INFORMATION SECURITY REQUIREMENTS FOR MOBILE DEVICES

Dear Customers!

To minimize the risk of intruders getting unauthorized access to the Customer Accounts and compromising key information, the Bank kindly requests that the Customers adhere the following information security measures:

• Use password protection on your mobile device; change passwords frequently. Do not use the same password for your mobile device protection and for accessing Eurolink system.

• Turn on automatic device lock after a period of inactivity.

• Do not give your device with Eurolink app launched to a third party.

• Do not disclose your mobile device password or Eurolink account password to third parties.

• Use the latest iOS version available for your mobile device. Install iOS security updates only from the vendor' website.

• Using Eurolink on "jailbroken" (hacked) mobile devices is not recommended.

• Make sure any backup copies you make of your mobile device data are encrypted.

• Do not access Eurolink when your mobile device is connected via open Wi-Fi hotspots in public areas (in cafes, airports, etc.) – at least WPA/WPA2 encryption must be used.

• Notify the Bank immediately if any suspicious transactions in Eurolink are detected by the Customer.

• If the mobile device is lost or stolen, please notify the Bank immediately.

• If you are planning to sell or give away your mobile device to a third party, make sure you delete the Eurolink app and restore the device to factory settings (so called "hard reset").