Instructions for secure use of the payment instruments

1. Always create a strong password for access to your computer or mobile device, Internet banking etc – sufficiently long password (min. 8 characters) containing capital letters, small letters, digits and special characters.

2. . Do not use easy to guess password or PIN, such as names and birthdates.

3. Change your password regularly once in a few months.

4. Do not write your password anywhere (at a visible place). Do not tell anyone under no circumstances your username or password.

5. The operational system of your computer or mobile device (Windows, iOS, Android, Linux) should be up-to-date and maintained by the respective vendor. Regularly renew (minimum once a month) the operational system and the installed applications.

6. Use a firewall in combination with commercial security software (min. anti-virus protection). Regularly update the system signatures and maintain their up-to-date versions.

7. Log in your Internet banking only from your computers and mobile devices.

8. If you have to use another device, change your password, as soon as you have access to your secure device.

9. Often check your accounts via the Internet banking.

10. Subscribe for SMS messages for each credit and debit on your accounts.

11. Once a month check your bank account statement, which your Bank provides to your email or on paper in every bank branch. The Internet banking provides access to your accounts 24 hours a day, which gives you a possibility for quick reaction upon a suspicion of fraudulent operations, please call at tel. + 359 0700 15 885

12. Always check whether the site, on which you perform the operation, is encrypted (whether it starts with http**s**). At the same time on all contemporary browsers the address band will be highlighted in green (and a 'lock' will appear) in case of a correct address and a security certificate of the site. Upon clicking on the 'lock' additional information will appear regarding the security – check this regularly.

13. When you exit your Internet banking (or another site with your registration and sensitive information), always use the “Exit” button (or similar), in order to exit the system. Otherwise your session remains open for 15 more minutes and it is possible to be hacked.

14. Beware of 'phishing' attacks. These are unrequested and malicious emails, which are falsely sent by the Bank, your counterparty, known provider or client, but in fact come from fraudsters, who want to acquire secret or sensitive information of you – such as user name, password for entry in the electronic banking, details of bank cards (names on the card, number, validity date, CVC or CVV code) or create false web sites, on which you

enter such information. A distinctive feature of such emails is that they always have an element of urgency and the need of disclosing personal/sensitive data. We remind you that the Bank (and all decent traders) do not require sensitive data of their clients via e-mail, postal service or phone calls, initiated by the Bank. Such information may be requested from you only if you initiate a call to the bank. For this reason if you receive such a message, you should delete it, and not open the links (or the attached files) in it. In these cases we recommend to you to call your Internet providers or information security officers to check the used protective systems. If you have a suspicion that you became a victim to such a fraud, you should contact immediately the Customer Service centre of Municipal Bank at tel. + 359 0700 15 885

15. In case you use QES for signature as soon as you exit the Internet banking, unplug the card reader with your QES from the computer.

16. As soon as you receive the card and PIN, change the PIN, you remember. Do not use easily recognizable codes, such as birthdates or other predictable dates.

17. Do not save, nor write your PIN anywhere.

18. Do not give your card to be used by another person.

19. Never give your card to the merchant, where you make a payment at a POS terminal, or to another person, who wants to help you with the operation at an ATM. Place the card in the POS /ATM by yourself.

20. Watch out for your card all the time – not to be recorded or the card content copied in any other way.

21. You must register your card for the “3D Secure payments" service – this will require the entry of additional password upon confirmation of Internet payments.

22. Do not save, nor write your 3D passwords anywhere.

23. Inspect carefully the ATM device for unusual buttons, cameras, spots, screens– and most of all disturbance of the corpus.

24. Always cover well the keyboard, when you enter your PIN.