Customer memo
Terms for the use of electronic means of payment
by the users of 'Nordea Client- Bank (Internet)' and 'Nordea Client- Bank (Windows)'
System in JSC Nordea Bank.

Dear Customer!

We are glad to see you among our customers and thank you for choosing our services. The System "Bank - Client / Windows" and "Bank - Client / Internet" for Clients of JSC Nordea Bank - legal entities, individual entrepreneurs or individuals engaged in private practice according to legislation of the Russian Federation(hereinafter referred to as the "System"), offered by Nordea Bank, is a reliable way to exchange information between the customer and the Bank. The technology implemented by the Bank ensures protection of communication channels and information sent within the System from unauthorized access of third parties. However, in order to prevent possible fraud with your account, JSC Nordea Bank recommends you to observe the following rules when working in the System:

1. If possible, use the System only from your personal computer (hereinafter referred to as "PC"). If you log in with someone else's computer, do not save your personal data or other information on it. Remember that the risk of information theft and further unauthorized use of any authentication information increases in access to remote banking System from guest computers, for example, in an Internet cafe, hotel, etc.

2. Use the Licensed Software on the computer you are working in the System, upgrade the software, especially information security programs, in accordance with the manufacturer's recommendations;

3. Be sure to install and maintain updated anti-virus software on the PC you work in the System.

4. Do not store the electronic key "dongle" (USB-token) and password to the System at place accessible to unauthorized persons.

5. Never pass the electronic key "dongle" (USB-token) and password to unauthorized persons, including relatives, friends or employees of the credit institution.

6. Regularly, at least 1 time per three months, change the password for USB-token, and also password to access the System "Bank - Client / Windows".

7. Use the virtual keyboard when entering the PIN code to enhance the safety and security of access to the System from spy ware.

8. Change immediately electronic signature key in cases of its actual or suspected compromise, as well as after key expiration date established by the Contract on Service of Clients of JSC Nordea Bank using Systems 'Nordea Client- Bank (Internet)' and 'Nordea Client- Bank (Windows)' (hereinafter referred to as the "Contract").

9. Block on the same day the electronic signature keys in all cases of dismissal or change of persons admitted to these keys, as well as managers of your organization, who signed the decision (power of attorney) for admission to the key of digital signature users.

10. Insert the USB-token with key information just prior to the signing of documents, and remove it immediately after registration and signing of documents in the System.

11. Access to the System "Client-Bank" with fixed IP addresses.

12. Do not respond to e-mails (including on behalf of Nordea Bank), which ask you to provide your personal data. Do not follow the "links" mentioned in these letters (including references to the System), as they may lead to clone sites.

13. Be sure to make correct address at connection to the System, as similar addresses may be used by third parties for illegal use of your bank accounts. Address of the System is specified in Nordea online system user's guide, on the front face of scratch cards, as well as on Nordea Bank's official website (www.nordea.ru).

14. If there is no connectivity to the System, please contact the Bank by telephone of our hotline or customer technical support service at your place of service at the following numbers:

General hotline information service in Moscow:
8 495 777 3477
- Technical support:
8 495 777 3473 (for calls from Moscow and Moscow region)
8 800 100 3473 (for calls from other regions)
e-mail: bcl@nordea.ru

15. We remind you that JSC Nordea Bank is not liable for the consequences of executing orders issued by unauthorized persons of the Client, if the Bank could not establish the fact of issuing orders by unauthorized persons despite using all the applicable banking rules and the procedures stipulated in the Contract , nor for the execution of an electronic document signed with the appropriate electronic signature, in case of delayed notification or failure to notify the Bank by the Customer about the key being compromised.