

Subject: “How to Use Safely a Bank Card” Checklist

As part of the work aimed at informing the general public of the risks associated with the use of bank cards and at enhancing its competence in financial matters the Bank of Russia has elaborated the Checklist for card holders in which it outlined measures that may help ensure a safe use of bank cards (hereinafter referred to as the Checklist).

The territorial branches of the Bank of Russia are invited to perform additional work with credit organizations with a view to enhancing information awareness of card holders. This work includes, inter alia, providing information on measures helping to ensure safety of bank cards, its requisites, personal identification numbers (hereinafter referred to as PIN) and other data as well as measures helping to mitigate risks that may arise in the process of performing card operations (transactions), or while paying for products and services with a card (including payments via Internet). It is also recommended that the territorial branches of the Bank of Russia place the Checklist (in a self-explanatory form) in all areas where card holders may be potentially served. The present Checklist of the Bank of Russia must be published in “The Bulletin of the Bank of Russia”.

Annex: Four (4) pages.

DEPUTY CHAIRPERSON OF THE BANK OF RUSSIA

T.N. CHUGUNOVA

“HOW TO USE A BANK CARD SAFELY” CHECKLIST

Compliance with the recommendations outlined in this Checklist will help you to ensure the maximum safety of your bank card, its requisites, PIN and other data and to mitigate the risks associated with the performance of card operations (transactions) in ATMs as well as risks arising in the process of paying for products and services by card (including via Internet).

General Recommendations

1. Never tell PIN to third persons including relatives, friends, bank employees, cashiers or persons helping you to use a card.
 2. Bear in mind PIN or (if it seems difficult for you) keep it separately from your card in a disguised form and in a place which is inaccessible for third persons including relatives.
 3. Under no circumstances should you give your card for a use by third persons including relatives. Only a person whose first and last names are mentioned on a card is authorized to use it.
 4. Upon receipt of a card sign it on its reverse side in a sector reserved for a signature of card holder (if available). This will mitigate the risk of unauthorized use of a card in case of its loss.
 5. Check how your card is stored and used. Don't expose your card to mechanical, thermal and electromagnetic influence, avoid any moisture. Don't keep your card next to mobile phones, household and office appliances.
 6. The phone number of a credit organization that has issued a card is indicated on its reverse side. A card holder must always keep contact phone numbers of a credit organization (a card issuer) as well as card number on other information carriers: in his/her notebook, mobile phone and/or other carriers but never next to a record containing a PIN.
 7. In order to prevent unlawful withdrawals of funds from a bank account it is appropriate to establish a maximum daily amount reserved for card operations and simultaneously to activate electronic alerting service which informs a card holder of all performed operations (transactions), i.e., via SMS or otherwise.
 8. Upon receiving a respective request (including the same from a staff member of a credit organization) never communicate your personal data or information on a bank card (including a PIN). Call back to a credit organization (issuer of a card) and tell about this request.
 9. It is not recommended to answer e-mails requesting, on behalf of a credit organization (card issuer), to provide your personal data. Don't use URLs mentioned in such emails (including URLs of the Internet Site of a credit organization) as they may navigate you to “fishing sites”.
 10. With a view to establishing information interoperability with a credit organization (card issuer) it is recommended to use only the requisites of communication facilities (mobile and fixed phones, faxes, interactive web-sites/portals, traditional and electronic mail, etc) mentioned in the documents that have been received directly from a credit organization (issuer of a card).
 11. Remember that disclosure of PIN, personal data or loss of a card may result in the performance, by third persons, of unlawful operations with funds placed on your bank account.
- If there is any suspicion that your PIN or personal data have been disclosed (which permits to perform unlawful operations with your bank account), or if your card has been lost you must immediately contact a credit organization (card issuer) and follow the instructions of its staff member. Before you contact a credit organization (card issuer) you bear in full the risk associated with unauthorized withdrawal of funds from your bank account. As it is normally prescribed in agreements with credit organizations (card issuers) the amount debited from your bank account as a result of unauthorized use of your bank card prior to the respective notification of a credit organization (card issuer) may not be reimbursed to a card holder.

Recommendations to be observed by a card holder in the process of performing card operations in ATMs

1. Always use ATMs which are installed in safe public areas (for example, government and municipal organizations, bank branches, trade centers, hotels, airports etc).
2. Don't use any devices requesting PIN to allow you inside a premise where ATM is installed.
3. If you see any third persons in close proximity to ATM you should choose a more convenient time to use it or find another ATM.
4. Before using ATM you must check if any additional device mismatching ATM's normal design is installed close to a PIN keyboard or slot for card processing (for example, you detect a PIN keyboard which is not correctly installed on ATM). In this case don't use such ATM.
5. If you see that ATM's PIN keyboard or slot for card processing is equipped with any additional devices mismatching ATM's normal design don't use your card in this ATM and tell about your suspicion to the staff members of a credit organization by phone using a phone number indicated on ATM.
6. Don't use any force to insert a card in a slot. If a card cannot be inserted in ATM don't use such ATM.
7. Before entering PIN make sure that people who are in close proximity to ATM cannot see it. When entering PIN always cover a keyboard with your hands.

8. If ATM functions incorrectly (i.e., ATM works in a standby mode for a long period of time or reboots spontaneously) don't use this ATM, cancel a current operation by pressing "Cancel" button and wait until ATM returns your card.
9. Upon receipt of cash in ATM count banknotes one after one, make sure that your card has been returned by ATM, wait until ATM issues a receipt form (if required), put them into your bag (purse, pocket) and only after that leave ATM location.
10. It is appropriate to preserve receipt forms which have been printed by ATM in order to further verify the amounts indicated with the amounts mentioned in the statement of your bank account.
11. Don't follow advice of any third persons and never accept their assistance while performing card operations in ATMs.
12. If in the process of performing a card operation ATM does not return your card you must contact immediately a credit organization using a phone number indicated on this ATM and explain the situation as well as contact a credit organization (card issuer) and follow the instructions of its staff member.

Recommendations to be observed while paying for products/services with a bank card

1. Don't use your card if you don't trust an organization where you buy product/services.
2. Request the performance of a card operation in your presence. That may substantially mitigate the risk of unlawful receipt of your personal data mentioned on your bank card.
3. While paying with your bank card for products/services a cashier may request a card holder to produce his/her passport, sign a receipt form or enter PIN. Before entering PIN make sure that people who are in close proximity to ATM cannot see it. Before signing a receipt form always check the indicated amount.
4. If "unsuccessful operation" occurs when you pay with a card for products/services you should preserve a copy of a receipt form issued by an ATM and then check whether such operation will be mentioned in the statement of your bank account.

Recommendations to be observed by a card holder while performing card operations in the Internet

1. Never use PIN while ordering products (services) via Internet or by phone/fax.
2. Never disclose personal data or card (account) information via Internet (i.e. PIN, passwords used in on-line applications of the Bank, term of validity of a card, credit limits, history of operations, personal data).
3. In order to prevent any unlawful withdrawal of funds from your bank account it is strongly recommended, while paying for products/services in the Internet, to use a separate bank card (so called "virtual card") which has a maximum limit of cash withdrawal and which may not be used while performing conventional payments in off line shops.
4. Use internet-sites of well established trade/service organizations only.
5. Always check the correctness of the internet addresses (URLs) of the organizations where you intend to buy products/services as similar URLs may be used for performing unlawful acts.
6. With the view to preserving confidentiality of personal data and/or card (account) information it is strongly recommended to use your PC only while buying products/services via Internet.
If a purchase of a product/service is performed via a foreign PC don't save any personal data and other information in it; upon completion of all operations make sure that personal data and other information have not been saved (by reloading the web-page of a seller via which a purchase has been effected).
7. Install antivirus software and regularly update it as well as other software used by you (i.e., operational system and applications); this measure may protect you against attacks of hostile software.