

CENTRAL BANK OF THE RUSSIAN FEDERATION

LETTER

No. 197-T of 7 December 2007

ON DISTANCE BANKING SERVICE RISKS

The Bank of Russia notes that the Russian segment of the Internet suffers from increased net attacks on websites and servers (hereinafter referred to as “Resources”) of credit institutions, as well as attempts to illegally acquire personal information of users of distance banking service (hereinafter referred to as “DBS”) (passwords, private keys of encryption tools and analogues of manual signature, PIN codes and numbers of bank cards, as well as personal information of their holders). Distributed denial-of-service attacks are among the most common. During such attacks a great number of computers (from a few hundreds to hundreds of thousands) with software specially modified by persons seeking to illegally acquire personal information of DBS users, at the command of such persons simultaneously start to send mass queries to the attacked resource, seriously disrupting or fully blocking its work. The resource’s owner, as a rule, cannot recover operation of the resource without the help of the Internet provider. Attacks can continue for several days making DBS unavailable to most clients of the credit organization, which may cause direct damage to such organization and its clients.

In view of the aforesaid the Bank of Russia considers expedient to advise credit institutions to include into agreements with the Internet providers obligations of parties to take measures in quick recovery of the resource operation in worst-case situations, as well as liability for undue fulfillment of such obligations.

In case of attempts to illegally acquire personal information of DBS users clients of credit organization receive e-mails offering on various pretexts (change of technical equipment, upgrade and verification of databases, etc.) to enter from the computer keyboard the said codes into fields of forms during emulated sessions of information interaction with a credit organization (e.g., through a duplicate of its website). At the same time malicious software can be transferred to the client’s computer from the website. Such software, i.e. viruses and “bookmarks”, runs in background mode and performs hidden functions connected with illegal acquisition of personal information of DBS users.

There are cases of illegal acquisition of bank card information during ATM transactions with the use of devices attached to PIN pads and Card readers, as well as "fake" ATMs installed in places beyond control by credit institutions and looking identical to ATMs used for DBS of credit organization clients.

Bank card information illegally acquired by various means is used to produce counterfeit bank cards partially (“white plastic”) or fully imitating the originals. When used in ATMs counterfeit bank cards provide their owners with all the functionality of original bank cards.

To illegally acquire personal information of DBS users interested persons also use different types of phone fraud. In particular, swindlers send SMSs to cell phones of clients of credit institutions prompting them to dial numbers that actually do not belong to such organizations. Clients also receive calls with messages from auto informers on the bank’s products and services offering to press keys on the phone to confirm their acquisition, etc. The bank's clients are thus provoked to enter into relations with swindlers aimed at acquisition of clients’ confidential information (e.g. bank card number and PIN code).

In view of the aforesaid the Bank of Russia would like to draw attention of credit institutions on importance of warning their clients by different means, including representative resources on the Internet (websites), on possible cases of illegal acquisition of personal information of DBS users. Information distributed as warning should include description of officially used ways and means of

information interaction with clients, as well as description of methods of illegal acquisition of clients' personal identification codes, information on bank cards and precautions DBS users should take. For example, credit institutions may recommend the following:

- to exclude possibility of illegal acquisition of personal information of DBS users (not to disclose it to unauthorized persons);
- to carry out transactions with the use of AMTs installed in safe places (in state institutions, bank offices, large shopping centers, hotels, airports, etc.);
- not to use banking cards in suspicious trade and service organizations;
- to keep an eye on the bank card during AMT transactions;
- not to use devices requiring entry of PIN code for access to the room with the ATM;
- not to use PIN code when ordering goods or services by telephone/fax or on the Internet;
- if the credit organization provides such possibility, to employ information of single-use cards ("virtual card") for payment of goods or services on the Internet;
- to use SMS notification on transactions carried out with DBS (if such service is available);
- to carry out information interaction with the credit organization only with the use of communication equipment (mobile and fixed phones, fax, interactive websites/portals, ordinary and electronic mail, etc.) mentioned in the documents received directly from the credit organization.

This letter is to be published in the "Bulletin of Banking Statistics".

Please, bring the information contained herein to the notice of credit institutions.

First Deputy Chairman
of the Bank of Russia
G.G.MELIKYAN