANCELLATION OF THE AGREEMENT, CARD CANCELLATION

8.1. The Agreement is terminated:

(a) on the last day of the card expiration date, unless another card has been issued by the Bank.
(b) upon closing the account to which the payment card was issued (if the card is issued to more than one account, the Agreement terminates by canceling the last of these accounts);
(c) upon termination of the notice period on the basis of a written notice of termination of the Agreement by one of the contracting parties;
(d) upon termination of the notice period on the basis of a written notice of termination of the relevant payment service framework agreement by one of the parties. For the purposes of the Article 8 of these Conditions, the relevant payment service framework agreement shall mean in particular the agreement on the opening of account, to which the card in question is issued;
(e) upon cancellation of the holder's right to dispose of the card by the account holder pursuant to paragraph 8.2 of these Conditions;
(f) upon a written agreement of the contracting parties on the cancellation or termination of the Agreement, or upon agreement of the contracting parties on the cancellation or termination of the relevant payment service framework agreement;
(g) by written withdrawal from the Agreement on the basis of provisions stipulated by these Conditions;
(h) if, in accordance with the relevant provisions of the GTC, legal regulations or the relevant payment service framework agreement, the relevant payment service framework agreement is revoked, the Agreement shall terminate together with such relevant payment service framework agreement.

8.2. An account holder may terminate the Agreement at any time or cancel the cardholder's right to dispose of it. Request of termination and cancellation must be made in writing and shall take effect on the day of its delivery to the Bank. Termination of the Agreement or cancellation of the card does not affect the settlement of payment transactions that were made via the card before the notice of termination or cancellation in question took effect.

8.3. The Bank is entitled to terminate the Agreement in writing with a two-month notice period, even without giving a reason. The notice period begins on the day the notice is delivered to the account holder. In such case, the Agreement will terminate upon expiry of the notice period. Termination does not affect the settlement of payment transactions that were made via the card before the termination of the Agreement.

8.4. If the relevant payment services framework agreement is terminated, the duration and the start date of the notice period is governed by provision 14.2 of the GTC.

8.5. In the event of a fundamental violation of these Terms and Conditions and/or of the Agreement or the relevant payment services framework agreement by an account holder or a cardholder, the Bank is entitled to withdraw from the Agreement at any time in writing. Withdrawal from the Agreement takes effect on the day of the written statement delivery to the account holder. Cardholder or the account holder is obliged to invalidate the card by cutting it over a magnetic tape and chip no later than 5 working days from the delivery of the withdrawal statement and to prevent access to the payment card data.

8.6. If the Agreement or the relevant payment services framework agreement is terminated or canceled by a written agreement of the contracting parties on the agreed date, the account holder or the cardholder is obliged to invalidate the card by cutting it over a magnetic tape and a chip no later than the next working day after the agreed day and to prevent access to the payment card data.

8.7. With the termination of the Agreement, an account holder is not relieved of the obligation to settle all obligations arising from the use of the given payment card and the obligation to invalidate the given payment card by cutting over magnetic tape and chip and to prevent access to payment

card data. The account holder remains responsible for all transactions made with the card before it is invalidated, blocked or placed on the stop list.

9. EFFECTIVENESS

9.1. These Conditions are valid from 1.3. 2021 ("issue date") and effective as of 15. 5. 2021 and replace the existing Conditions.

9.2. In accordance with Article 44 of the GBC, the Bank is entitled to amend these Conditions unilaterally.

9.3. The Bank will inform the account holder and the cardholder of any changes to the Conditions and data on reporting the loss or theft of the card pursuant to Article 6.3 of the Conditions in a suitable manner (e.g. by a message sent within the electronic banking service, via the Bank's website, account statement information, etc.).