Conditions for Online Banking

BERENBERG
PARTNERSHIP SINCE 1590

1 Service

(1) The customer 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. Furthermore, pursuant to Section 675f (3) of the German Civil Code (BGB) they are entitled to use payment initiation services and account information services pursuant to Section 1 (33) and (34) of the German Payment Services Supervision Act (»Zahlungsdienstaufsichtsgesetz«, ZAG). In addition, they may use other third-party services selected by them.
(2) Customer(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

(1) The Participant may use online banking if the Bank has authenticated him/her.
(2) Authentication is the procedure agreed separately with the Bank by which the Bank can verify the identity of the Participant or the authorised use of an agreed payment instrument, including the use of the Participant's personalised security feature. Using the authentication elements agreed for this purpose, the Participant can identify himself/herself to the Bank as an authorised Participant, access information (see Section 3 of these Conditions) and place orders (see Section 4 of these Conditions).
(3) Authentication elements are

- knowledge elements, i.e. something that only the Participant knows (e.g. personal identification number [PIN]),
- possession elements, i.e. something that only the Participant owns (e.g. device for generating or receiving transaction numbers [TAN] that can be used once and which prove the Participant's ownership, such as the girocard with TAN generator or the mobile device), or
- elements of inherence, i.e. something that the Participant is (e.g. fingerprint as a biometric feature of the Participant).

(4) The Participant is authenticated by the Participant transmitting the knowledge element, proof of possession and/or proof of inherence element to the bank in accordance with the Bank's request.

3 Accessing the online banking service

(1) The Participant is given access to the Bank's online banking service once

- he/she enters their individual participant ID (e.g. account number, logon name) and
- he/she identifies himself/herself using the authentication element(s) requested by the Bank, and
- there is no blocking of access (see Nos. 8.1 and 9 of these Conditions).

Once access to online banking has been granted, information may be accessed or orders placed in accordance with No. 4 of these Conditions.
(2) For access to sensitive payment data within the meaning of section 1 (26) sentence 1 ZAG (e.g. for the purpose of changing the customer's address), the Bank shall request the Participant to identify himself/herself using an additional authentication element if only one authentication element was requested to access online banking. The name of the account holder and the account number are not sensitive payment data for the payment initiation service and account information service used by the Participant (section 1 (26) sentence 2 ZAG).

4 Orders

4.1 Issuing orders and authorisation

The Participant must confirm the efficacy (provide authorisation) of an order (e.g. transfer). The Participant must use authentication elements as requested (e.g. entering a TAN as proof of possession). The Bank confirms receipt of the order via online banking.

4.2 Revocation of orders

Whether an 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) 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 on the Bank's online banking webpage or 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 business day.
(2) The Bank will execute the order when the following conditions for execution have been met:

- the Participant has authorised the order (see No. 4.1 of these Conditions);
- 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 (see No. 1 (3) of these Conditions); 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 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 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 Customer notification of online banking transactions

The Bank shall inform the customer 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 Protection of authentication elements

(1) The Participant shall take all reasonable precautions to protect his/her authentication elements (see No. 2 of these Conditions) against unauthorised access. Otherwise, there is a risk that online banking may be misused or used in any other unauthorised way (see Nos. 3 and 4 of these Conditions).
(2) In order to protect the individual authentication elements, the Participant shall pay particular attention to the following:
(a) Elements of knowledge, such as the PIN, shall be kept secret; they must in particular

- not be communicated orally (e.g. by telephone or in person),
- not passed on outside online banking in text form (e.g. by e-mail, messenger service),
- not be stored unsecured electronically (e.g. storage of the PIN in plain text in the computer or in the mobile device) and
- not be recorded on a device or stored as a transcript together with a device that serves as a possession element (e.g. girocard with TAN generator, mobile terminal, signature card) or for checking the inherence element (e.g. mobile terminal with application for online banking and fingerprint sensor).

Form 47.000 · 09.2019

(b) Possession elements such as the girocard with TAN generator or a mobile terminal must be protected against misuse, in particular

- the girocard with TAN generator or the signature card must be kept safe from unauthorised access by other persons,
- it must be ensured that unauthorised persons cannot access the Participant's mobile terminal device (e.g. mobile phone),
- it must be ensured that other persons cannot use the online banking application (e.g. online banking app, authentication app) located on the mobile terminal device (e.g. mobile phone),
- the application for online banking (e.g. online banking app, authentication app) must be deactivated on the Participant's mobile device before the subscriber gives up possession of this mobile device (e.g. by selling or disposing of the mobile phone),
- the evidence of the ownership element (e.g. TAN) may not be passed on orally (e.g. by telephone) or in text form (e.g. by e-mail, messenger service) outside online banking, and
- the Participant who has received a code from the bank to activate the possession element (e.g. mobile phone with application for online banking) must keep it safe from unauthorised access by other persons; otherwise there is a risk that other persons will activate their device as the possession element for the Participant's online banking.

(c) Elements of inherence, such as the Participant's fingerprint, may only be used as an authentication element on a participant's mobile device for online banking if no other person's elements of inherence are stored on the mobile device. If the mobile device used for online banking stores the inherence elements of other persons, the knowledge element issued by the Bank (e.g. PIN) is to be used for online banking and not the inherence element stored on the mobile device.

(3) In the mobile TAN procedure, the mobile device with which the TAN is received (e.g. mobile phone) may not be used simultaneously for online banking.

(4) The telephone number stored for the mobile TAN procedure must be deleted or changed if the participant no longer uses this telephone number for online banking.

(5) Notwithstanding the obligations under paragraphs 1 to 4, the Participant may use his/her authentication elements in relation to a payment initiation service and account information service selected by him/her as well as another third-party service (see Number 1(1) sentences 3 and 4 of these Conditions). Other third-party services shall be selected by the Participant with due care.

7.2 Bank security information

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

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

The Bank shall show the Participant the order data received by it (e.g. amount, account number of the payee, securities identification number) via the Participant's separately agreed device (e.g. mobile terminal, chip card reader with display). Prior to authorisation, the Participant is obliged to check that the displayed data correspond to the data intended for the order.

8 Disclosure and notification obligations

8.1 Blocking notice

(1) If the Participant becomes aware of

- the loss or theft of a possession element for authentication (e.g. girocard with TAN generator, mobile device, signature card) or
- the improper use or other unauthorised use of an authentication element

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

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

(3) Should the Participant suspect unauthorised or fraudulent use of any of his/her authentication elements, he/she must also issue a blocking notice.

8.2 Notification of unauthorised or incorrectly executed orders

The customer 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 of these Conditions, the Bank will block

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

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 elements of the Participant, or
- unauthorised or fraudulent use of an authentication element is suspected.

(2) The Bank will notify the customer if possible prior to but at the latest immediately subsequent to the blocking, stating the reasons for the blocking. Reasons may not be given if the Bank would thereby contravene statutory obligations.

9.3 Lifting the block

The Bank will lift a block, or replace the affected authentication elements, if the reasons for the blocking are no longer exist. The Bank shall notify the customer hereof without delay.

9.4 Automatic blocking of a chip-based possession element

(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 posession element 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.

9.5 Access blocking for payment triggering services and account information services

The Bank may refuse account information service providers or payment initiation service providers access to a payment account of the customer if objective and duly substantiated reasons in connection with unauthorised or fraudulent access of the account information service provider or payment initiation service provider to the payment account, including unauthorised or fraudulent initiation of a payment transaction, justify such refusal. The Bank shall inform the customer of any such refusal of access by the agreed means. The information shall be provided as far as possible before, but at the latest immediately after, the refusal of access. Reasons may not be given if the Bank would thereby violate statutory obligations. As soon as the reasons for refusing access no longer exist, the Bank shall lift the access block. It shall inform the customer thereof without delay.

10 Liability

10.1 Liability of the Bank in the event of the execution of an unauthorised order and for an order which has not been executed, or has been executed incorrectly or late

The Bank's liability for an unauthorised order or an order which has not been executed, or has been executed incorrectly or late 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 customer in the event of misuse of an authentication element

10.2.1 Liability of the customer 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 element or other misuse of an authentication element, the customer 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 customer 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 element prior to the unauthorised payment transaction, or
- the loss of the authentication element 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 notification under these Conditions, the customer 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 has failed to comply with one of his/her duties of care in accordance with

- No. 7.1 (2),
- No. 7.1 (4),
- No. 7.3 oder
- No. 8.1 (1).

(4) Notwithstanding paragraphs 1 and 3, the customer 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 (24) of the Payment Services Supervisory Act. Strong customer authentication requires in particular the use of two independent elements from the categories of knowledge and inherence (see No. 2 (3) of these Conditions).

(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 customer 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 customer is not a consumer, the following shall also apply:

- The customer 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.

10.2.2 Liability of the customer for unauthorised dispositions other than payment services (e.g. securities transactions) prior to the blocking notice

If the dispositions other than payment services (e.g. securities transactions) transactions prior to blocking notice pertain to use of a lost or stolen authentication element or other misuse of an authentication element and if the Bank suffers a loss as a result, the principles of contributory negligence shall determine the extent to which the customer and the Bank shall have to bear the loss.

10.2.3 Liability 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 unauthorised 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.