M.M.WARBURG & CO
BANK

General security tips for internet payments

- 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 tips and current warnings under 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 weblinks. Your online banking access always uses a secure server. Make sure that the login URL always starts with "https://".

- No member of staff, or that of our partner (e.g. mastercard) will ever ask you for confidential data like your password or a TAN in emails or over the telephone. Never disclose such confidential information to unauthorised third parties.

- If possible, please only use our web application or safe HBCI software for online banking.

- Please note that when you log in, you need only enter your customer number and your personal identification number (PIN). If you are asked to enter other personal data or a TAN, do not do so and inform us immediately.

- Use always strong passwords. They should contain a random combination of numbers, characters and special characters. Repetition, 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 an unauthorised third party has access to your details or a TAN, your online banking or creditcard must be blocked immediately. You can block online banking from the website under administration, by entering 3 false pins or by calling the below mentioned blocking hotline. You can block your creditcard by calling +49 116 116.

- Do not use public computers or wireless LAN to made transfers as you do not have any information about the security precautions used.

- Once you sign on to a website you must sign off before you shut down the site. Only by signing off can you reliably cut the data link.

General security tips for mobile TAN

- Delivery of the TAN by SMS is an important security component for your use of online banking. If you should lose your mobile telephone, please inform us at once by calling the below mentioned blocking hotline. We will immediately block online access to your account.

- Never enter your mobile telephone number in a webform.

- If you are asked to load a security certificate on to your mobile telephone in connection with online banking, do not do so and inform us immediately. Neither a certificate nor an additional application is needed in order to use the mobile TAN.

- You should not use the same device to receive your mobile TAN as you did for your online banking. Protection is not guaranteed when only using a mobile phone to conduct online banking.

- When using the mobile TAN check the data displayed on your mobile phone with the entered data in the system. Only use the mTAN if the data is identical.

General security tips for the TAN generator

- The TAN generator is an important security component for your use of online banking. Please ensure that unauthorized persons do not obtain possession of the device.

- If you should lose or misplace your TAN generator, please inform us at once by calling the below mentioned blocking hotline. We will immediately block online access to your account. It will not be possible then to reactivate this TAN generator, so a new one will have to be sent to you.

Blocking Hotline

Within Germany: 0800 588 78 25

Internationally: +49 201 3101 102