# Online-Banking terms and conditions


More detailed information about the bank is contained in the "Price and Service list"

**1. Offered services**

Online-Banking is a special service provided by the bank (see the price and service list for using Online-Banking, which is also provided on the relevant Internet pages of Piraeus Bank).

(1) The account holder can process bank transactions using Online-Banking within the scope provided by the bank. In addition, the account holder can retrieve the bank's information using the Online-Banking services. The bank reserves the right to expand or restrict the scope of the banking transactions that can be processed via Online-Banking at any time. Orders transmitted to the bank prior to the changes of the offered services are not affected by these modifications. The bank shall notify the client about such changes in a suitable form.

(2) The following jointly refers to account holders and persons authorized to make dispositions as a "Participant".

(3) Use of the Online-Banking services is subject to the disposition limits separately agreed with the bank.

**2. Conditions for using Online-Banking services**

To process banking transactions by means of Online-Banking,
the participant requires the personalized security features and authentication instruments agreed with the bank, so that the participant may identify him-/herself to the bank as an authorized participant (see number 3) and to authorize orders (see number 4).

**2.1 Personalised security features**

Personalised security features, which can also be alphanumeric in nature, are:
– the personal identification number (PIN),
– single use transaction numbers (TAN).

**2.2 Authentication instruments**

TANs can be provided to the participant on the following authentication instruments:
– on a list with single use TANs, or
– by means of a mobile end-user device (for instance a mobile phone) to receive a TAN by SMS (mobileTAN).

The participant is entitled to change his/her PIN any time. If the PIN is changed, the previous PIN expires.

**3. Online-Banking access**

The participant is granted access to Online-Banking when
– he/she has transmitted his/her individual customer identification and his/her PIN,
– the bank's verification of these data has resulted in the participant's access authorization, and
– access is not blocked (see numbers 8.1 and 9).

The participant can retrieve information or enter orders after access to Online-Banking has been granted.

**4. Online-Banking orders**

**4.1 Entering and authorizing orders**

For Online-Banking orders (for instance funds transfers) to be valid, the participant must authorise said banking orders with the agreed personalised security feature (TAN) and transmit this to the bank by means of Online-Banking. The bank confirms receipt of the order by means of Online-Banking.

**4.2 Rescinding orders**

The ability to rescind Online-Banking orders is governed by the special terms and conditions for the respective order type (for instance terms and conditions for funds transfer).

Orders can only be rescinded outside of Online-Banking, unless the bank has made express provisions for the option to rescind within the Online-Banking system.

**5. Processing of Online-Banking orders by the bank**

(1) Online-Banking orders are processed as part of the ordinary processing procedures on the business days designated for processing the respective order type (for instance funds transfer) in the Online-Banking page of the bank or in the "Price and Service list". If the order is received after the point in time indicated in the Online-Banking page of the bank or in the "Price and Service list" (acceptance cut-off), or if the point in time of the receipt does not occur on a business day pursuant to the "Price and service list" of the bank, the order shall be deemed as having been received on the following business day. Processing then begins on said day.

(2) The bank shall process the order if the following processing conditions are met:
• the participant has legitimised him-/herself with his/her personalised security feature;
• the participant is authorised for the respective order type (for instance securities order);
• the Online-Banking data format is adhered to;
• the separately agreed Online-Banking authorization limit has not been exceeded;
• the processing conditions pursuant to the special terms and conditions applicable to the respective order type (for instance sufficient account balance pursuant to the terms and conditions for funds transfer) are met.
If the processing conditions pursuant to sentence 1 have been met, the bank shall process the online orders in accordance with the provisions of the special terms and conditions applicable to the respective order type (for instance terms and conditions for funds transfer, terms and conditions for securities transactions).
(3) If the processing conditions pursuant to paragraph 2 sentence 1 have not been met, the bank shall not process the Online-Banking order, and shall inform the participant by means of Online-Banking about not processing the order, and, if possible, about the reasons for the rejection and the options to correct the errors that have resulted in the rejection.

**6. Informing the account holder about online dispositions**

The bank shall inform the account holder at least once monthly about the dispositions made via Online-Banking by the method agreed to for account information.

**7. Participants' duty to exercise diligence**

**7.1 Technical connectivity to Online-Banking**

The participant is required to establish technical connectivity to Online-Banking exclusively by means of the Online-Banking access channels (for instance Internet address) separately communicated by the bank. Authorised access channels are those Internet addresses provided for Online-Banking on the bank's Internet pages.

**7.2 Confidentiality for personalised security features, and safekeeping of authentication instruments**

(1) The participant must
• maintain confidentiality of his/her personalised security features (see number 2.1) and shall only transmit these using the Online-Banking access channels separately communicated by the bank, and
• safeguard his/her authentication instrument (see number 2.2) from access by other persons.
Any other person who is in possession of the authentication instrument, can, in combination with the associated personalised security features, misuse the Online-Banking process.
(2) The following shall be noted specifically to protect the personalized security feature and the authentication instrument:
• the personalised security feature must not be stored electronically (for instance in the customer's system).
• when entering the personalised security feature, assurances must be made that other persons are not able to see said personalised security feature.
• the personalised security features must not be entered outside of the separately agreed Internet pages (for instance not in online merchant pages).
• the personalised security features must not be forwarded outside of the Online-Banking process, e.g. not by e-mail.
• the participant may not use more than one TAN, for instance to authorise an order, to lift a block, or to activate a new TAN list.
• when using the mobileTAN procedure, the device that is used to receive the TAN (for instance mobile telephone) may not be concurrently used for Online-Banking.
- a request by electronic message (e.g e-mail), to download a link contained therein for purposes of (supposed) Online-Banking of the bank, and to enter personal access information using said link, must not be complied with.
- requests outside of the original access methods provided by the bank, which ask for confidential information, such as PIN, access codes or password/online TAN, must not be responded to.
- a TAN must not be entered into a login page (homepage) for (supposed) Online-Banking of the bank.
- before its respective access to Online-Banking, the participant must ensure that commercially available security measures (such as antivirus programs and firewall) are installed on the employed system, and that said security measures, as well as the system and application software employed, are regularly updated. The participant can obtain examples of commercially available security measures on the Internet pages of the bank.

**7.3 Security of the client's system**

The participant is required to observe the security instructions on the Internet page of the bank regarding Online-Banking, in particular the measures to protect the hardware and software employed by the client's system.

**7.4 Review of order data using data provided by the bank**

If the bank displays data to the participant from the participant's Online-Banking order (e.g. amount, payment recipient's account number) in the client's system or by means of another device of the participant (for instance mobile telephone) for purposes of confirmation, the participant is required to verify that the displayed data match the data provided for the transaction before submitting the confirmation.

**8. Notification and information duties**

**8.1 Block notification**

(1) If the participant becomes aware of

• the loss or theft of the authentication instrument, the misuse or

• the otherwise unauthorised use of its authentication instrument or the participant's personal security feature,

the participant is required to immediately inform the bank about this (block notification). At any time, the participant has the ability to provide the bank with a block notification by means of the separately provided contact information.

(2) The participant shall immediately report any theft or misuse to the police.

(3) If the participant suspects that another person

• has obtained unauthorised possession of its authentication instrument or knowledge of his/her personalised safety features, or

• makes unauthorised use of the authentication instrument or the personalised safety feature,

the participant is also required to provide a block notification.

**8.2 Notification about unauthorised or erroneously executed orders**

Immediately after determining an unauthorised or erroneously executed order, the account holder is required to inform the bank.

**9. Access block**

**9.1 Block on the participant's initiative**

The bank shall perform a block on the participant’s initiative, in particular in the event of a block notice pursuant to number 8.1

• for Online-Banking access for the participant or all participants, or

• the participant's authentication instrument.

**9.2 Block on the bank's initiative**

(1) The bank is entitled to block Online-Banking access for a participant if

• the bank is entitled to terminate the Online-Banking contract for an important reason,

• this is justified due to factual circumstances in connection with the security of the authentication instrument or the personalised security feature, or

• suspicion arises for a not authorised or fraudulent use of the authentication instrument.

(2) the bank shall inform the account holder about the substantive reasons for the block, preferably before, but no later than immediately after the block is enacted.

**9.3 Lifting the block**

The bank shall lift a block or replace the personalised security feature and/or the authentication instrument if the reasons for the block are no longer given. The bank shall immediately notify the account holder about this.

**10. Liability**

**10.1 The bank's liability in connection with an unauthorised Online-Banking disposition and a not, or erroneously executed Online-Banking disposition**

The bank's liability in connection with an unauthorised Online-Banking disposition and a not, or erroneously executed Online-Banking disposition is governed by the special terms and conditions agreed for the respective order type (for instance terms and conditions for funds transfer, terms and conditions for security transactions).

**10.2 Account holder's liability in connection with misuse of its authentication instrument**

**10.2.1 Account holder's liability for unauthorised payment transactions prior to the block notification**

(1) If unauthorised payment transactions before the block notice are based on the use of a lost, stolen, or otherwise misplaced authentication instrument, the account holder shall be liable for any damage the bank incurs from this up to an amount of EUR 150.00, without regard as to whether the participant is culpable for the loss, theft, or other misplacement of the authentication instrument.

(2) If unauthorised payment transactions occur prior to the block notice due to a misuse of the authentication instrument, without the authentication instrument having been lost, stolen, or otherwise misplaced, the account holder shall be liable for any damage the bank incurs from this up to an amount of EUR 150.00, if the participant has culpably breached its obligation to safeguard the personalised security features.

(3) If the account holder is not a consumer, it shall be liable for damage due to unauthorised payment transactions above and beyond the liability limits of EUR 150.00 pursuant to paragraphs 1 and 2 if the participant has negligently or wilfully breached his/her notification and diligence duties pursuant to these terms and conditions.
(4) The account holder is not required to compensate damages pursuant to paragraphs 1, 2 and 3 if the participant was unable to provide the block notice pursuant to number 8.1, because the bank failed to provide the means to accept a lockout notification, thus causing the damage.
(5) If unauthorised payment transactions occur prior to the block notice, and the participant has wilfully or grossly negligently breached its diligence duties pursuant to these terms and conditions, or acted with fraudulent intent, the account holder shall bear the resulting damages in full. Gross negligence on the part of the participant may have occurred in particular if the participant
• fails to immediately report the loss or theft of the authentication instrument or the misuse of the authentication instrument or the personalised security features to the bank after having become aware of said loss or theft (see number 8.1 paragraph 1),
• stored the personalised security feature in the client's system (see number 7.2 paragraph 2 1. dash),
• gave the personalised security feature to another person thus causing the misuse (see number 7.2 paragraph 1 2. dash),
• entered the personalised security feature recognisably outside of the separately agreed Internet pages (see number 7.2 paragraph 2 3. dash),
• forwarded the personalised security features outside of the Online-Banking process, for instance by e-mail (see number 7.2 paragraph 2 4. dash),
• noted the personalised security feature on the authentication instrument, or stored the personalised security feature together with the authentication instrument (see number 7.2 paragraph 2 5. dash),
• has used more than one TAN to authorise an order (see number 7.2 paragraph 2 6. dash),
• when using the mobileTAN process, employs the device that was used to receive the TAN (for instance mobile telephone) to also conduct Online-Banking (see number 7.2 paragraph 2 7. dash).
(6) Liability for damages that are caused within the timeframe that applies to the availability limit is restricted to the respectively agreed availability limit.

**10.2.2 Bank's liability after the block notice**

As soon as the bank has received the participant's block notice, the bank shall assume all damages incurred in connection with unauthorised Online-Banking dispositions after said notice has been given. This does not apply if the participant acted with fraudulent intent.

**10.2.3 Exclusion of liability**

Liability claims are excluded if the circumstances used to rationalise a claim are based on an unusual and unforeseeable event, where the party that cites this event had no influence on this event, and would have been unable to avoid the consequences of said event in spite of exercising the required diligence.

**11. Termination**

The Online-Banking contract may be terminated subject to the provisions in the general business terms and conditions.

**12. General business and special terms and conditions**

The general business terms and conditions (T&Cs) apply additionally, as do the special/contractual terms and conditions agreed to for products respectively available for use in Online-Banking. The text of these terms and conditions can be reviewed in the business offices of the bank; these terms and conditions are handed out upon request. In addition, the T&Cs can be viewed, downloaded and stored from the Internet pages of Piraeus Bank (www.piraeusbank.de). Changes to the T&Cs, the terms and conditions for using Online-Banking, as well as the terms and conditions agreed for the respective product can be announced by the bank in writing, or in another suitable form, such as information in the Online-Banking system, if this announcement provides the user with means to store or print the changes in a readable format. Said changes shall be regarded as approved if the participant does not send his/her objections in writing or by electronic means within eight (8) weeks after the announcement. The bank shall again call separate attention to this consequence with the announcement.

**13. Applicable law**

The contractual relationship between the participant and the bank is governed by the laws of Germany.