Security advises
related to electronic banking services

Dear Customer,

Electronic channels are considered the most secure means of payment today. However, this is only true if you familiarize yourself with the necessary safety precautions and act accordingly during use.

Attempts to misuse electronic banking products have also increased in Hungary recently. KDB Bank Europe Ltd. has already taken several steps to reduce risks through various security solutions. Since this is in our mutual interest, we also need the involvement of our customers. Therefore, we would like to help you with some important advice so that you can use the electronic services of our Bank safely.

General safety advice:

- Secure your network. Protect your devices (computer, mobile phone, tablet) with a firewall and regularly updated antivirus and antispyware software and run a full system scan at least monthly. (Try not to use trial versions, but only full versions of these programs, because only the latter comes with the latest updates and support.)
- If you connect to the Internet via a router and can change your settings, change the default password of the router and turn on the built-in firewall function (if available). It is recommended to regularly update the firmware that ensures the operation of the router. If you are using a wireless router, use WPA/WPA2 encryption, a fixed IP address, turn on MAC address filtering and allow access to the router only for your own computer.
- Keep up to date the operating systems used by your devices (Windows, Linux, MacOS, iOS, Android) and the applications installed on your devices by regularly installing official updates and patches released by manufacturers. If possible, turn on (or don't turn off) the automatic update function.
- Use only legal software on your devices and don't install apps from unknown sources or dubious origins.
- We recommend that you set your browser's privacy settings to a high level of security whenever possible to warn you during use before opening harmful content.
- **Do not install applications that are used to access to and control your computer/smartphone/tablet remotely (e.g. AnyDesk, TeamViewer, RustDesk)** or do not give anyone remote access to devices used for banking!
- Do not connect media of unknown origin (USB flash drive, memory card, CD, DVD, external hard drive, etc.) to your computer.
- Disable automatic connection of your devices to unknown wireless networks (Wi-Fi, Bluetooth).
- Under no circumstances does our Bank ask for personal or confidential identification data (e.g. user ID, password, phone number), nor does it ask you to enter, reconcile or change them, either by email or SMS! If you experience that (e.g. you appear to receive a message from the Bank with the Bank's logo/colours informing you that your ID has been misused, or asking you to visit a website), do not open the link, do not provide your data, and, please, inform the Bank's Call Centre immediately at the following contact details: +36 1 473 4440, info@kdbbank.eu.
- Our bank does not send or install any NetBank applications, certificates, links, etc. on customers' mobile phones, nor does it ask customers to do so. In connection with the use of electronic banking services, our Bank sends to mobile phones only the code required to sign orders - valid for 5 minutes - as well as ViCA registration password and initial login password via SMS. If you receive anything else, they were not sent by our Bank, so please delete them!
- **Our bank sends SMS messages from +36 70 706 0532 and +36 30 344 4094**. If you receive an SMS from another sender number, it was not sent by our Bank!
- If you receive an e-mail or SMS with a similar subject, please do not reply to it in any form, do not click on the Internet links in the letter, and do not provide your personal data and the information necessary to identify you (user ID, password, code / password received via SMS).
- Use add-ons and plug-ins to your browser to a limited extent! Do not install any add-on for your browser whose developer/vendor you do not trust, or do not or rarely use the add-on.

- Always handle messages, attachments or links from unknown senders with special care, and avoid replying to or opening them if possible.
- Backup your device regularly to prevent data loss.

Security tips for using Internet banking:

- **Never handle your banking business on public Wi-Fi.** Use your own devices for internet banking, not public devices (e.g. internet cafes, libraries) or devices accessible to many different people.
- In all cases, start the KDB NetBank service directly from the bank's website (https://www.kdbbank.eu) at the address published by KDB Bank, or directly type in the NetBank page address: https://netbank.kdbbank.eu. Always check that the name (https://netbank.kdbbank.eu) of the Internet banking website is displayed correctly in the address bar of your browser. Make sure that the **title begins with https://** string (not http:// sequence), and that the **icon with a small lock** 🔒 indicating a secure connection appears in your browser. It is very important that you never start NetBank via a link received by email!
- If you experience that you are asked for personal or identification data, passwords, codes in a message referring to maintenance, modernization or other reasons on the NetBank login interface – sometimes with bad Hungarian, difficult to understand, grammatically incorrect wording – for data reconciliation or any other purpose, do not provide it under any circumstances!
- To exit NetBank, always use the "Exit" menu item! After exiting, clear your browser history (open websites, cache, cookies, active logins).
- If you use NetBank from a public or unusual place, we recommend that you change your login password to a computer considered secure (typically your own) as soon as possible!
- In case of warnings about certificate errors, please disconnect and contact our Bank!
- Do not leave your computer unattended and exit the currently visited website or program or lock the screen when you stop using it.
- Do not keep other browser windows open or run other programs while using NetBank. Close your browser after use.
- The content of the transaction authentication SMS message and the login SMS message is different in each case, so we recommend that you always read the SMS messages received from the Bank before entering the code contained therein in NetBank!
- If you sign with an SMS code, check in the text of the SMS used to sign transactions whether the data you entered on NetBank/PC Kontakt are actually included in the message (amount and beneficiary account number in case of one transfer item, item number/total amount in case of multiple items). If you sign with ViCA, you have the opportunity to check the order details (amount, beneficiary account number) itemized in the application before approval. Sign the order with the SMS code/ViCA application only after verification!

Security advice related to password management and biometric identification:

- Use complex passwords at least 8 characters long, containing uppercase and lowercase letters, numbers, special characters. Do not use personal information (e.g. name, date of birth, phone number, address, PIN, etc.) in your passwords. Do not use the same password on multiple sites!
- It is recommended that you change the password you use regularly, at least every three months.
- Never give your password to anyone. Do not write down the password, do not save it on your computer or mobile device, never store passwords for Internet banking in browsers!
- Always make sure no one is watching you while entering your password!
- **If you suspect that your password or code has been/could have been compromised, please change it immediately!**
- Please ensure that your username and password are highly protected. Please carefully check all emails and SMS messages you receive and never provide these information in response to requests received electronically or through other channels. Always check that the login attempt or transaction you are being asked to approve is actually initiated by you! Never approve an unknown request! **Remember that if your login details are compromised, falling into the hands of a third party, you could give access to fraudsters in the online space not only for your own account but also for other accounts over which you are an authorized person.** This can multiply the potential damage that these fraudsters can cause in their abusive activities. You are therefore also reminded that you should only grant an authorization to a person in whom

you have the utmost confidence, also if you are confident in his or her knowledge of the digital space and his or her preparedness against cyber attacks.
- If you would like to be able to log in to NetBank/PC Kontakt / approve transactions only with your ID when using biometric identifiers (e.g. fingerprints) in the ViCA application, please delete the recorded biometric identifiers belonging to other persons from your device.
- Use the security SMS services provided by our Bank (Full SMS service, Mini SMS service, Security bank card SMS service) and make sure that you always have your mobile phone with you!

Safety advice for mobile devices (smartphone, tablet):

- Use screen unlock protection by setting a strong enough PIN, password of at least 5 digits, unique pattern or biometric identifier (e.g. fingerprint, faceprint) and setting up an automatic screen lock.
- Do not install applications/software downloaded directly from the Internet on your devices, instead use official sources or distribution channels (e.g. Google Play Store for Android devices, App Store for iOS devices).
- Do not break the factory permission settings of your mobile device (root, jailbreak), as this will weaken the overall level of protection of the device!
- Always check the permissions requests and services that you want to use by the application you want to install, and if an application wants to use features that do not fit into its profile (e.g. wallpaper application wants to send SMS), do not proceed with the installation. Always do this check when updating applications, because new app versions often ask for extra permissions!
- It is recommended to turn off unused services (Wi-Fi, Bluetooth, GPS, NFC) and enable them only for actual use.
- If supported by your device's operating system or device manufacturer, we recommend that you encrypt data stored on your device's background storage.

We would also like to draw your attention to the security advice related to electronic banking services contained in the Financial Navigator booklets published by the National Bank of Hungary:

- https://www.mnb.hu/fogyasztovedelem/bankszamlak/elektronikus-banki-szolgaltatasok/e-banking-biztonsag
- https://www.mnb.hu/fogyasztovedelem/bankszamlak/elektronikus-banki-szolgaltatasok/internetes-csalasok

Please also note the security advice on the following pages:

- KiberPajzs: https://kiberpajzs.hu/
- National Cyber Security Center: https://nki.gov.hu/it-biztonsag/tartalom/tudaskozpont/

If you have any questions about the above, or if you wish to notify the Bank of anomalies or security issues, please contact our Call Centre on banking days at +36 1 473 4440 or by e-mail at info@kdbbank.eu.

Sincerely,
KDB Bank Europe Ltd.