

## THE NATIONAL BANK OF UKRAINE

### **RECOMMENDATIONS for payment cards holders as regards their (cards) usage**

Compliance with these recommendations will give possibility to ensure payment cards holders their reliable storage, non-disclosure of the details of payment card, personal identification number (hereinafter referred to as PIN) and other data, and also will decrease possible risks while operation performance using payment card in ATMs, funds transfer for goods and services payment, and through Internet as well.

Recommendations are valid in the part that do not contradict rules of usage of payment card of corresponding payment system (in case of its submittal by issuer to holder).

These recommendations do not apply to payment cards of the National system of mass electronic payments.

#### **General recommendations**

1. Never disclose PIN to strangers, including relatives, acquainted, employees of the bank, cashiers and persons trying to help you while payment card using.

2. PIN should be remembered or kept separately from payment card in inaccessible for strangers, including relatives, place.

3. Never give payment card for usage by other persons, including relatives. If surname and name of individual are marked on payment card, i.e. only this individual is entitled to use payment card.

4. Do not disclose and do not inform personal data or information on payment card (including PIN) on demand of any strangers, including employees of the bank. In case of such a situation occurrence, you should call to issuing bank and notify about this fact.

5. While payment card receiving, put signature on its reverse side in the space determined for signature of payment card holder. It will decrease risk of payment card usage without your consent in case of its loss.

6. Be attentive to conditions of storage and usage of payment card. Do not expose payment card to mechanical, temperature and electromagnetic actions, and prevent it from ingress of moisture. Payment card can not be stored together with mobile phone, household and office equipment, as well as near metal objects and other magnetic carriers/devices.

7. Phone of issuing bank that issued payment card is indicated on reverse side of payment card. It is also necessary to always have contacts of issuing bank, number of payment card on other information carriers: in notebook, mobile phone etc., but not together with the PIN record.

8. To prevent illegal operations using payment card and funds withdrawal from your card account it is reasonable to set daily limit to the amount and number of operations using payment card and simultaneously connect electronic service of notification on performed operations (for example, notifications as short messages to mobile phones (SMS) or by other way).

9. It is not recommended to answer to electronic letters where it is proposed to provide personal data. It is not necessary to open pages in Internet (sites/portals), indicated in the letters (including official page of the Bank in Internet), as it can be lookalike pages, through which illegal actions/doubtful operations using data of your payment card can be performed.

10. With the aim of information interaction with issuing bank it is recommended to use only details of communication facilities (mobile, fixed phones, fax, interactive pages in the Internet (sites/portals), ordinary and e-mail etc.), which are indicated in the documents received directly in the issuing bank.

11. Bear in mind that in case of PIN, personal data disclosure, loss of payment card there is a risk of performance of illegal actions with funds on your account by the third parties.

In case of payment card loss, the holder should immediately inform the issuer about it. In other case, the issuer bears no responsibility for funds transfer initiated before receiving of such a notice by means of this payment card if otherwise is not stipulated by the agreement.

#### **Performance of operations through ATM**

1. We recommend you to perform operations on usage of payment cards through ATMs installed in safe places (for example, in institutions, banks, big shopping malls, hotels, airports etc.)
2. Do not use devices requiring PIN entering for access to the place where ATMs are located.
3. Before ATMs using, examine it as regards availability of additional devices that do not comply with the construction and located in place of PIN entering, and in place (slot), determined for cards acceptance (for example, if keyboard for PIN entering is installed unevenly). Do not use such an ATM in case of the aforesaid revealing.
4. If keyboard or place for card acceptance of the ATM are equipped by additional devices that do not comply with its construction, do not use it for operations performance with payment card usage and notify the Bank about it by phone indicated on the ATM.
5. Do not use manual power to insert payment card into the slot determined for cards acceptance. If payment card is not inserted easily, do not use such an ATM.
6. Enter PIN in such a way so that persons being nearby could not see it. While PIN entering cover the keyboard with your hand.
7. If ATM works incorrectly (for example, being in waiting mode for a long time, unintentionally rebooting), refuse from the services of such an ATM, cancel current operation, pushing the button "Cancel" on the keyboard and wait for payment card return.
8. After cash receiving in the ATM it is necessary to count it and make sure that payment card was returned by the ATM, wait for cheque in case of its request and only after this go away from the ATM.
9. Printed cheques from the ATM should be stored for reconciliation of the indicated amounts with statement on cash flow on card account.
10. It is not required to take any actions using hints of the third parties, and also do not accept their help while operation performing through ATM using payment card.
11. If while operation performing through ATM, payment card was not returned, it is necessary to call to the Bank by phone indicated on the ATM, and describe the situation occurred, and apply to the issuing bank that gave this payment card due to this reason.

### **Bank transfer of funds**

1. Do not use payment card in trading network to pay for goods and services, if you have some doubts as regards merchant/seller/cashier (in restaurant, shop, refuelling station etc.).
2. Settlements with payment card usage have to be performed only in your presence. It will ensure minimization of risk of illegal receiving of your personal data indicated on payment card.
3. While payment card using to pay for goods and services seller/cashier can require from payment card holder passport, sign receipt or enter PIN. Before PIN entering it is necessary to make sure that the third parties being in immediate proximity to you will not be able to see it. Before receipt signing, it is necessary to check obligatory the amount indicated on it.
4. If the operation on goods and services payment with payment card usage failed, it is necessary to store one copy of the issued by terminal receipt to check absence of the indicated operation in cash flow statement.

### **Operations performance through Internet**

1. Do not use PIN while goods and services ordering via Internet, as well as by phone/fax.
  2. Do not provide the information on payment card or card account through Internet, for example, PIN, passwords of access to the accounts, payment card validity, credit limit, personal data etc.
  3. To avoid illegal actions or doubtful operations using data of payment card of the international payment system it is recommended for payment for goods (services) via Internet to use separate payment card (so-called "virtual card") with boundary limit, that is stipulated only for this target and which does not give possibility to perform operations in trading network and cash withdrawal with its usage.
  4. It is necessary to use pages in Internet (sites/portals) of only famous and checked Internet shops.
  5. Please, make sure in correctness of the pages addresses in Internet (sites/portals), to which you connect and through which you are going to perform payments for goods (services), as similar addresses can be used for performance of illegal actions or doubtful operations with payment card personal data usage.
  6. We recommend to perform payments for goods (services) purchased though Internet only from your computer not to disclose personal data and/or information on card account.
- If payment for goods (services) is made through somebody's computer, it is recommended after completion of all settlements to make sure that personal data and other information was not stored (by means of reopening of the page of seller on which payment for goods was performed).

7. It is necessary to install antivirus software to personal computer and perform its regular updating and updating of other software products (operating system, applications). It will protect you from unlicensed software (viruses) penetration.

### **Card account closing**

1. Bear in mind, that current/card accounts shall be closed under client's application, if otherwise is not stipulated by the agreement.

2. In case of quitting or early termination of agreement upon your initiative, if you are not going to use an account in future and if the Bank stipulated fee charge for its servicing, it is reasonable to close current/card account opened for you for salary receiving. Due to this reason you have to apply do the bank with application on account closing if otherwise is not stipulated by the agreement, and return payment card (if required), get cash flow statement as regards current account.

3. While card account closing (after fulfillment of obligations or in case of termination or expiry of agreement) the bank is obliged to issue funds balance (if any) and upon request of payment card holder – certificate on account closing and payment card return, loans and interest on it. Funds shall be issued by cash or upon client's request transferred to another account.