INSTRUCTIONS FOR MERCHANTS ACCEPTING PAYMENTS VIA PAYMENT CARDS

UniCredit Bank
Czech Republic and Slovakia, a.s.

UniCredit Bank

TABLE OF CONTENTS

These Instructions contain the relevant rules formulated by the card associations and thus constitute the terms and conditions formulated by professional organisations in accordance with Section 1751 (3) of Act No. 89/20212 Coll., the Civil Code. These Instructions (hereinafter referred to as the "Instructions" are in effect from 1ST August 2025 and are intended for businesses with whom UniCredit Bank Czech Republic and Slovakia, a.s. (hereinafter referred to as "UniCredit Bank") has concluded an Agreement on Acceptance of Payment Cards (hereinafter referred to as "Merchants").

1. DESCRIPTION AND TYPES

1.1 DEFINITION OF TERMS USED HEREIN

Authorisation
The process by which the validity of the payment card and coverage of the given payment by such card are verified.

Authorisation centre
The place where payment authorisation, i.e. verification of the validity of the payment card and verification of coverage of the given payment by such payment card, is carried out.

Authorisation code
A four- to six-digit sequence of numbers or numbers and letters that serves as confirmation of consent to the executed transaction.

Bank
The Bank processes the Merchant's transactions executed by means of Mastercard, Visa payment cards and the Alipay application.

Banking day
A banking day is understood to be a day when banks are open to the public in the Czech Republic.

Cash Advance
Disbursal of cash upon presenting a payment card.

CVC2 (CVV2)
Security code comprising the last three digits printed on the back of the payment card (Card Verification Code / Value).

Identification document
A valid identity card, driver's licence with photo, passport or ID card with photo in the case of a European Union country.

Cardholder
A natural person who fulfils the conditions for the issuance and use of a payment card and whose name and surname may be indicated on the payment card.

EFT/POS terminal
A device intended for the electronic processing of transactions executed by means of payment cards.

Card schemes
The companies Visa International, Mastercard Worldwide and Alipay.com Co.

Mail Order/Telephone Order (MO/TO)
Payments rendered by payment card when the identification data is provided by the cardholder in written form or by telephone with subsequent written confirmation, without the Merchant having the option to see the payment card.

Card owner
The bank that issued the card to the holder for use (i.e. card issuer).

mPOS
mPOS is a portable electronic device that enables acceptance of payment cards and is connected to the authorisation centre via a smartphone or tablet.

Point of sale
The place where the Merchant accepts cashless payments for goods and services.

Merchant / Contractual Partner
A legal entity or natural person who conducts business and has concluded an Agreement on Acceptance of Payment Cards with UniCredit Bank.

PCIDSS
(Payment Card Industry Data Security Standard) International rules defining the conditions for handling cardholder data contained on payment cards.

Payment card
A payment card is a plastic card with dimensions of approximately 85 mm × 54 mm, whose appearance, data arrangement and security elements correspond to the specifications of the relevant card scheme on the front and back of the card. A payment card enables its holder to make cashless payments for goods and services and to withdraw cash. The payment card remains the property of the card issuer and is issued to the cardholder for use. Payment cards are non-transferable.

Period of payment-card validity
The period during which the cardholder is authorised to use the payment card to pay for goods and services and to withdraw cash. The period of validity is indicated on the lower half of the front of the payment card.

Exchange office
A place that provides disbursal of cash upon presentation of a Mastercard or Visa payment card.

Transaction
Payment for goods and services using a payment card.

Receipt
A document about payment rendered by payment card confirming the acceptance of goods or the use of services.

Visual inspection
Inspection of the presence and correctness of all security elements, see Chapter 1.2–1.5. The purpose of such inspection is to prevent the use of counterfeit cards.

Payment-card issuer
The Bank or other financial institution that is authorised to issue Visa and Mastercard payment cards. The payment-card issuer is concurrently authorised to block payment cards.

Prohibited card
A card that is designated on the terminal display with the text "RETAIN CARD" during payment authorisation. A prohibited card is also understood to be a payment card whose security features do not correspond to the requirements of the card schemes (see the card illustrations). A prohibited card may not be used to pay for goods or services or for disbursal of cash. It must be retained, rendered unusable and handed over to the bank.

1.2 HOW TO ACCEPT PAYMENT CARDS

A PAYMENT CARD IS DEEMED INVALID FOR EXECUTING TRANSACTIONS AND THE MERCHANT MAY NOT ACCEPT IT FOR PAYMENT IF:

- the signature on the card does not match the signature on the receipt (after correct entry of the PIN, the Merchant does not have to demand the cardholder's signature; acceptance of cards via EMV chip is described in Chapter 2.3).
- the period of validity shown on the card has expired.
- the card is demonstrably presented by a person other than the person indicated on the card and whose signature appears on the back of the card.
- the signature is damaged (by erasing, overwriting, etc.).
- the card is mechanically damaged or has been rendered unusable.
- CVV2 or CVC2 – the three-digit code on the back of the card – is missing.
- the number shown on the display of the EFT/POS electronic terminal or printed on the receipt does not match the number on the front of the card. In such case, it is necessary to retain the card!

The payment card may not be marked with the inscription "SPECIMEN", "VOID" or "VZOR", nor may it have been cut or otherwise damaged.

If any of the above descriptive elements, data or characteristics are missing or if you have any doubts about the validity of the given card, please contact the authorisation centre without delay and state the phrase "code 10".

1.3 HOW TO PREVENT ATTEMPTS TO COMMIT PAYMENT-CARD FRAUD AT AN ELECTRONIC TERMINAL

The behaviour of some customers may indicate that they are attempting to commit fraud when paying by card. Please bear in mind, however, that suspicious behaviour does not necessarily mean illegal activity – you know your customers, so let your instincts guide you.

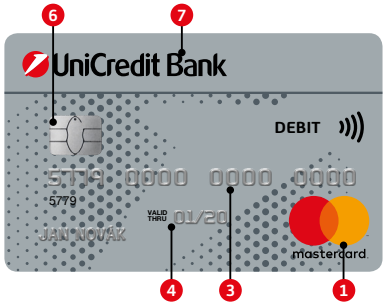
Pay attention to customers who:
– purchase large amounts of goods that are easily exchangeable for cash (e.g. prepaid cards, top-up codes, etc.)
– carry out a large number of consecutive contactless transactions up to the amount of CZK 500 – for transactions up to this amount, a contactless chip usually does not require entry of the PIN code or a signature for confirmation, so a card used in this manner may have been stolen.
– returns to the store after a successful purchase in order to buy again (more).

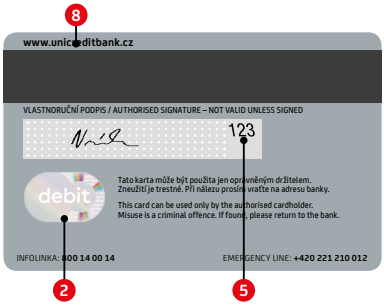
If you encounter behaviour that arouses your suspicion:
– demand to see an identification document (see the definition of terms) and verify whether the data contained in the document matches the data on the card; write the number of the identification document on the receipt).
– follow your company's procedures and alert your superior.
– call the authorisation service and state the phrase "I am authorising with code 10" to the operator and then follow the operator's instructions.

NEVER PUT YOUR OWN SAFETY AT RISK.

1.4 DESCRIPTION OF THE MASTERCARD PAYMENT CARD

Mastercard payment card features:





1 Mastercard logo
It consists of two interlinked circles in red and yellow.

2 Hologram
Interlinked circles with the inscription “Mastercard” on the edge of the right circle.

3 Card number

4 Card validity

5 Three-digit security code (CVC2)

6 Chip or contactless chip

7 Name and logo of the issuer

8 General instructions and address of the card issuer

Other optional elements:

Cardholder’s name

Signature panel
If present on the card, the cardholder‘s signature serves as a specimen signature. The signature panel may not be damaged and may not contain the word “VOID”.

Magnetic stripe
Protective UV symbol The letters “m” and “c” are only visible under ultraviolet light.

The payment card may also contain other information, such as the company name, a photograph of the holder, or special characters.

1.5 DESCRIPTION OF THE VISA PAYMENT CARD

Visa payment card features:

1 Visa logo
The Visa logo may have different vertical orientations.

2 Card number (only part of the card number may be provided)

3 Card validity

4 Chip or contactless chip

5 Magnetic stripe

6 Name and logo of the issuer

Other optional elements:

Cardholder's name

Three-digit security code (CVV2)

Signature panel
If present on the card, the cardholder's signature serves as a specimen signature. The signature panel may not be damaged and may not contain the word "VOID".

Hologram
Dove in flight

General instructions and address of the card issuer

Protective UV symbol
The capital letter 'V' is only visible under ultraviolet light.

The payment card may also contain other information, such as the company name, a photograph of the holder, or special characters.

2. ELECTRONIC PAYMENT TERMINAL

2.1 CARD PAYMENT VIA AN ELECTRONIC TERMINAL

Mastercard, Visa and V Pay payment cards can be accepted at stores.

The Merchant must sell goods and provide services to cardholders at the same prices and under the same conditions as to customers who pay cash. At its place of business, the Merchant may not set any price limits from which it will accept payments made using Mastercard, Visa and V Pay.

2.2 PROCEDURE FOR USING AN ELECTRONIC TERMINAL

The Merchant shall proceed in accordance with the manual provided by the company that carried out installation of the terminal. A properly signed sales receipt or a sales receipt confirmed by means of a code or using the biometric method and issued upon insertion of the payment card into the terminal serves as proof of the given transaction and of the cardholder's acknowledgement of the debts owed to the Merchant arising from the transaction (acceptance of contactless cards – see Chapter 2.4).

GENERAL INFORMATION:

- **The Merchant must finish its daily operation upon closure of the terminal.**
- The Merchant shall proceed in accordance with the manual provided by the company that carried out installation of the terminal.

By permitting transactions using a terminal, the employee is not relieved of the obligation to check:

- that the customer's signature matches the specimen signature on the card or to verify the cardholder's identity (this does not apply to payment cards that have no signature panel); checking the cardholder's identity is understood to involve checking the information specified below and writing it on the sales receipt:
  - type of document
  - document number
  - document issuer
  - name and surname of the person presenting the document corresponding with the data on the payment card if the name is shown on the card

  Only a national identity card, passport or identification document valid in the relevant EU country can be used for verification of identity. The employee shall perform a visual inspection of the payment card (this does not apply to contactless cards) and verify:
  - whether the security elements are visually in order
  - whether the card is damaged, has been rendered unusable or has been cut – if so, the employee shall reject the card and return it to the customer

2.3 EMV – ACCEPTANCE OF CHIP CARDS

- It is necessary to execute chip-card transactions (EMV standard) using **only** the terminal's chip reader.
- After selecting the type of transaction and entering the amount when prompted by the terminal (or cash-register system), enter the chip card with the chip facing up into the reader in the payment terminal (see the image below).
- If a transaction is executed using a chip, in most cases the cardholder will be prompted to enter the PIN, or as the case may be, to use the biometric verification method.
- If a transaction is executed using a chip, it is usually not necessary to sign the receipt (no line for the cardholder's signature is printed on the receipt). In some cases, a signature line may be printed on the receipt; in such a case, the cardholder's signature is required.

2.4 ACCEPTANCE OF CONTACTLESS CARDS

Contactless transactions are certified by the Visa and Mastercard card schemes and enable transactions via both contactless payment cards and mobile telephones with NFC technology supporting the PayPass and PayWave standards. Such transactions can be processed by presenting other contactless media (e.g. a sticker or contactless wristwatch). Use of the PayPass and PayWave technology is uniformly indicated by the following symbol:

Simplicity:
- Contactless payments are carried out simply by placing a contactless card or mobile telephone near the contactless reader of the payment terminal.
- In the case of a payment up to CZK 500, it is not necessary (with some exceptions) to authorise the contactless transaction by entering the PIN or signing the receipt.

Security:
- It is not possible to accidentally make a payment. Contactless payments are executed by placing the card near the payment terminal at a minimum distance.
- Individual settings from the payment-card issuer my require a PIN/signature even for transactions under CZK 500 for the purpose of ensuring security of payments.
- Contactless payments over CZK 500 shall be confirmed by entering a PIN or providing a signature according to prompts from the terminal.

2.5 CARD PAYMENT VIA mPOS

An mPOS is an electronic device for accepting payment cards via smartphones and tablets.

GENERAL INFORMATION:

- The Merchant must finish its operation upon daily closure of the mPOS.
- When executing a transaction, the Merchant shall proceed in accordance with the manual issued by the service company that provided the mPOS.
- The mPOS does not print receipts for cardholders. The Merchant must offer cardholders the option to send receipts via SMS or e-mail.
- Receipts for the Merchant are retained only in electronic form, and access to them is described in the manual issued by the service company that provided the mPOS.

2.6 ACCEPTANCE OF ALIPAY

The Merchant can accept payments via the Alipay mobile application. Alipay enables its users to pay for goods/services using a QR code, which is displayed on the display of the EFT/POS terminal and on other devices that serve for the acceptance of payment cards. Detailed information about executing Alipay transactions is provided in the manual issued by the supplier of the EFT/POS terminal.

3. OTHER

3.1 EXCHANGE OFFICE, CASINOS

ESSENTIAL STEPS AND PROCEDURES THAT MUST BE CARRIED OUT WHEN ACCEPTING CARDS:

The following must be printed on the receipt:
- the document's date of issue
- the amount and currency of the transaction
- the card number and the Merchant's identification number

If the transaction has not been verified by entering a PIN or biometric method and for Visa card transactions over USD 500 (equivalent in another currency) the cardholder's identity must be verified by checking a valid identification document (see the definition of terms) and adding the following to the sales document:
- type of identification document
- the cardholder's signature, which must match the signature shown on the signature panel on the back of the card if the card has a signature panel (this does not apply to chip cards and cards for which the paymentcard issuer does not require a signature – in such case, transactions are confirmed by entering a PIN or by means of the biometric method)

3.2 PRE-AUTHORISATION

PRE-AUTHORISATION can be used in cases when the amount of the transaction is not known in advance.

Pre-authorisation can be carried out via payment terminals (EFT/POS) at hotels, vehicle-rental facilities and rental shops of all types. The employee estimates the amount that the customer will pay for the service (e.g. based on the length of stay, the duration of the period for which a vehicle or other goods are rented) and then pre-authorises the transaction.

RECOMMENDATION: When the client arrives or picks up the vehicle/device or other goods, request the payment card for which pre-authorisation has been carried out and have the cardholder sign the receipt with the authorisation code and the amount.

When completing the transaction (check-out from a hotel, return of a vehicle/device or goods), the Merchant carries out **COMPLETION OF PRE-AUTHORISATION**.

- Completion of pre-authorisation cannot be carried out without prior pre-authorisation.
- Pre-authorisation must always be completed or cancelled within 30 days.
- In the case of embossed cards, pre-authorisation and completion thereof can be carried out without the presence of the payment card. The Bank recommends that completion of pre-authorisation always be carried out with the presence of the payment card due to the possibility that the cardholder may file a claim with respect to the transaction.
- Pre-authorisation may not be requested as a warranty for damage or loss.
- If, during the completion of pre-authorisation, the actual amount is lower than the estimated amount for which pre-authorisation was carried out, the Merchant shall complete pre-authorisation in the usual way in the amount actually drawn.
- Pre-authorisation is valid for only 30 days from the date when it is carried out (in the event that the client wants to make a reservation a longer time in advance, carry out pre-authorisation of the transaction 25–30 days before the cardholder's arrival).
- Before carrying out pre-authorisation, it is necessary to inform the cardholder of the fact that pre-authorisation will be carried out and that it is necessary to state the value of the pre-authorised amount.

In the case of cards issued by the company **Mastercard Inc.**, the following exceptions apply:
- The amount upon completion of pre-authorisation (final authorisation) must be equal to or less than the pre-authorised amount. If the actual amount exceeds the pre-authorised amount, the Merchant shall complete pre-authorisation for the pre-authorised amount and must subsequently authorise the difference between the pre-authorised and actual amounts.

In the case of cards issued by the company **Visa Inc.**, the following exceptions apply:
- Pre-authorisation is valid for 30 days from the date when it is carried out (this applies for accommodation facilities and vehicle-rental facilities). In the case of other rental shops, pre-authorisation is valid for only seven days.
- If the actual amount exceeds the pre-authorised amount by less than 15%, the Merchant can complete pre-authorisation in the usual way. If the actual amount exceeds the pre-authorised amount by more than 15%, the Merchant shall complete pre-authorisation for the pre-authorised amount and must subsequently authorise the difference between the pre-authorised and actual amounts.

Successful completion of pre-authorisation cannot be cancelled using the RETURN function, as such a transaction may cause an exchange-rate difference and the cardholder could incur damage as a result.

Successfully completed pre-authorisation cannot be cancelled using the CANCEL function. In the case of refunding money due to an erroneous transaction, it is necessary to request, in writing, that the Bank cancel such transaction. Such request shall be sent to the e-mail address obchodnici.reklamace@unicreditgroup.cz.

3.3 MO/TO (MAIL ORDER / TELEPHONE ORDER)

MO/TO
MO/TO is a transaction executed on the basis of a written or telephone order of goods or services, where the future payment will be carried out without physical presentation of the card by its holder to the provider of the goods or services.

MO/TO transactions can be executed only on the basis of a special agreement with the Bank!

- The Merchant ensures that the "Account Debit Agreement" form has been completed (see Annex 2; hereinafter referred to as the "Form").
- With his/her signature, the cardholder confirms, in writing, his/her consent to the execution of the transaction.
- On the date of receipt of the order, the Merchant enters the transaction into the electronic terminal.
- Upon authorisation, the Merchant renders the CVV2/CVC2 code on the Form illegible by blacking it out or cutting it out of the marginal part of the Form. The Merchant will then dispose of the cut-out part of the Form by shredding or burning it.

Form – Account Debit Agreement
By issuing this form and signing it, the cardholder acknowledges his/her obligation to pay for the ordered goods or services and confirms the correctness and accuracy of the data provided on the Form.

All types of document must be legibly completed and may not contain any corrections or strikethroughs. The Form may not be retained with information about the CVV2/CVC2 code, even in the case of a rejected transaction.

Dispatch of goods:
A Merchant that dispatches goods to a cardholder must send the goods in such a manner that makes it possible to unambiguously demonstrate delivery of the goods and acceptance by the recipient.

3.4 OTHER TYPES OF TRANSACTIONS

NO SHOW
Payment for a reservation that is not cancelled and not used – e.g. the customer orders a service (reservation of a hotel room) and does not cancel it or does not cancel it in time. If such a case occurs, the Merchant is authorised, in accordance with the rules issued by the scheme, to charge the customer for only one night or for one day of vehicle/device rental as compensation!

Conditions:
- The Merchant must inform the client of the charge by fax or e-mail.
- The Merchant must have the card information (card number, period of validity) available. For this type of transaction, the Merchant shall never request a CVV2/CVC2 code.
- The Merchant must have a written order of goods or services.
- The Merchant must have the right to such compensatory billing in its terms and conditions for the provision of services. The Merchant shall prepare a sales receipt with all requisites, including the words "No Show" in the space intended for the cardholder's signature.

DELAYED OR AMENDED CHARGES
ADDITIONAL CHARGING OF SERVICE FEES
If, after the transaction has been executed and the cardholder has departed, it is ascertained that the service has not been paid for in the full amount (e.g. unpaid telephone calls, consumption of refreshments from the hotel minibar, fine for an offence committed), the Merchant may demand payment of the unpaid amount. The Merchant shall complete a supplemental sales receipt with all requisites and legibly write "Signature on File" (or "S.O.F.") in the space intended for the cardholder's signature. The Merchant must inform the cardholder of the reason for such additional charge by fax or e-mail. The Merchant shall also send a copy of the sales receipt to the cardholder's address.

However, all of these methods of charging the cardholder (MO/TO, No Show, S.O.F.) are charged to the Merchant subject to cancellation. Therefore, the given transaction is valid if the cardholder does not file a claim against it, i.e. does not deny having used the goods or services provided by the Merchant.

NOTICE FOR MERCHANTS PROVIDING ACCOMMODATION SERVICES:

In connection with the Agreement on Acceptance of Payment Cards for Accommodation Services, the Merchant may settle payments for its services without the physical presence of the payment card by executing the following types of transactions: pre-authorisation, No Show, S.O.F., Advance Deposit (guaranteed reservation), Priority/Express Check-Out Service. In the case of Advance Deposit transactions where the Merchant charges the payment card for the planned accommodation in advance, it is necessary to emphasise that such transactions are always charged subject to cancellation. If the cardholder files a claim against such a transaction, the Bank shall be authorised to debit, without the Contractual Partner's prior consent, the amount thus paid from subsequent payments to the Contractual Partner.

Suspicious behaviour of clients that could lead to fraud:

- Reservations for an unusually long period or for a large number of persons, usually sent by e-mail directly to the hotel.
- The payment card is rejected in the course of authorisation and the customer immediately sends more and more card numbers or requests that the total amount of the transaction be divided among multiple offered card numbers.
- You are approached by a foreign travel agency that guarantees accommodation for its clients by presenting a payment card and concurrently requests that you send a commission for its service to its bank account.

How to proceed in such cases:

- If you have used the Advance Deposit (guaranteed reservation) method to charge an amount for a reservation and the cardholder subsequently cancels the reservation, never accede to refunding the amount in any way other than to the original card number (not, for example, to a bank account, in cash or by dispatching goods).
- Never accept orders of other services or goods that are not directly associated with accommodation services (e.g. purchase and delivery of electronics).
- If the guest is present, always demand physical presentation of the payment card and execute the transaction using the card (magnetic strip, chip, contactless). Never agree to use payment-card information dictated to you by the person presenting the card (e.g. from a mobile telephone, computer).

In order to reduce the risk of claims arising from possible fraudulent transactions, the correct and appropriate procedure in the case of guaranteed reservations is to carry out pre-authorisation at the POS terminal and to subsequently complete the transaction with the presence of the payment card upon the guest's arrival. The card will thus be verified by the POS terminal. If the guest is present, always request physical presentation of the card and execute the transaction with the presence of the card (magnetic strip, chip, contactless). Another possible way to prevent fraudulent reservations is to accept cards via an e-commerce payment gateway (push pay payments) with 3D security.

If you have any questions, please contact the payment-card security department or the authorisation service.

3.5 RETENTION OF PAYMENT CARDS

The Merchant must retain a payment card in the following cases:
- The Merchant received a "RETAIN CARD" order from the authorisation centre.
- The security elements on the card do not correspond to the schemes' requirements (see Chapter 1.2–1.5). Contact the authorisation centre and state the phrase "code 10", whereupon the operator will verify the authenticity of the card, or as the case may be, instruct the Merchant to retain the card.

The payment card is the property of the company that issued it, i.e. the card issuer. The customer is only the holder of the card. A request for authorisation is submitted via a computer network to the card issuer, which decides on the response to such request. The employee therefore must comply with the issuer's demand to retain the customer's payment card. **If the cardholder wants to know the reason for the retention of his/her payment card, he/she must contact the card issuer.**

When a card is retained, the Merchant shall use all reasonable and non-violent means to ensure that the card remains in the Merchant's possession. The Merchant shall render the retained card unusable in view of the cardholder, and upon request, issue the customer with "CONFIRMATION OF RECEIPT OF A RETAINED PAYMENT CARD" (see Annex 1).

The Merchant shall fill out the "CONFIRMATION OF RECEIPT OF A RETAINED PAYMENT CARD", which must contain the Merchant's name, address and identification number, the employee's name and address, the employee's account number, the date of retention and the date of sending the card, the reason for retention, and the payment-card number. The Merchant shall hand over the confirmation together with the payment card to any UniCredit Bank branch in person or send it by registered mail within one week to the UniCredit Bank payment-card department (see the TELEPHONE CONTACTS AND DIRECTORY).

The Merchant shall never provide the contact information of the authorisation centre to a cardholder.
In the cases described above, the Bank will decide on the payment of a reward for the retention of a payment card. The finder of a payment card is not entitled to a reward.
In the event of finding a payment card at its place of business, the Merchant shall fill out a "CONFIRMATION OF RECEIPT OF A FOUND PAYMENT CARD" (see Annex 3).

How to render Visa and Mastercard cards unusable
A payment card is rendered unusable by cutting it along the card number. Send retained payment cards to the address shown below:

UniCredit Bank – Card Centre CZ
Processing & Authorisations
BB Centrum – Filadelfie Building
Želetavská 1525/1
140 92 Prague 4 – Michle

3.6 CLAIMS

CLAIMS EXECUTED AT THE PAYMENT TERMINAL

The cardholder files a claim regarding the quality of provided goods or services
In the event that the cardholder files a claim with the Merchant regarding the quality of provided goods or services, the Merchant shall issue a refund of the claimed amount using the RETURN function in the terminal. Note: The RETURN function in the terminal is protected by a password set by the supplier. We recommend that the Merchant sets its own password via our helpline after installation of the terminal.

CLAIM REQUEST FILED BY THE MERCHANT

In the event of an incorrect settlement of a transaction (the cardholder is no longer present), the Merchant may file a claim request in writing (by e-mail, see the contact information below) by sending a "CLAIM REQUEST" form to the Bank (see Annex 4). For technical reasons, it is not possible to execute cancellations and partial cancellations of transactions for an amount of CZK 1 or less.

Additional settlement of transactions and transaction differences (this does not apply to Alipay transactions)
- The Merchant is not automatically entitled to additional settlement.
- The Bank must request the issuing bank's consent for additional debiting of the client's account.
- Additional settlement is ALWAYS SUBJECT TO CANCELLATION. If the cardholder files a claim against this transaction, this payment shall be charged to you later from your next payment, as the claimed transaction is not authorised.
- The BANK DOES NOT PERFORM additional settlement of amounts less than CZK 100.

4. SETTLEMENT OF TRANSACTIONS

4.1 SETTLEMENT OF PAYMENT TRANSACTIONS BY THE BANK

If the Merchant breaches the conditions under which the Agreement was concluded, for example, if the Merchant submits incorrect or incomplete documents or executes an unauthorised transaction, the Merchant will not be reimbursed for the transaction. In certain cases, the Merchant may be reimbursed for the transaction. If, however, the payment-card issuer does not reimburse the payment thus rendered or reverses recognition of a payment that has already been made, the Bank is authorised to offset such payment as its own receivable toward the Merchant against any of the Merchant's receivables toward the Bank. If the Merchant does not have any receivables toward the Bank, the Merchant will be called upon to remit the disputed amount to UniCredit Bank.

SUCH A CASE MAY OCCUR IF:

- authorisation was not carried out
- the sales receipt does not contain the customer's signature
- (if a signature was required for transaction using a POS terminal)
- the transaction was executed with a counterfeit card or through misuse of the card number, etc.

STATEMENT OF CARD TRANSACTIONS

UniCredit Bank normally credits the amounts from card transactions according to the total amounts per day (business date), i.e. for all card schemes together. Transactions are always credited separately for individual establishments. The net amount, i.e. the amount minus the provision, is credited to the Merchant's account unless the Merchant and the Bank agree on a different model for charging commissions.

IDENTIFICATION OF PAYMENTS IN THE STATEMENT OF PAYMENT-CARD TRANSACTIONS

Examples of transaction statements are available at:
https://www.unicreditbank.cz/cs/ostatni/struktura-a-format-elektronickych-vypis.html

IDENTIFICATION OF PAYMENTS IN ACCOUNT STATEMENTS

Sender:
UCB Merchants, account no. 9342510001/2700 for CZK, 9342510087/2700 for EUR, 9342510044/2700 for USD.

Variable symbol:
The full number of the Agreement, including the point of sale, e.g. 12001501.

Specific symbol:
Date of transaction settlement.

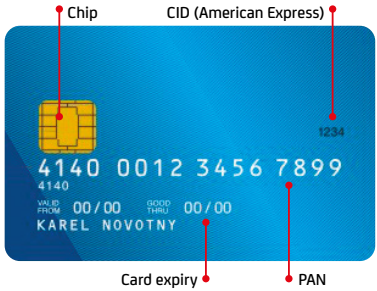
5. PCIDSS

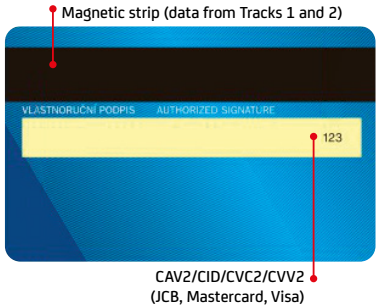
The Payment Card Industry Data Security Standard (PCIDSS) comprises a set of international rules that define the conditions for handling cardholder data contained on cards. These international rules, whose compliance with is required by card schemes and companies, are intended for organisations that process, transfer and store cardholder data (from payment cards and about card transactions). The purpose of the PCIDSS is to limit the risk of leaks of cardholder data and to thus prevent the misuse of such data. As a model framework for ensuring security, the PCIDSS contains the most appropriate procedures for minimising the risk of data theft. This standard is binding for all merchants that accept payment cards, and its basic requirements are included in the Product Terms and Conditions for Acceptance of Payment Cards.

By properly protecting cardholder data, you protect your customers and thus also your business.

Cardholder data that must be protected according to PCIDSS requirement No. 3.4:
- card number
- cardholder's name
- date of expiry of the card's validity

Sensitive authentication data that may not be stored in any way after authorisation, not even in encrypted form:
- all data from the card's magnetic strip or chip
- CVV2/CVC2
- PIN / PIN block





All items indicated with a red line are sensitive cardholder data. The data from the back of the payment card or the chip may not be stored in any way. The other indicated data may be stored if necessary for business or process reasons; however, such data must be protected according to the PCIDSS.

Build and maintain a secure network and systems.
1) Install and maintain network security controls.
2) Use secure configurations for all system components.

Protect your payment card details.
3) Protect the stored data of payment cardholders.
4) Encrypt the transmission of payment cardholder data over open public networks.

Maintain a vulnerability management program.
5) Protect all systems and networks from malicious software.
6) Develop and maintain secure systems and software.

Implement strict access control measures.
7) Restrict access to payment cardholder data and system components to authorised personnel only.
8) Identify users and verify access to system components.
9) Restrict physical access to cardholder data.

Regularly monitor and test your networks.
10) Record and monitor all access to system components and cardholder data.
11) Regularly test the security of your systems and networks.

Maintain information security policies.
12) Support information security through organisational policies and programmes.

If it is ascertained that a leak or misuse of cardholder data has occurred at the Merchant or the Merchant's agent, the Merchant must report such fact without delay to the Bank by e-mail at Cards.Fraud.Control@unicreditgroup.cz.

The rules issued by the card companies define the level to which Merchants are assigned based on the type and number of transactions executed per year. The Bank determines the level to which a given Merchant belongs.

Requirements for validation of Merchants' compliance with the PCIDSS (by level)

Merchant level	The Bank's validation requirements
1. Merchants with turnover of more than six million transactions per year	Audit conducted by an external auditor (QSA) or certified internal auditor (ISA), with a final report on compliance + a quarterly ASV scan (if applicable)
2. Merchants with turnover of one million to six million transactions per year	Audit conducted by an external auditor (QSA), with a report on compliance (ROC) or completion of a self-assessment questionnaire (SAQ), including attestation of compliance (AOC) by an internal certified auditor (ISA) + quarterly ASV scan (if applicable)
3. Internet Merchants with turnover of 20,000 to one million e-commerce transactions per year	Completion of a self-assessment questionnaire (SAQ) or demonstration of the use of a certified (in terms of the PCIDSS) provider of services or solution where the Merchant does not come into contact with payment-card numbers + quarterly ASV scan
4. Other	Completion of a self-assessment questionnaire (SAQ), including attestation of compliance + quarterly ASV scan (if applicable)

Abbreviations:
QSA (Qualified Security Assessor) – external certified auditor who conducts the onsite PCIDSS audit. A list of auditors is available on the official PCIDSS website.
ASV (Approved Scanning Vendor) – approved provider of monitoring. A company approved by the PCIDSS to provide services involving the monitoring of external vulnerabilities.
ISA (Internal Security Auditor) – an employee of the Merchant who has completed the PCIDSS certification programme.
SAQ (Self-Assessment Questionnaire) – A tool used by an entity for verification of its own compliance with the PICDSS.

All detailed information about the PCIDSS is available in Czech on the portal at www.pcistandard.cz; the original English version is available on the portal at www.pcisecuritystandard.org.

Please direct any questions regarding the PCIDSS to: cards.fraud.control.ubis@unicredit.eu.

Service providers (agents)

It is possible that, in carrying out its activities, the Merchant uses the services of a service provider and shares cardholder data with such provider. Service providers include, for example, airline and accommodation booking agents, operators of reservation systems, payment-gateway providers, webhosting companies, loyalty-programme operators, call centres, etc.

In such case, the obligation to protect cardholder data in accordance with the PCIDSS rules applies also to such companies, and the Bank **must be informed of such cooperation**.

These providers must also be in compliance with the PCIDSS and must register on the websites of the individual associations.

The Merchant may use only such service providers that are fully in compliance with the PCIDSS, and the Merchant bears full responsibility for them, including in the event of a data leak that occurs on the part of a service provider.

If the Bank ascertains that the Merchant is using a service provider that is not in compliance with the PCIDSS, then the Bank is authorised to suspend processing of the Merchant's transactions.

You can find out whether your agent is registered on the websites of the individual companies (see below):
Visa: here
Mastercard: here

6. TELEPHONE CONTACTS AND DIRECTORY

HELP-LINE: (nonstop)	**221 210 014**
TECHNICAL SUPPORT TO MERCHANTS:	**221 210 014, 013**
PAYMENT CLAIMS:	**955 962 876** **obchodnici.reklamace@unicreditgroup.cz**
ADDRESS FOR SENDING RETAINED PAYMENT CARDS:	**UniCredit Bank – Card Centre** Processing & Authorizations BB Centrum – Filadelfie building Želetavská 1525/1 140 92 Praha 4 – Michle
CONSUMABLE MATERIALS	
SONET, společnost s.r.o.: (terminal rolls) Payment-terminal operating manuals are available at www.sonet.cz/ke-stazeni/	**543 423 540, obchod@sonet.cz**
Aevi CZ s.r.o.: (terminal rolls)	**221 210 014, kz.objednavka@officeo.cz**
PAYMENT-CARD SECURITY DEPARTMENT – REPORTING OF COMPROMISED CARDHOLDER DATA: (e.g. loss/theft of receipts, electronic data or computer, network attacks, etc.)	**Cards.Fraud.Control@unicreditgroup.cz**
RESPONSE TO REQUEST FOR DOCUMENTATION:	**disputes.obchodnici@unicreditgroup.cz**

7. CONSUMABLES
PAYMENT-TERMINAL ROLLS

PAYMENT-TERMINAL ROLES CAN BE ORDERED FROM THE SUPPLIER OF THE GIVEN TERMINAL:

SONET, společnost s.r.o.
1. By e-mail sent to obchod@sonet.cz. In the e-mail, specify the name of your company, the required number of rolls, the delivery address and your contact information.
2. By telephone at number 543 423 543.
3. Via your payment terminal using the following procedure:
   a) on the home screen of the POS terminal – MAIN MENU
   b) select the hPOS function, confirm, ORDER, confirm
   c) on the next screen, select the product ROLLS; here it suffices to enter the required number of rolls and select send.

In the event of a problem, you will be contacted automatically.

DELIVERY AND PAYMENT METHODS:
1. in-person pickup at the registered office of SONET, Lužická 9, Brno, payment in cash
2. courier service (provided by SONET), payment made to the courier service upon delivery

Aevi CZ s.r.o.
By e-mail sent to kz.objednavka@officedepot.com. In the e-mail, specify the name of your company, the required number of rolls, the delivery address and your contact information.
The consumable materials will be sent to you together with the invoice via the PPL courier service.

8. ANNEXES

ANNE X NO. 1

UniCredit Bank

POTVRZENÍ O PŘEVZETÍ ZADRŽENÉ PLATEBNÍ KARTY VISA / MC
HOT CARD RECEIPT CONFIRMATION

Číslo karty
(Card number)

Platnost karty
(Card expiry)

Datum zadržení karty
(Date of pick-up)

Jméno obchodníka
(Merchant name)

Číslo smlouvy o přijímání PK
(Merchant number)

Jméno zadržitele
(Retainer's name)

Telefon
(Phone number)

Datum převzetí
(Date of receipt)

.....
Jméno a podpis pracovníka
(Name and signature of employee)

.....
Jméno a podpis zadržitele karty
(Name and signature of retainer)

Odměna se vyplácí pouze v případě zadržení karty na pokyn autorizačního centra UniCredit Bank Czech Republic and Slovakia, a.s.
The reward is paid only if the card is retained at the request of the UniCredit Bank Czech Republic and Slovakia, a.s. authorisation centre.

Číslo účtu zadržitele
(Retainer's account number)

Měna
(Currency)

Specifický symbol
(Specific symbol)

Kód banky
(Bank code)

Souhlasím s vyplacením odměny ve prospěch výše uvedeného účtu.
I agree with paying the reward to the above-mentioned account number.

.....
Jméno a podpis zadržitele karty
(Name and signature of retainer)

Tuto část vyplňuje pracovník oddělení vypořádání kartových obchodů UniCredit Bank Czech Republic and Slovakia, a.s.

Datum odeslání na účet

.....
Jméno pracovníka, podpis

Odesláním formuláře beru na vědomí, že banka bude zpracovávat osobní údaje v něm vyplněné z titulu nezbytnosti pro plnění smlouvy mezi bankou a smluvním partnerem za účelem naplnění práv a povinností touto smlouvou dohodnutých.
By submitting the form, I acknowledge and am aware that the Bank's processing of my personal data entered in the form is necessary for the performance of the contract by and between the Bank and the Contracting partner for the purposes of the rights and obligations agreed under this contract.

UniCredit Bank Czech Republic and Slovakia, a.s. I Sídlo / Registered Office: Želetavská 1525/1, 140 92 Praha 4 – Michle, www.unicreditbank.cz
IČO / Identification Number: 64948242 I Obchodní rejstřík / Commercial Register: Městský soud v Praze, oddíl B, vložka 3608 / Municipal Court in Prague, Section B, file 3608 I Směrový kód banky / Bank Code: 2700 I Swift Code: BACXCZPP

UniCredit Bank

SOUHLAS SE ZATÍŽENÍM ÚČTU

Vyplní obchodník (Merchant will fill in the following information):

Číslo objednávky (Order number)	
Datum (Date)	
Adresa obchodníka (Merchant address)	
Jméno odpovědného zástupce (Name of author. person of merchant)	
Popis zboží/služeb (Description of goods/services)	
Cena zboží/služeb (Price of goods/services)	
Dopravné (Transport costs)	
CELKOVÁ ČÁSTKA A MĚNA (vždy v CZK) (TOTAL PRICE)	

Vyplní držitel karty (Cardholder will fill in the following information):

Jméno a příjmení držitele karty (Name and surname of the cardholder)	
Adresa (Address)	
Telefon, fax (Phone No., Fax No.)	
Číslo karty (Card number)	
Platnost karty (Card expiry)	
Popis objednávaného zboží/služeb (včetně množství a ceny/měny) Description of goods/services ordered (incl. number of pieces and price/currency)	

Držitel svým podpisem stvrzuje správnost a pravdivost uvedených údajů. UniCredit Bank Czech Republic and Slovakia, a.s., za žádných okolností nezasáhne nebo neponese odpovědnost za jakékoliv spory, které event. vyvstanou mezi obchodníkem a držitelem karty v důsledku platby prostřednictvím výše uvedené platební karty nebo karet za zboží či služby.
(According to my request, I wish to pay the ordered goods/services with my credit card. All stated information above is correct and true.)

Datum objednávky
(Order date)

Vlastnoruční podpis držitele karty
(Signature of authorised cardholder)

Odesláním formuláře beru na vědomí, že banka bude zpracovávat osobní údaje v něm vyplněné z titulu nezbytnosti pro plnění smlouvy mezi bankou a smluvním partnerem za účelem naplnění práv a povinností touto smlouvou dohodnutých.
By submitting the form, I acknowledge and am aware that the Bank's processing of my personal data entered in the form is necessary for the performance of the contract by and between the Bank and the Contracting partner for the purposes of the rights and obligations agreed under this contract.

Kontrolní kód z platební karty (Last three digits printed on the signature panel of the card):

MASTERCARD/CVC2 – Card Validation Code 2

VISA/CVV2 – Card Verification Value 2

Po provedení autorizace a před archivací objednávky odstřihněte kontrolní kód.
(Please cut off the control code after authorisation before archiving the document)

UniCredit Bank Czech Republic and Slovakia, a.s. I Sídlo / Registered Office: Želetavská 1525/1, 140 92 Praha 4 – Michle, www.unicreditbank.cz
IČO / Identification Number: 64948242 I Obchodní rejstřík / Commercial Register: Městský soud v Praze, oddíl B, vložka 3608 / Municipal Court in Prague, Section B, file 3608 I Směrový kód banky / Bank Code: 2700 I Swift Code: BACXCZPP

UniCredit Bank

POTVRZENÍ O PŘEVZETÍ NALEZENÉ PLATEBNÍ KARTY VISA / MC

FOUND CARD RECEIPT CONFIRMATION

Číslo karty
(Card number)

Platnost karty
(Card expiry)

Datum nalezení karty
(Date card found)

Jméno obchodníka
(Merchant name)

Číslo smlouvy o přijímání PK
(Merchant number)

Jméno nálezce
(Finder's name)

Telefon
(Phone number)

Datum převzetí
(Date of receipt)

.....
Jméno a podpis pracovníka
(Name and signature of employee)

.....
Jméno a podpis nálezce karty
(Name and signature of finder)

Tuto část vyplňuje pracovník oddělení vypořádání kartových obchodů UniCredit Bank Czech Republic and Slovakia, a.s.

Manipulační poplatek v USD

Natipován dne

.....
Jméno pracovníka, podpis

Odesláním formuláře beru na vědomí, že banka bude zpracovávat osobní údaje v něm vyplněné z titulu nezbytnosti pro plnění smlouvy mezi bankou a smluvním partnerem za účelem naplnění práv a povinností touto smlouvou dohodnutých.
By submitting the form, I acknowledge and am aware that the Bank's processing of my personal data entered in the form is necessary for the performance of the contract by and between the Bank and the Contracting partner for the purposes of the rights and obligations agreed under this contract.

UniCredit Bank Czech Republic and Slovakia, a.s. I Sídlo / Registered Office: Želetavská 1525/1, 140 92 Praha 4 – Michle, www.unicreditbank.cz
IČO / Identification Number: 64948242 I Obchodní rejstřík / Commercial Register: Městský soud v Praze, oddíl B, vložka 3608 / Municipal Court in Prague, Section B, file 3608 I Směrový kód banky / Bank Code: 2700 I Swift Code: BACXCZPP

ANNEX NO. 4

UniCredit Bank

ŽÁDOST O REKLAMACI
CLAIM REQUEST

E-mail: obchodnici.reklamace@unicreditgroup.cz

Číslo smlouvy o přijímání PK (Merchant number)	
Telefon (Phone No.)	
Jméno a podpis žadatele (Applicant's name and signature)	
Číslo terminálu (Terminal No.)	
Datum transakce (Transaction date)	
Částka transakce (Transaction amount)	
Číslo karty (Card No.)	
Platnost (Card expiry)	

Doúčtování rozdílu transakce (Increase transaction amount) ☐
SPRÁVNÁ ČÁSTKA (Correct amount)
ČÁSTKA ROZDÍLU (Difference)

Odúčtování rozdílu transakce (Decrease transaction amount) ☐
SPRÁVNÁ ČÁSTKA (Correct amount)
ČÁSTKA ROZDÍLU (Difference)

Storno transakce (Cancel of transaction) ☐

Doúčtování transakce (Manually input transaction) ☐

Jiná žádost (Other request)

Popis (Description):

Spolu se žádostí o reklamaci je nutné zaslat (Please enclose the following documents):
- **kopii účtenky z platebního terminálu** (POS sales slip copy)
- **kopii pokladní účtenky** (ECR sales slip copy)

Odesláním formuláře beru na vědomí, že banka bude zpracovávat osobní údaje v něm vyplněné z titulu nezbytnosti pro plnění smlouvy mezi bankou a smluvním partnerem za účelem naplnění práv a povinností touto smlouvou dohodnutých.
By submitting the form, I acknowledge and am aware that the data entered in the form and the Bank's processing of my personal data is required for the performance of the contract by and between the Bank and the Contracting partner for the purposes of the rights and obligations agreed under this contract.