NOTICE OF SECURITY RISKS WHEN USING INTERNETBANKING

Security notices related to Internetbanking use

1. In connection with the electronic communication services we provide, please allow us to inform you of a number of security risks associated with these services and notify you of the basic options you have as a user to protect your personal data, login name and access password for Internetbanking, electronic key or SMS code sent to your telephone number and any other sensitive information (hereinafter "confidential information") and to protect your computer against misuse. These are the basic rules you should follow in order to protect your confidential information and your computer.

2. The bank is obliged at its own cost in its sphere of influence to deploy equipment and organizational measures for the purposes of ensuring the security of confidential information whenever feasible and against usual threats that could compromise such confidential information.

3. The client is obliged at its own cost in its sphere of influence to take action for the purposes of ensuring the security of confidential information whenever feasible and against usual threats that could compromise such confidential information. The client is aware of the risks associated with providing electronic communication services and undertakes to respect the preventative steps and procedures shown below to ensure the security of confidential information. Failure to respect these rules and measures could lead to an abuse of confidential information and damages to a client or third party.

4. With respect to the highest level of protection for client confidential information and property, the bank recommends that clients agree with the bank on electronic payment order authorization using SMS codes or authorization using electronic signature and use the graphical keyboard when entering your password during Internetbanking login.

Risks associated with providing electronic communication services

1. Electronic communication services are provided using data or telephone lines (hereinafter "data links") that the bank does not operate; such data links are operated by a third party different from the bank. The bank has no control over security for these data links and is unable to completely eliminate all potential risks of the abuse of confidential information during transmission over these data links. There is no way to completely exclude the risk of unauthorized access to confidential information by a third party (i.e. a hacking attack, risks internal to the data network operator, "middle man" attacks, third party eavesdropping on the communication between parties, wiretapping of telephone calls, data manipulation, etc.) during the transmission of confidential information.

2. Some of the risks associated with providing electronic communication services are also in the client's sphere of influence. Such risks include insufficient security measures on the computer used to log in to

Internetbanking and for submitting bank payment orders as well as incorrect handling of confidential information by the client, which allows such information to be abused by a third party.

3. The bank is not responsible for any damages suffered by a client or a third party as a result of the abuse of confidential information unlawfully obtained from data links that are outside of the bank's sphere of influence, the client's computer or as a result of the improper handling of such information by the client if such breach has not been committed by the bank.

Preventative measures taken by the bank

1. The bank takes specific preventative measures within its sphere of influence to lessen the risk of abuse of confidential information. Such measures include the encryption of all data (e.g. user name and password for Internetbanking) transmitted between the client and the Fio server. All data is encrypted using the 128-bit SSL standard. The encryption of data significantly decreases the chances that a client's confidential information will be discovered and abused by a third party during transmission over data links.

2. The bank also provides clients with the opportunity to use additional security elements to protect access to Internetbanking, including the option to use the graphical keyboard for entering the Internetbanking password, which reduces the risk of a third person obtaining this data and the ability to confirm electronic orders submitted by the client using a commission agreement using SMS messages to a specifically defined client telephone number or electronic signature.

Keeping confidential information secret

1. Protect your confidential information and keep it private to prevent its misuse.

2. Do not write down your confidential information anywhere. If you do happen to write down your confidential information, make sure to keep it in a place that is not easily accessed by others.

3. Do not enter your confidential information in front of anyone else and do not share your confidential information with others, even family members or other close friends.

4. Set up your password as a combination of numbers and upper and lowercase letters without any connection to you or people close to you. Simple passwords with personal traits are easy to break. Do not use your date of birth, birth number, telephone number or any consecutive digits in your password. Change your passwords on a regular basis. Never change your Internetbanking password on any form other than the form kept in the Global Settings tab in Internetbanking. In no case will the bank request you use any other procedure to change your password. Your initial password must be changed when you first login to Internetbanking. This password is only valid for 365 days due to security restrictions. Once this period expires, you'll be prompted to change your password the next time you login to Internetbanking.

5. Never send confidential information via email or SMS, do not enter such information on any website other than the page used to log in to Internetbanking, even if you receive an email or SMS that calls on you in the name of the bank to send your confidential information or enter it into a different website. The bank will never send you any such type of message.

Protecting electronic keys

1. Protect the electronic key you use when placing orders from abuse, alteration or theft, copying, etc. Your electronic key can be used to infiltrate your identity and to submit orders in your name. Abuse of your electronic key can cause you serious damage.

2. Only install an electronic key on a computer you are certain is protected from potential threats from being connected to data networks. Do not install an electronic key on a publicly-accessible computer.

3. Keep an electronic key on another form of portable storage media, store this media in a place that will not lead to its abuse, alteration, theft, copying or damage.

Preventative measures in the client's sphere of influence, securing the client's computer

1. Only use the Internetbanking application on computers that are properly secured against abuse of confidential information and data. Do not use the Internetbanking application in an internet cafe or using a publicly accessible computer or on any computer where you are uncertain of if the computer is protected to prevent an abuse of confidential information and data.

2. Convince yourself that you are communicating with the correct service provider before logging in to Internetbanking. The bank's server address is http://www.fio.sk/. Check to ensure you are using a secured connection (verify SSL encryption certificate validity) and also check the bank's server before logging in to the Internetbanking application and when placing orders using the Internetbanking application. If you have any doubts as to if you are communicating with the bank or not and if the connection is properly secured or not, do not take any action that could lead to the publication or abuse of your confidential information and immediately contact the bank's client support.

3. The computer you decide to use to access Internetbanking should be secured by a legal firewall, anti-virus and anti-spyware protection with regular updates to keep these protections up-to-date. Update these programs using common methods. Regularly monitor information about new threats, viruses, spyware, etc. and ensure that your computer is properly secured.

4. Use a legal and regularly updated operating system on your computer. Regularly monitor messages from your operating system regarding any problems or deficiencies in the operating system and install fixes in a timely manner on your computer.

5. If you use Internetbanking on a specific computer, avoid downloading and installing freeware programs or other programs that are easily obtained online if you are uncertain if these programs contain viruses, spyware or are from any other untrustworthy source. Only visit known, trustworthy and secure pages online. Do not open suspicious or unrequested emails from unknown senders with suspicious names or suspicious content on such computers. Delete all such emails without opening them. Protect your email inbox with a spam filter.

6. No licensing agreement for any freeware is sufficient to guarantee you that software does not contain any components that could damage or otherwise interfere with the security of the data on your device.

7. Basic information on ways to secure your computer and the risks your computer faces can be found (in Czech) at: http://www.microsoft.com/cze/athome/security/default.mspx

SMS security

1. A SIM card, which holds the telephone number you defined for receiving authorization SMS codes from the bank (hereinafter only "SIM card") is the most important component for receiving authorization SMS codes. Always ensure this SIM card is under your supervision; a telephone without a SIM card cannot communicate with the bank or receive authorization.

2. Do not leave your mobile phone or SIM card anywhere you cannot supervise them.

3. Avoid lending your mobile phone and SIM card to third persons, even if you can observe how they use the phone and the SIM card is replaced.

4. Use your PIN code to protect your telephone from unauthorized use by a third person if your phone could ever be outside of your supervision or control. Keep this code secret and do not provide it to any third person or lose it.

5. AThe authorization code delivered to you by the bank must be kept secret and do not provide the SMS authorization code to anyone else.

6. Depending on technical progress made in the field of mobile telephones, secure your telephone and prevent third parties from automatically connecting or spying on your telephone.

Contact client support

If you receive an email with notice of any changes in the way you login to Internetbanking, information about a change in the address of the login page or if you observe any abnormal or otherwise suspicious behaviour on the login page, including an automatic redirect or other suspicious circumstances, do not do anything that could lead to a compromise or misuse of your confidential information and immediately contact the bank's client support and request further instructions for how to proceed.