Conditions for Online Banking

BERENBERG
PARTNERSHIP SINCE 1590

1 Service

(1) The account/safe custody account holder and attorney(s) can conduct banking business online using the range of online banking services offered by the Bank and can also use online banking to obtain information from the Bank. In addition, they are entitled to use a payment triggering service in accordance with Section 1 (33) of the Payment Service Supervisory Act (Zahlungsdienstaufsichtsgesetz) for triggering a payment order as well as an account information service in accordance with Section 1 (34) of the Payment Services Supervision Act for reporting information on a payment account.

(2) Account/securities account holder(s) and attorney(s) are collectively referred to as »Participant(s)«. Account(s) and safe custody account(s) are collectively referred to as »Account(s)«, unless expressly stated otherwise.

(3) The use of online banking is subject to the transaction limit agreed separately with the Bank.

2 Preconditions for the use of online banking

For the use of online banking, the Participant requires the personalised security features and authentication media agreed with the Bank in order to identify himself/herself as an authorised Participant (see No. 3) and to authorise orders (see No. 4). Instead of a personalised security feature, a biometric feature of the Participant can also be agreed upon for authentication or authorisation purposes.

2.1 Personalised security features

Personalised security features are personalised features that the bank provides to the Participant for authentication purposes. Personalised security features, which can also be in alphanumerical format are for example:

- the personal identification number (PIN),
- single-use transaction authentication numbers (TANs),
- the user code for the electronic signature.

2.2 Authentication media

Authentication instruments are personalised instruments or procedures, the use of which has been agreed between the Bank and the account holder and which are used by the Participant to issue an online banking order. The personalised security feature (e.g. TAN) can be made available to Participants using the following authentication tools in particular:

- PIN letter,
- list of single-use TANs,
- TAN generator, which is part of a chip card or another electronic device that generates TANs,
- online banking app on a mobile device (e. g. mobile phone) for receiving or generating TANs,
- mobile device (e.g. a mobile telephone) to receive TANs via text message (mobileTAN),
- chip card with signature function, or
- any other authentication medium containing signature keys.

3 Accessing the online banking service

The Participant is given access to the online banking service once

- the Participant has forwarded the account number or the individual Participant identification media and the PIN or electronic signature or used their biometric feature,
- a check of this data by the Bank establishes that the Participant is authorised to access the online banking service, and
- the access is not blocked (see Nos. 8.1 and 9).

Once the Participant has been granted access to the online banking service, the Participant is authorised to query information or issue orders. The above shall also apply if the Participant initiates payment orders via a payment triggering service and requests payment account information via an account information service (see No. 1 (1), third sentence).

4 Online banking orders

4.1 Issuing orders and authorisation

For online banking orders (e.g. credit transfers) to be effective, the Participant must authorise them using the personalised security feature provided by the Bank (e.g. TAN) or with the agreed biometric feature and send them to the Bank via online banking. The Bank confirms receipt of the order via online banking.

The above shall also apply if the Participant triggers and transmits a payment order via a payment triggering service (see No. 1 (1), third sentence).

4.2 Revocation of orders

Whether or not an online banking order can be revoked is governed by the special conditions applicable to the relevant type of order (e.g. Conditions for Credit Transfers). Orders can only be revoked outside online-banking unless the Bank expressly provides a facility for revoking them as part of the online banking service.

5 Processing of online banking orders by the Bank

(1) Online banking orders are processed on the business days stated on the Bank's online banking page or in the »List of Prices and Services« (»Preis- und Leistungsverzeichnis«) for the processing of the relevant type of order (e.g. credit transfer) as part of normal daily business operations. If the order is received after the time stated on the Bank's online banking page or stipulated in the List of Prices and Services (acceptance deadline) or if the date of receipt is not a business day as stipulated in the List of Prices and Services, the order is deemed to have been delivered on the following business day. The order will only begin to be processed on that day.

(2) The Bank will execute the order when the following conditions for execution have been met:

- the Participant has authorised the order;
- the Participant is authorised to issue the relevant type of order;
- the online banking data format has been adhered to;
- the separately agreed online banking transaction limit has not been exceeded; and
- further conditions for execution as set out in the special conditions applicable to the relevant type of order (e.g. sufficient account cover as described in the Conditions for Credit Transfers) have been met.

If the conditions for execution set out in sentence 1 have been met, the Bank executes the online banking orders in accordance with the provisions of the special conditions applicable to the relevant type of order (e.g. Conditions for Credit Transfers, Conditions for Dealings in Securities).

(3) If the conditions for execution set out under para. 2 sentence 1 are not met, the Bank will not execute the online banking order. It will provide participants with information on this via online banking and, as far as possible, will indicate the reasons and possibilities for correcting errors that led to the rejection.

6 Account holder notification of online banking transactions

The Bank shall inform the account holder at least once a month about the transactions executed via online banking through the agreed account information channel.

7 Participant's duties of care and attention

7.1 Technical connection to the online banking service

The Participant shall establish the technical connection to the online banking service via the online banking access channels notified separately by the Bank (e.g. Internet address). In order to initiate a payment order and obtain information about a payment account, the Participant may also establish the technical connection to online banking via a payment initiation service or an account information service (see No. 1 (1) sentence 3).

7.2 Secrecy of the personalised security features and safe storage of the authentication media

(1) The Participant shall

- treat his/her personalised security features (see No. 2.1) with strict confidence, and
- safely store his/her authentication medium (see No. 2.2) in a place where it cannot be accessed by third parties.

This is due to the fact that anyone who is in possession of knowledge of the authentication medium, and also has the relevant personalised security feature, can misuse the online banking service.

The obligation to maintain confidentiality with regard to the personalised security features referred to in sentence 1 shall not apply if the Participant submits them to the payment initiation service selected by him/her for the purpose of issuing a payment order or obtaining information on a payment account (see No. 1 (1), third sentence).

(2) Particular note should be taken of the following information on the protection of the personalised security feature and the authentication medium:

- The personalised security feature may not be stored electronically unsecured.
- The personalised security feature is only to be entered in a manner that assures that it may not be detected by anyone else.
- The personalised security feature must not be forwarded by e-mail.
- The personalised security feature (e.g. PIN) may not be stored in the same place as the authentication medium.
- When authorising an order or lifting a block, for example, the Participant must not use more than one TAN.
- In the mobileTAN system, the device used for receiving the TAN (e.g. mobile telephone) must not be used simultaneously for online banking.

7.3 Bank security information

The Participant must take note of the security information on the Bank's website about online banking, particularly the measures required to protect the hardware and software used (customer system).

7.4 Checking the order data against the data shown by the Bank

To the extent that the Bank shows data from the Participant's online banking order (e.g. amount, creditor account number, securities identification number) to the Participant in the customer system or via another device of the Participant (e.g. mobile telephone, chip card reader with display) for confirmation, the Participant is obliged, before giving his/her confirmation, to check that the data shown corresponds to the data intended for the transaction.

8 Disclosure and notification obligations

8.1 Blocking notice

(1) If the Participant becomes aware

- that the authentication medium is missing, has been stolen or misused, or
- that the authentication medium or a personal security feature has been used without authorisation,

the Participant must notify the Bank thereof without delay (blocking notice). The Participant can also send a blocking notice to the Bank at any time using the contact data given to him/her separately.

(2) The Participant must immediately report any theft or misuse to the police.

(3) Should the Participant suspect that a third party has, without authorisation,

- gained possession of his/her authentication medium or become aware of his/her personalised security feature, or
- used the authentication medium or the personalised security feature,

the Participant must also send a blocking notice.

8.2 Notification of unauthorised or incorrectly executed orders

The account holder shall inform the Bank without delay on finding that an orders was unauthorised or executed incorrectly.

9 Blocking

9.1 Blocking at the Participant's request

At the Participant's request, particularly in the case of a blocking notice as set out in No. 8.1, the Bank will block

- the online banking access for him/her or for all Participants, or
- his/her authentication medium.

9.2 Blocking by the Bank

(1) The Bank is authorised to block the online banking access for a Participant in cases where

- the Bank is entitled to terminate the online banking agreement for reasonable cause,
- this appears justified on account of factual reasons relating to the security of the authentication medium or the personalised security feature, or
- unauthorised or fraudulent use of the authentication medium is suspected.

(2) The Bank will notify the account/safe custody account holder if possible prior to but at the latest immediately subsequent to the blocking, stating the reasons for the blocking.

9.3 Lifting the block

The Bank will lift a block, or replace the personalised security feature or the authentication medium, if the reasons for the blocking are no longer given. The Bank shall notify the account/securities account holder hereof without delay.

9.4 Automatic blocking of a chip-based authentication medium

(1) The chip card with signature function blocks itself if an incorrect user code for the electronic signature is entered three times in succession.

(2) A TAN generator as part of a chip card that requires a separate user code to be entered blocks itself if an incorrect user code is entered three times in succession.

(3) In this case, the authentication media stated in paragraphs 1 and 2 can no longer be used for online banking. The Participant can contact the Bank in order to arrange for the online banking service to be reactivated.

10 Liability

10.1 Liability of the Bank for unauthorised online banking transactions and for online banking transactions that are not or incorrectly executed or delayed

The Bank's liability for an unauthorised online banking transaction or an online banking transaction unexecuted, defectively executed or delayed is governed by the special conditions agreed for the respective type of order (e.g. Conditions for credit transfers, Special Conditions for Dealings in Securities).

10.2 Liability of the account/safe custody account holder in the event of misuse of a personalised security feature or an authentication medium

10.2.1 Liability of the account holder for unauthorised payment transactions prior to the blocking notice

(1) If the unauthorised payment transactions prior to blocking notice pertain to use of a lost, stolen or otherwise misplaced authentication medium or other misuse of an authentication medium, the account holder is liable to the Bank for damage thus incurred up to an amount of EUR 50.00, regardless of whether the Participant is at fault.

(2) The account holder is not obliged to compensate the damage if

- it was not possible for him/her to become aware of the loss, theft, loss or any other misuse of the authentication instrument prior to the unauthorised payment transaction, or
- the loss of the authentication medium is caused by an employee, an agent, a branch of a payment service provider or any other entity to which the activities of the payment service provider have been outsourced.

(3) In cases where unauthorised payment transactions are made prior to the blocking notice and the Participant has acted fraudulently or intentionally or in gross negligence breached the duties of care and attention under these conditions, the account holder shall be fully liable in

respect of any losses incurred as a consequence thereof, notwithstanding paragraphs 1 and 2 above. Gross negligence on the part of the Participant can be deemed to have occurred, in particular, if the Participant

- fails to notify the Bank of the loss or theft of the authentication medium or of the misuse of the authentication medium or the personalized security feature immediately upon becoming aware thereof (see No. 8.1 para. 1),
- has stored the personalised security feature electronically unsecured (see No. 7.2 para. 2, first indent),
- has not kept personalised security feature strictly confident and this resulted in the misuse (see No. 7.2 para. 1),
- has forwarded the personalised security feature by e-mail, (see No. 7.2 para. 2, third indent),
- noted the personalised security feature on the authentication medium or stored it in the same place as the authentication medium (see No. 7.2 para. 2, fourth indent),
- used more than one TAN to authorise an order (see No. 7.2 para. 2, fifth indent),
- in the mobileTAN system, he/she used the device used for receiving the TAN (e.g. mobile telephone) for online banking as well (see No. 7.2 para. 2, sixth indent).

(4) Notwithstanding paragraphs 1 and 3, the account holder shall not be obliged to pay damages if the Bank has not required the participant to provide strong customer authentication in accordance with Section 1 para. 24 of the Payment Services Supervisory Act, even though the Bank was obliged to provide strong customer authentication in accordance with Section 68 para. 4 of the Payment Services Supervisory Act. Strong customer authentication requires in particular the use of two independent elements from the categories of Knowledge (something the Participant knows e.g. PIN), Ownership (something the Participant possesses e.g. TAN generator) and Inherence (something distinct to the Participant e.g. fingerprint).

(5) Liability for losses incurred during the period to which the transaction limit relates shall be limited in each case to the amount of the agreed transaction limit.

(6) The Account Holder shall not be obliged to pay compensation for the damage in accordance with paragraphs 1 and 3 if the Participant was unable to hand in the blocking notice in accordance with No. 8.1 because the Bank had not ensured the possibility of accepting the blocking notice.

(7) Paragraphs 2 and 4 to 6 shall not apply where the Participant has acted fraudulently.

(8) If the account holder is not a consumer, the following shall apply in addition:

- The account holder shall be liable for damages due to unauthorised payment transactions exceeding the liability limit of 50 euros according to paragraphs 1 and 3 if the Participant has negligently or intentionally violated his duties of notification and due diligence in accordance with these terms and conditions.
- The limitation of liability in para. 2, first indent, shall not apply.

10.2.1 Liability of the securities account holder for unauthorised securities transactions prior to the blocking notice

If the unauthorised securities transactions prior to blocking notice pertain to use of a lost or stolen authentication medium or other misuse of the personalised security feature or the authentication medium and if the Bank suffers a loss as a result, the principles of contributory negligence shall determine the extent to which the safe custody account holder and the Bank shall have to bear the loss.

10.2.3 Liability of the Bank as from the blocking notice

As soon as the Bank has received a blocking notice from a Participant, it shall assume all losses arising after this time as a result of unauthorized online banking transactions. This does not apply if the Participant acted with fraudulent intent.

10.2.4 Exclusion of liability

Claims for liability are excluded if the circumstances that give rise to a claim are the result of an unusual and unforeseeable event over which the party citing the event in question has no influence and the consequences of which it could not have avoided with all due care and attention.