Security requirements of the Customer's communication device and its use

During the distance selling process, the Customer may initiate electronic contracting only through his/her own phone number (also assigned to him/her by the service provider).

For Customer identification, for making electronic legal declarations (signing the contract), for the secure use of the equipment/devices used by the Customer in order to take recourse to the Bank's mobile application service (mBanking) (including in particular, but not limited to: smart phone, personal computer (desktop, laptop), tablet, including software and hardware components and e-mail account (hereinafter: Equipment), and for the protection of the Customer's personal data and bank secrets, it is essential to ensure the adequate maintenance of such equipment/devices, the security of the Equipment by continuously meeting the following - including, but not limited to - security requirements: but not exclusively by continuously meeting the following security requirements for which Customer is solely responsible.

In general, the device:

- available only after successful identification of the customer on the device, the data used for identification are regularly changed, not easy to guess (for PIN code – in case of Smartphone / Tablet-, password)
- its components (operating system, firmware, browser, applications) are regularly updated in accordance with the manufacturer's recommendations and are securely set up
- your network connections are securely set up (use appropriate wireless network security procedures (eg encryption and authentication), restrict access to network devices),
- its display is only visible to the customer during the process
- Saving the username and password in the browser is not recommended
- It is recommended to use a password that is at least 8 characters long and contains small and capital letters, numbers, special characters, does not contain a meaningful dictionary word, it is also recommended to use a dedicated password, the customer should avoid reusing the password used in other services, it is recommended to use a secure password store in general

In addition:

For Smartphone / Tablet device:

- the protection mechanisms, authorization system and other subsystems of the operating system on the device have not been modified (root - Android, jailbreak - iOS)
- SMS Preview is not enabled on a locked display
- PIN is not containing easily guessable, not contains e.g. birthdays, repetitive characters like 111111

For desktop / laptop device:

• has licensed, up-to-date malicious code protection (virus protection, anti-malware) - virus scanning runs regularly, and its scope extends to downloaded files, media connected to the device, with modern protection solutions (eg firewall)]

Moreover, the Customer ensures that access to the communication equipment used for Customer identification and for making electronic legal declarations during the distance selling process is strictly limited to the Customer excluding any access by a third party.

Provisions excluding the Bank's liability

The Bank fully excludes its liability for damages arising from the inadequate security settings or inadequate security level of the Device.

The Bank shall not be held liable for damages arising from any technical flaws of the Customer's equipment or from the Customer's failure to establish adequate connection with the Bank due to such flaws.

The Bank shall deem all applications initiated by Customers logged on to the online application interface verifiably with the relevant identification code (mobile phone) and authenticated by the one-time password sent to the Customer's mobile device to have been initiated by the person specified on the application form, and the Bank shall not check the user authorisation of the person using the identification code and the password (mobile phone) or the circumstances of the use. The Bank shall not be liable whatsoever for damages incurred by the Customer or by any other person arising from applications initiated by unauthorised persons using the identification code and the password assigned thereto.

Related to the operation of the network, in certain case it may happen even with due care, messages sent to each other are revealed to unauthorised third parties during the use of the phone and the internet. In consideration of the above, the Customer acknowledges that there are risks associated with the use of the service for disposal, and the Customer has decided to use the service after having considered such risks. In this regard, the Bank shall not be held liable for information constituting bank secret being revealed to unauthorised third parties in the course of electronic communication for reasons beyond the Bank's control.

Budapest, 16.10.2020