M.M.WARBURG & CO
BANK

## General Safety Instructions

- Please make sure that your PC or smart phone is sufficiently protected with up-to-date firewalls and antivirus software. Update your software regularly and check for malware on a weekly basis. An altered appearance of your apps or icons may indicate malware infection.
- Please find further security guidance and warnings on www.bsi-fuer-buerger.de.
- Always enter our internet address for online banking directly into your browser. Do not use bookmarks or favorites and do not follow web links. Your online banking access always has to use a secure server. Make sure that the login URL always starts with "https://".
- Please note that we will never send emails containing the link for our online banking website.
- No member of our staff, or that of our partners (e.g. Mastercard), will ever ask you for confidential data like your password or a TAN in emails or via telephone. Do not disclose such information to third parties.
- Please only use our web application or safe HBCI software for online banking.
- Please note that when you log in, you need to enter your customer number and your personal identification number (PIN) only. If you are asked to enter other personal data or a TAN, do not follow these instructions and inform us immediately.
- Use always strong passwords that hardly can be spied. They should contain a random combination of numbers, characters and special characters. Repetitions, known names, birthdays and numerical sequences are not suitable for passwords. Do not note your password on your hard disk, address book or telephone directory.
- If you suspect that a third party has access to your details or a TAN, your online banking or credit card must be blocked immediately. You can block online banking through the website selecting the administration tab, by entering a false PIN three times or by calling the blocking hotline below. You can block your credit card by calling +49 116 116.
- Do not use public computers or wireless LAN to make transfers as you do not have any information about the security precautions used.
- After using the online banking, please sign off before shutting down the website. Only by doing so, the data stream can be cut off reliably.

M.M.WARBURG & CO
BANK

## Mobile TAN Usage

- Delivery of the TAN by SMS is an important security component for the use of our online banking. If you have lost your mobile phone or if it has been stolen, please inform us at once by calling the below mentioned blocking hotline. We will immediately block online access to your account.
- Do not enter your mobile phone number in a web form. We will not ask you to confirm your phone number via a web form or to use it for making modifications.
- If you are asked to load a security certificate on to your mobile phone concerning the online banking, do not follow the instructions and inform us immediately. Neither a certificate nor an additional application is needed in order to use the mobile TAN.
- Do not use the same device to receive your mobile TAN as you do for your online banking. Protection is not guaranteed, if you are solely using a mobile phone to conduct online banking.
- When using the mobile TAN, compare the data displayed on your mobile phone with the entered data in the system. Only use the TAN, if the data is identical.

## TAN-Generator Usage

- The TAN-generator is an important security component for the use of online banking. Please ensure that unauthorized persons do not obtain possession of the device.
- If you have lost or misplaced your TAN-generator or if it has been stolen, please inform us at once by calling the below mentioned blocking hotline. We will immediately block online access to your account.

## BLOCKING HOTLINE

*National (free of charge) Phone +49 800 588 78 25*
*International and from mobile network Phone +49 511 3012-102*