

MEMO  
"ON MEASURES FOR THE SAFE USE OF BANK CARDS  
WHEN PERFORMING TRANSACTIONS VIA THE INTERNET"

Compliance with the recommendations contained in this Memo will ensure the maximum safety of the bank card, its details, PIN code and other data, as well as reduce possible risks when performing transactions using a bank card via the Internet.

Never under any circumstances transfer your bank card for use to third parties, including relatives. If the name and surname of an individual are marked on the bank card, then only this individual has the right to use the bank card. Do not listen to the advice of third parties, and do not accept their help when conducting transactions with a bank card.

Phone credit organization - Issuer of a Bank card (the credit institution that issued the Bank card) listed on the reverse side of your card. You must also always have the contact phone numbers of the credit institution that issued the bank card and the bank card number on other media: in your notebook, mobile phone and/or other media, but not next to the PIN code entry, CVV/CVC.

For the purpose of information interaction with the credit institution issuing the bank card (the credit institution that issued the bank card), it is recommended to use only the details of the means of communication (mobile and landline phones, fax machines, interactive web sites/portals, regular and e-mail, etc.), which are specified in the documents received directly from the credit institution issuing the bank card.

Please note that in case of disclosure of the PIN code, CVV/CVC, personal data, loss of the bank card, there is a risk of illegal actions with the funds in your bank account by third parties. In order to prevent such illegal actions, it is recommended to use a separate bank card (the so-called virtual card) with a maximum limit, intended only for this purpose, for conducting transactions on the Internet.

If there are assumptions about the disclosure of the PIN code, CVV/CVC, personal data that allows you to commit illegal actions with your bank account, as well as if the bank card was lost, you must immediately contact the credit institution that issued the bank card (the credit institution that issued the bank card) and follow the instructions of an employee of this credit institution. Until the moment of contacting the credit institution that issues the bank card, you bear the risk associated with unauthorized debiting of funds from your bank account. As a rule, according to the terms of the agreement with the credit institution issuing the bank card, funds debited from your bank account as a result of unauthorized use of your bank card before the notification of the credit institution issuing the bank card are not refunded.

The use of a bank card on the Internet is associated with increased risks, including, but not excluding: with the risk of financial loss; the risk of duplication technical device; the risk of changes messages; risk of loss (theft) access codes passwords; the risk of failure of operations; the risk of conflict situations beyond the control of the credit institution; the risk of write-off of funds from the payer's card in case of transfer of access codes and passwords to another person; the risks of using electronic means of payment to third persons, without the permission of the payer; with the risk of interception by third parties in the communication channels during their use of information about access codes and passwords, information about the payer, information about transactions carried out, information about payment recipients, as well as other information about the payer.

When conducting transactions over the Internet, make sure that the address of the website you are connecting to is correct, because similar addresses can be used for illegal actions. Carefully check the browser's address bar - the site name should be written without errors, the address should start with HTTPS (<https://paysend.com/>).

It is recommended to make transfers only from your computer in order to preserve the confidentiality of personal data and / or information about the bank card (s) (account). If the transfer is made using someone else's computer, it is not recommended to save personal data and other information on it, and after completing all operations, you need to make sure that the personal data and other information are not saved (by reloading the web page in the browser <https://paysend.com/>).

Install antivirus software on your computer and regularly update it and update other software products you use (the operating system and application programs), this can protect you from the penetration of malicious software.