

# **PAYMENT CARDS OF PPF banka a.s.**

## **Guide for Using Payment Cards for Online Payments**

## Contents:

1. General information .....	3
2. Using Cards for online payments .....	3
3. 3D Secure.....	4
3.1. What is 3D Secure.....	4
3.2. Advantages of 3D Secure.....	4
3.3. 3D Secure payment procedure.....	4
3.4. Setting up 3D Secure for Cards issued by the Bank .....	5
3.5. Using cookies with 3D Secure.....	5
4. Details of Card settings, including permission for E-commerce Transactions and contact details for 3D Secure and how to make changes .....	6
4.1. Display and changes via Internetbanking.....	7
4.2. Display and changes through Homebanking.....	7
5. Procedure of E-commerce Transactions with 3D Secure .....	8

## 1. General information

The conditions for using payment cards ("Card") are set out in the *Business Conditions of PPF banka a.s., for Payment Cards* ("SBC"), in Card contract documents, in the *General Business Conditions of PPF banka a.s.*, ("GBC") and in this Guide.

Expressions, abbreviations or phrases beginning with capital letters have meaning stated in the GBC, SBC, or this Guide. The current version of the Guide is available at [www.ppfbanka.cz](http://www.ppfbanka.cz).

Support for Cards is provided by Customer Service, which can be contacted on Business Days during Business Hours from 8 a.m. to 6 p.m. at +420 224 175 902 or at [customer.service@ppfbanka.cz](mailto:customer.service@ppfbanka.cz). Customer service will handle questions sent via e-mail and outside the above hours, during Business Hours on the following Business Day.

## 2. Using Cards for online payments

E-commerce Transactions, a feature enabling Cards to be used for online payments to the Merchants who accept this payment method, can be allowed on each Card issued by the Bank. The payment is executed as a payment without the physical presence of the Card.

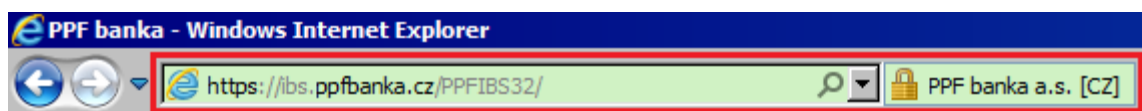
The Merchant may request the following details for E-commerce Transactions:

- Card number and validity;
- The card association that has issued the Card; in the case of PPF banka a.s., it is MasterCard;
- Name of the Card Holder;
- The CVC/CVC2 code (Card Verification Code): a three-digit security code on the back of a Card (may also be called CVV/CVV2); **do not disclose your PIN to the Merchant under any circumstances; the PIN is not a security code.**

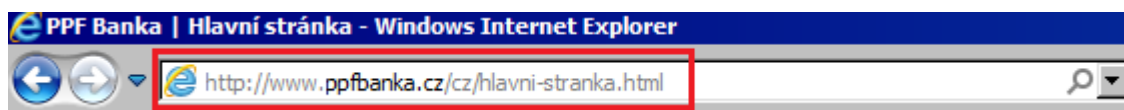
**By submitting the requested details through the Merchant's website or through another channel (fax, e-mail etc.), you have authorised the Payment Transaction in question. It cannot be revoked thereafter.**

Various e-Merchants use different security systems for E-commerce Transactions:

- **3D Secure:** You are not providing your Card details to the Merchant but to a 'payment gateway'. Only providers certified by Card associations (MasterCard and VISA), who are audited on a regular basis for compliance with the security rules for data protection, may operate payment gateways.
- **The SSL (Secure Sockets Layer) / TLS (Transport Layer Security) protocol:** Communication between the Merchant and the Holder is encrypted with the help of security certificates, and so protected against wiretapping, falsifying and forging. The addresses of secured websites begin with **https://**.



- **Unsecured Merchant:** You provide the Merchant with all your Card details in an unsecured form (addresses of unsecured websites begin with **http://**) and the Merchant can use them at any time. Any third party who 'wiretaps' them on the internet can abuse them.



If you want to use your Card for online payments then choose Merchants who support the secured transmission of Card details. In the event of any doubt about the Merchant's credibility we recommend opting for a different method of payment.

**We recommend that you refrain from shopping at unsecured Merchants.**

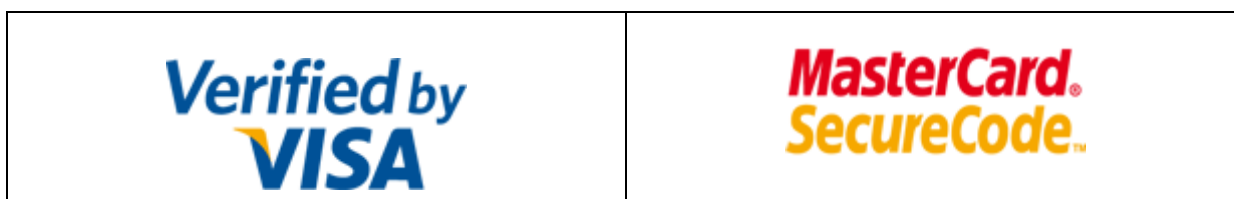
## 3. 3D Secure

### 3.1. What is 3D Secure

3D Secure is an international standard for improving the security of E-commerce Transactions. It is a Card security method that protects Holders and their data against the execution of unauthorised Payment Transactions when paying over the Internet to a Merchant supporting the 3D Secure service.

Card details are not provided directly to the Merchant but are transmitted to a payment gateway, wherein they are encrypted and transmitted for verification directly to the bank that has issued the Card; the Merchant will therefore not receive the Card details and cannot abuse them.

Websites of Merchants using 3D Secure bear the “MasterCard Secure Code” or “Verified by Visa” logo.



### 3.2. Advantages of 3D Secure

- You confirm the payment by a unique authorisation code that you receive via a text message at the mobile phone number you have provided, or via a message to an e-mail address.
- You do not have to remember any password; you will receive a new authorisation code for every payment.
- This service is completely free of charge, including the sending of the text or e-mail messages with the authorisation code.
- An overwhelming majority of e-shops in the Czech Republic and Europe already support this security standard.
- If you shop at a 3D Secure Merchant, you eliminate the risk of your sensitive Card details leaking from the Merchant, which may result in a potential abuse of your Card by an unauthorised person. You do not submit your Card details on the Merchant’s website but through a secured payment gateway that is better protected against data leakage.

### 3.3. 3D Secure payment procedure

- **At the e-shop, you select the goods or service, opt for Card payment, and confirm your purchase order.**
- **You enter the Card details into a form on the payment gateway.**
- The Card details are then encrypted and via a secure connection, transmitted directly between the shopper and the payment gateway.
- The request is then verified with the bank.
- If the execution of E-commerce Transactions is allowed on the Card, you will receive a single-use authorisation code with which you confirm and complete the E-commerce Transaction.
- The bank then authorises the E-commerce Transaction and transmits this information back to the payment gateway, which sends a message to the Merchant that the payment has been authorised.
- This process is very quick and usually only takes a few seconds.

- In the case of recurring payments (eg. regular payment of subscriptions, software licenses, etc.). Verification takes place through 3D Secure only once – when carrying out the first transaction. Subsequent payments already do not require authentication.

Situation is the same for recurring payments entered before the introduction of 3D Secure – performs continue without verification.

### 3.4. Setting up 3D Secure for Cards issued by the Bank

Using 3D Secure is mandatory for all Holders.

This means in practice that for executing E-commerce Transactions with Merchants who use 3D Secure, the Card Holder must provide the Bank with the mobile phone number or e-mail address to which single-use authorisation codes will be sent to the Holder. **If a Holder does not provide the Bank with a mobile phone number or an e-mail address, they will not be able to pay at such Merchants.** If Holders provide both of these contact details, they will then be able to select the method by which the single-use authorisation code is to be sent to them when paying.

Where e-Merchants do not support 3D Secure, it will still be possible to pay for the purchase using the Card even without confirmation by a single-use authorisation code. **However, we do not recommend shopping at such Merchants** (see point 2. above).

### 3.5. Using cookies with 3D Secure

If the E-commerce transaction is authorized through 3D Secure, The Supplier of this service uses so called cookies. Holder is aware of this fact at the bottom of the 3D Secure authentication home page, where he/she can also see the details.

**PPF** Banka **MasterCard**  
SecureCode.

**Choose a delivery method** CZ ENG

Choose a method of authorization code delivery.

**To a mobile phone** Send as an SMS

**To an e-mail** Send to an e-mail

In case of need, contact your relationship manager or Customer Service, tel. (+420) 224 175 902, e-mail customer.service@ppfbanka.cz.

[Help](#) | [Close](#) Powered by Global Payments Europe

This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. [Find out more here.](#) ✕

**Cookies are used exclusively by the Supplier who is fully responsible for processing the data thus obtained, the Supplier contact is given in the information on the use of cookies available in the link in the notification. Bank does not use or does not process cookies when paying by card on the Internet.**



## COOKIES INFORMATION

Dear User,

Upon and subject to the relevant legislation we hereby informed you that this website use the cookies, namely "session cookies", which are essential to the functionality of the website for providing the service which you have requested or to transmit messages. Session cookies while using web services cannot be excluded.

Others cookies are used in your browser and help to deliver a better and more personalized service e.g. by remembering certain choices you've made so you don't have to re-enter them (e.g. choice of preferred language).

You can prevent the installation of the cookies by selecting the appropriate settings on your browser. If you do so, you may not be able to access or to take full advantage of all our website services.

Global Payments Europe, s.r.o., with registered office at V Olšínách 626/80, Strašnice, 100 00 Prague 10, Czech Republic, business identification number: 27088936, registered with the Commercial Register administered by the Municipal Court in Prague, Section C, Insert 95419  
[www.globalpaymentsinc.com](http://www.globalpaymentsinc.com)

## 4. Details of Card settings, including permission for E-commerce Transactions and contact details for 3D Secure and how to make changes

You can find whether E-commerce Transactions are allowed or prohibited on a Card in Internetbanking ("IB") or Homebanking ("HB"), including the contact details (i.e. the mobile phone number and, if applicable, the e-mail address) provided by the Holder for receiving the authorisation codes for the 3D Secure verification of E-commerce Transactions (see below).

**Contact details always relate to the Holder (a natural person) and apply to all of that person's Cards regardless of the Payment Accounts with which a Card has been issued. Thus, Cards can be issued with Payment Accounts of different companies or even natural persons; however, for the Holder, the same contact details will always apply. It is not possible for one Holder to set up different contact details for their various Cards.**

Only the Client can allow E-commerce Transactions on a Card, either in person at the Bank's Place of Business or over the telephone through their relationship manager.

The setting up and/or the change of a Holder's contact details can be requested in person at the Bank's Place of Business or through IB and HB. **If a Holder has not yet provided the Bank with a certain type of contact detail, they must also sign their consent to personal data processing.**

**The setting up and/or the change of contact details for receiving the authorisation codes for 3D Secure will only be effective from the following Business Day.**

## 4.1. Display and changes via Internetbanking

You can check the permission for E-commerce Transactions and the contact details (the mobile phone number and, if applicable, the e-mail address) for a Holder in IB in the Payment Card Details, the **Payment Cards** option (see the [User Guide for Internetbanking Services](#), Part II, point 3.1.).

### Payment Card Detail

Card Limit	Limit Amount	Drawing of Limit
ATM Limit	50.000,00 CZK	0,00 CZK
POS Limit	50.000,00 CZK	0,00 CZK
<b>Total Weekly Limit</b>	<b>100.000,00 CZK</b>	<b>0,00 CZK</b>

---

Card number:	5458 54xx xxxx 5136
Card type:	MasterCard Embossed Card
Card Holder:	PANKRÁC ÚTERNÍ
Card valid from:	1/2016
Card valid to:	1/2019
Card status:	Active
Card Insurance:	
Travel Insurance:	QUALITY
E-commerce Transactions:	Allowed
Mobile phone number:	42072xxxxx43
Email:	PU****@EMAIL.CZ
Contactless Transaction:	Allowed
Displaying CA balance via ATM:	Allowed
Card Automatic Renewal:	Set
Main CA number:	000000.80016
Main CA currency:	CZK
Associated CA number:	000000.80024
Associated CA currency:	EUR

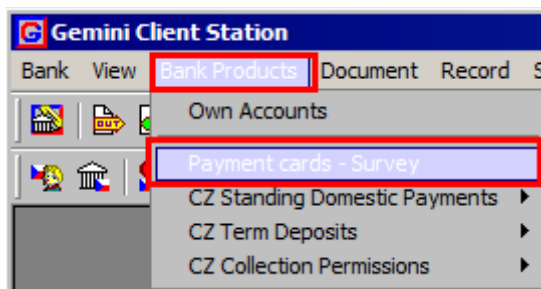
Settled Transactions
Card Transactions
Unsuccessful Transactions

Back
Print

Contact details for 3D Secure can be changed directly through IB, either by a request in the **User** option (see [User Guide for Internetbanking Services](#), Part III, point 4.1.4.), or by an unformatted message with the full identification of the Holder whose contact details are to be changed (see [User Guide for Internetbanking Services](#), Part III, point 2.2.).

## 4.2. Display and changes through Homebanking

You can check the permission for E-commerce Transactions and the contact details (the mobile phone number and, if applicable, the e-mail address) for a Holder in HB in Payment Card Details, the **Bank Products** and **Payment Cards – Survey** option.



In the Card overview, you will find the required details in the columns **E-commerce TRN**, **Mobile phone number** and **E-mail**.

Bank	Card number	Card Holder	Card type	Card vali...	Card ...	Main CA	Main CA cur.	As...	C...	E-commen...	Mobile phone number	Email
PMBA	558387xxxx...	PANKRAC UTERNI	MasterCard ...	6/2013	6/2016	000000 ...	CZK			<input checked="" type="checkbox"/>	42099xxxxx99	ML****@PPF.EU

Contact details for 3D Secure can be changed directly through HB by an unformatted message with the full identification of the Holder whose contact details are to be changed (you can find the procedure in the User Guide that is part of the HB installation diskette).







## 5. Procedure of E-commerce Transactions with 3D Secure

In the e-shop, select the Card payment method with the MasterCard logo.



You will then be redirected to the payment gateway, in which you enter the Card details. Different payment gateways may require different details, but at least the Card number, the expiry date of the Card and the CVC/CVC2 code must be entered at all times.

For sending the payment for 3D Secure verification, click the **Pay** or similar button.

Summary of your order	Safe card payment	Mobile payment
<p><b>Vendor:</b> Internet Mall, a.s. Delnicka 213/12 170 00 - Praha (CZ) <a href="http://www.mall.cz">www.mall.cz</a></p> <p><b>Order number:</b> 478816054</p> <p><b>Total:</b> <b>276,00 CZK</b></p> <p><b>MasterCard SecureCode</b> Verified by <b>VISA</b></p>	<p>You can pay by card:</p> <p>      </p> <p>Does your card permit online payment?</p> <p>Your card number: <input type="text" value="1234567890012345"/></p> <p>Card valid till: <input type="text" value="01"/> / <input type="text" value="14"/></p> <p>Verification code: <input type="text" value="111"/> also CVC2 / CVV2 <a href="#">Where is it?</a></p> <p><b>Pay 276,00 CZK</b></p>	<p>  </p> <p>You can now pay safely using MasterCard® Mobile</p>

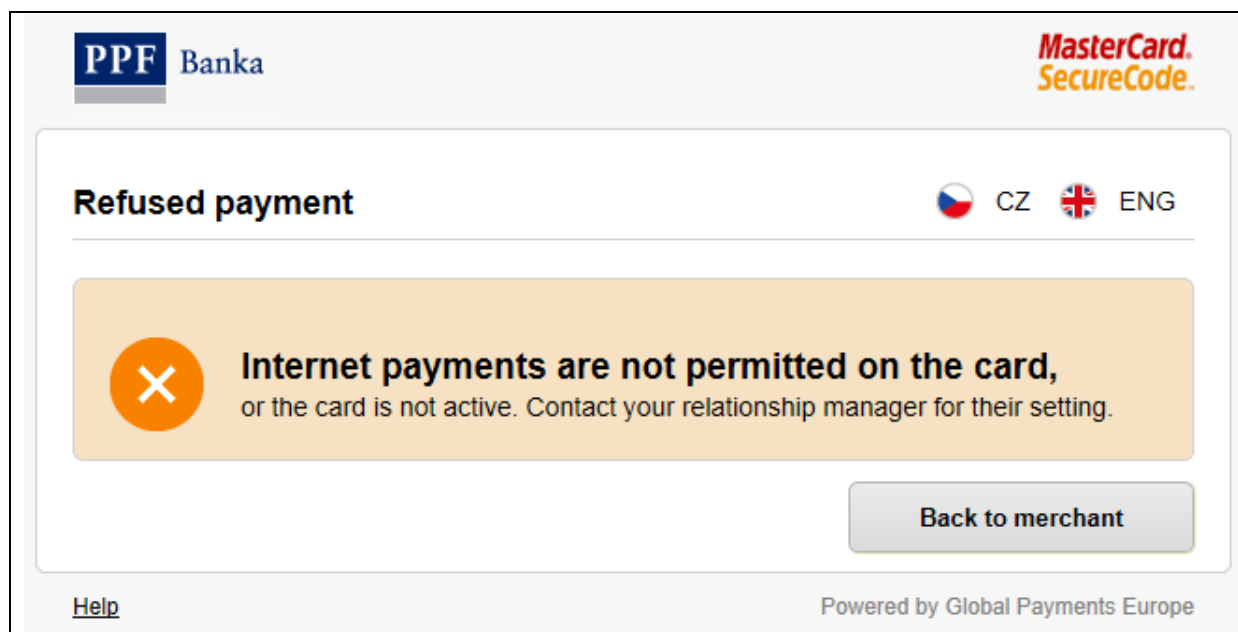


Options for the method of authorisation code delivery will be displayed – click on the relevant button for the transmission of the code.

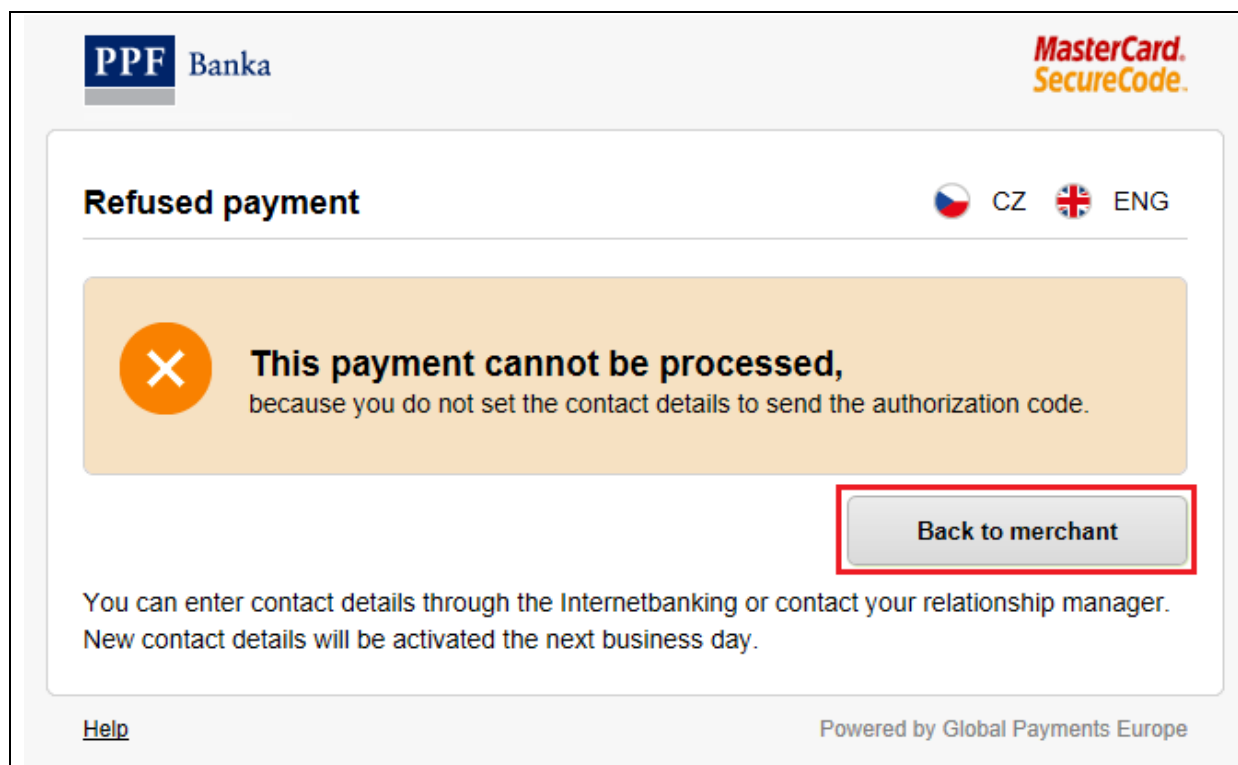
In the upper right-hand corner of the screen, you can also change the language in which payment authorisation will take place, either in Czech or in English. You can make this change on any screen and at any time during the entering of the authorisation code.

The screenshot displays the PPF Banka online payment interface. At the top left is the PPF Banka logo, and at the top right is the MasterCard SecureCode logo. The main heading is "Choose a delivery method". In the top right corner of this section, there is a language selection box with flags for CZ (Czech) and ENG (English). Below the heading, the instruction reads "Choose a method of authorization code delivery." There are two main options: "To a mobile phone" with a mobile phone icon and a "Send as an SMS" button, and "To an e-mail" with an envelope icon and a "Send to an e-mail" button. At the bottom, there is contact information for customer service and a "Powered by Global Payments Europe" notice.

If E-commerce Transactions are not allowed on the Card, the payment is rejected and the following warning is displayed:



If E-commerce Transactions are allowed on the Card but you have not provided the Bank with a mobile phone number, the payment is rejected and the following warning is displayed.



If E-commerce Transactions are allowed on the Card and you have provided the Bank with a mobile phone number or an e-mail address, the screen for entering the authorisation code is then displayed.

On the left-hand side of the screen, a payment summary is displayed: the name of the Merchant, the amount, the date on which the payment was made and the encrypted Card number.

Once you receive the authorisation code, enter it in the relevant field (1.) on the right-hand side of the screen and click **Confirm** (2.).

You can have the authorisation code sent to you again (3.) and if you have also provided the Bank with an e-mail address, you can also select again the method of authorisation code delivery (4.).

**You must enter the authorisation code and complete the E-commerce Transaction by the end of the time limit for code entry (approximately 10 minutes).** If you do not enter the code within the time limit the E-commerce Transaction will be discontinued without payment. You must then repeat the payment to the Merchant.

The delivery of a text or e-mail message usually takes a few seconds, but sometimes it may take longer. If you haven't received the text or e-mail message after one minute then request a new authorisation code to be sent to you with the help of the link in the window for code entering (see above).

**PPF** Banka **MasterCard.**  
SecureCode.

**Payment verification** CZ ENG

**Please enter received authorization code for confirmation of the next payment:**

Merchant:	Zluty.cz	1.	2.
Amount:	40 CZK	333333	Confirm
Date:	03.11.2014		
Payment card:	**** * 5136		

**Send an authorization code again?** 3.

+42072\*\*\*\*743 Send again

4. Select again the method of sending



If the above mentioned contact details are not current, you can change them through the Internetbanking or contact your relationship manager. New contact details will be activated the next business day. This information is not shared with the merchant.



[Help](#) | [Close](#) Powered by Global Payments Europe

If you enter the authorisation code correctly the E-commerce Transaction will continue and the payment to the Merchant is completed.

If you enter the authorisation code incorrectly you can enter it again; in such a case, enter the authorisation code in the respective field (1.) on the right-hand side of the screen and click **Confirm** (2.).


In this case too you can have the authorisation code sent to you again and if you have provided the Bank with an e-mail address, you can also select again the method of authorisation code delivery (3.).

**Authorization code was entered incorrectly** 
 CZ  ENG

**Please enter received authorization code for confirmation of the next payment:**

Merchant:	Zluty.cz	1.	2.
Amount:	40 CZK	987456	Confirm
Date:	03.11.2014		
Payment card:	**** * 5136		



**Send an authorization code again?**  
+42072\*\*\*\*743

3.

Send again

Select again the method of sending



If the above mentioned contact details are not current, you can change them through the Internetbanking or contact your relationship manager. New contact details will be activated the next business day. This information is not shared with the merchant.


[Help](#) | [Close](#)
Powered by Global Payments Europe

Should you enter the authorisation code incorrectly five times the E-commerce Transaction is discontinued without payment and at the same time, Card payment over the internet is disabled.

E-commerce Transactions will only be enabled again on the following Business Day.

**PPF** Banka **MasterCard.**  
**SecureCode.**

**Refused payment**  CZ  ENG



**The payment was refused,**  
because you have exhausted the allowed number of attempts to enter the authorization code.

[Back to merchant](#)

For security reasons, all attempts of paying with a payment card on the internet will be rejected today. Possibility of payment will be restored the next day.

In case of need, contact your relationship manager or Customer Service:  
tel. (+420) 224 175 902, e-mail [customer.service@ppfbanka.cz](mailto:customer.service@ppfbanka.cz)

[Help](#)

Powered by Global Payments Europe

If you need to, you can display Help by clicking the button on the bottom left-hand corner of every screen. Help will open in a new window, which you can then close by clicking on the “x” in the upper right-hand corner.

PPF Banka | Handbooks and Ma... acs.gpesecure.com Help

**PPF** Banka **MasterCard. SecureCode.**

## Help

- We have increased security when paying by card online.
- When paying by card you will receive an authorization code by which you confirm the payment on the internet.
- You may choose method of sending the authorization code: the cell phone or e-mail.
- The authorization code can be sent repeatedly by chosen method, or you can choose other method of its delivery.
- Resending and incorrect entry of an authorization code is limited to 5 attempts. For security reasons, card will be blocked for such a secure internet payment after depletion of these attempts until the end of the day. Possibility of payment will be restored the next day.
- Entering or change of contact details for sending an authorization code will be valid from the next business day.
- In case of need, contact your relationship manager or Customer Service, tel. (+420) 224 175 902, e-mail [customer.service@ppfbanka.cz](mailto:customer.service@ppfbanka.cz).