HAUCK AUFHÄUSER LAMPE

Further details on the bank are contained in the "List of Prices and Services".

Terms and Conditions for the use of Online Banking

(Last update: 30.04.2020)

1. Range of Services

(1) The customer and his authorized representatives may carry out banking transactions via online banking to the extent offered by the bank. In addition, the customer and his authorized representatives can call up information from the bank via online banking and are entitled under Section 675f (3) of the German Civil Code (BGB) to use payment initiation services and account information services in accordance with Section 1 (33) and (34) of the Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz - ZAG), provided that the use of Signature Folders is excluded. In addition, they may use other third-party services selected by them.

(2) In the following, customer and authorized representative are referred to as "participants". Account and securities account are hereinafter uniformly referred to as "account".

(3) The order limit agreed separately with the bank apply to the use of online banking. The participant may change these limits by a separate agreement with his/her bank. This paragraph 3 shall not apply in the case of the use of Signature Folders.

2. Requirements 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 to enable the bank to verify the identity of the participant or the legitimate use of an agreed payment instrument, including the use of the participant's personalized security feature. Using the agreed identification elements, the participant can identify himself to the bank as an authorized participant, access information (see section 3) and place orders (see section 4).

(3) Authentication elements are

- **Knowledge elements**, i.e. something that only the participant knows (e.g. personal identification number (PIN)),
- **Ownership elements**, i.e. something that only the participant owns (e.g. a device for generating or receiving one-time transaction numbers (TAN) that prove the participant's ownership, such as the girocard with TAN generator or the mobile terminal), or
- **Elements of being**, i.e. a unique feature of the participant's being (inherence, e.g. fingerprint as biometric characteristic of the participant).

(4) The participant is authenticated by the participant transmitting the knowledge element, proof of ownership and/or proof of the element of being to the bank in accordance with the bank's request.

3. Access to Online Banking

(1) The participant shall gain access to online banking if:

- he/she gives his/her individual participant identification (e.g. account number, registration name) and
- he/she identifies him/herself using the authentication elements requested by the Bank, and
- his/her account is not locked (see points 8.1 and 9)

Once access to online banking has been granted, the participant can call up information or place orders (see No. 4).

(2) In order to access sensitive payment data within the meaning of § 1 (26) sentence 1 ZAG (e.g. for the purpose of changing the customer's address), the bank requires the participant to identify himself/herself using a different authentication element if only one authentication element was requested when accessing 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. Online Banking Orders

4.1 Placing of orders

The participant must approve orders (e.g. bank transfers) for their execution (authorization). Upon request, he/she must use authentication elements for this purpose (e.g. entering a TAN as proof of ownership). The bank confirms receipt of the order via online banking.

4.2 Withdrawal of orders

The withdrawability of an order is governed by the special conditions applicable to the respective type of order (e.g. Conditions for transfers). Orders may only be withdrawn outside of online banking, unless the bank explicitly provides for a revocation option in online banking.

5. Processing of orders by the bank

(1) Orders are processed in accordance with the normal course of business on the business days specified for the processing of the respective type of order (e.g. credit transfer) on the bank's online banking site or in the "List of Prices and Services". If the order is received after the time point (acceptance period) indicated on the bank's online banking page or specified in the "List of Prices and Services" or if the time of receipt does not fall on a business day according to the bank's online banking page or the bank's "List of Prices and Services", the order is deemed to have been received on the following business day. Processing does not begin until that day.

(2) The bank will execute the order if the following conditions for execution apply:

- the participant has authorized the order (see point 4.1);
- the participant's authorization for the relevant order type (e.g. securities order or transfer order) is present;
- the online banking data format is complied with;
- the separately agreed online banking transaction limit has not been exceeded (see No. 1 paragraph 3). This provision does not apply in the case of the use of Signature Folders;
- the conditions for execution in accordance with the special conditions applicable to the relevant type of order (e.g. sufficient account cover in accordance with the conditions for credit transfer transactions) have been met.

If the conditions for execution set out in sentence 1 are met, the bank shall execute 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 Securities Transactions).

(3) If the conditions for execution pursuant to paragraph 2 sentence 1 are not met, the bank does not execute the order and will provide the participant with information about the non-execution and, as far as possible, about the reasons for it and the possibilities for correcting any errors that led to the rejection.

6. Informing the account holder about online banking orders

The bank informs the account holder at least once a month about the transactions made via online banking in the manner agreed for account information.

7. Due Diligence Obligations of the Participant

7.1 Protection of the Authentication Elements

(1) The participant must take all reasonable precautions to protect his/her authentication elements (see point 2) from unauthorized access. Otherwise there is a risk that the online banking service may be misused or otherwise used without authorization (see numbers 3 and 4).

(2) In order to protect the individual authentication elements, the participant must pay particular attention to the following:

a) Knowledge elements, such as the PIN, must be kept secret; in particular they must:

- not be communicated orally (e.g. by telephone or in person),
- not be passed on outside of 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 on the computer or mobile device) and
- not be written down on a device or kept as a copy together with a device that serves as an ownership element (e.g. girocard with TAN generator, mobile end device, signature card) or for checking the element of being (e.g. mobile end device with application for online banking and fingerprint sensor).

b) Ownership elements, such as the girocard with TAN generator or a mobile end device, must be protected against misuse, in particular:

- the girocard with TAN generator or the signature card must be kept safe from unauthorized access by other people,

- it must be ensured that unauthorized parties cannot access the participant's mobile terminal (e.g. mobile telephone),
- it must be ensured that other people cannot use the online banking application (e.g. online banking app, authentication app) on the mobile 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 participant gives up possession of this mobile device (e.g. by selling or disposing of the mobile phone),
- the verification of the ownership element (e.g. TAN) must not be passed on verbally (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 ownership element (e.g. mobile telephone with online banking application) must keep it safe from unauthorized access by other people; otherwise there is the risk that other people may activate their device as an ownership element for the participant's online banking.

c) Elements of being, such as the participant's fingerprint, may only be used as an authentication element on a mobile terminal of the participant for online banking if no elements of being of other people are stored on the mobile terminal. If the mobile terminal used for online banking stores other people's elements of being, the knowledge element issued by the bank (e.g. PIN) must be used for online banking and not the element of being stored on the mobile terminal.

(3) With the mobile TAN method, the mobile device with which the TAN is received (e.g. mobile telephone) must not be used simultaneously for online banking.

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

(5) Notwithstanding the protection obligations set out in paragraphs 1 to 4, the participant is permitted to use its authentication elements in relation to a payment initiation service and account information service selected by the participant as well as any other third-party service (see paragraph 1, first paragraph, sentences 3 and 4). The participant must select other third-party services with the due care required in such transactions.

7.2 Security instructions of the Bank

The participant must respect the security instructions on the bank's website for online banking, in particular the measures to protect the hardware and software used (customer system).

7.3 Validation of the order data with data displayed by the Bank

If the Bank shows the participant the order data received by her/him (e.g. amount, account number of the beneficiary, securities identification number) in the customer system or via another device of the participant (e.g. mobile phone, chip card reader with display) for confirmation, the participant is obliged to check the correspondence of the displayed data with the data intended for the order before the confirmation.

8. Notifications and Information Obligations

8.1 Lock Notification

(1) If the participant notices
- the loss or theft of an ownership element for authentication (e.g. mobile device, signature card) or
- the misuse or other unauthorized use of its authentication element

the participant must inform the bank of this immediately (lock notification). The participant may also submit a lock notification to the bank using the contact data provided separately.

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

(3) If the participant suspects unauthorized or fraudulent use of one of his authentication elements, he must also submit a lock notification.

8.2 Notification of unauthorized or incorrectly executed orders

The participant must notify the bank immediately upon discovery of an unauthorized or incorrectly executed order.

9. Lock of Use

9.1 Lock at the request of the participant

The bank locks at the participant's request, in particular in the case of the lock notification pursuant to No. 8.1
- the online banking access for him or all participants, or
- his/her authentication elements for using online banking.

9.2 Lock at the request of the Bank

(1) The bank may lock the online banking access for a participant if
- it is entitled to terminate the online banking agreement for good cause,
- objective reasons relating to the security of the authentication elements justify this, or
- there is a suspicion of unauthorized or fraudulent use of an authentication element.

(2) The bank will inform the customer, stating the relevant reasons, if possible before, but at the latest immediately after the lock has been imposed, using the agreed communication channel. The statement of reasons may be omitted if the bank would thereby violate legal obligations.

9.3 Unlock of the Access

The Bank will lift a lock or replace the authentication elements concerned if the reasons for the lock no longer apply. It will inform the customer of this without delay.

9.4 Automatic locking of a chip-based authentication device

(1) The chip card with signature function locks itself if the usage code for the electronic signature is entered incorrectly three times in succession.

(2) A TAN generator that requires the entry of its own user code will lock itself if it is entered incorrectly three times in a row.

(3) A TAN procedure locks itself if the TAN is entered incorrectly five times in succession.

(4) The authentication instruments mentioned in paragraphs 1, 2 and 3 can then no longer be used for online banking. The participant may contact the Bank to restore the use of online banking.

10. Liability

10.1 Liability of the Bank in the event of an unauthorized online banking transaction and a non-executed or incorrectly executed online banking transaction

The bank's liability in the event of an unauthorized order and a non-executed or incorrectly executed order is governed by the special conditions agreed for the relevant type of order (e.g. Conditions for bank transfers, Conditions for Securities Transactions).

10.2 Liability of the account/custody account holder in the event of misuse of his/her authentication elements

10.2.1 Liability of the customer for unauthorized payment transactions before the lock notification

(1) If unauthorized payment transactions prior to the blocking notification are made using a lost, stolen or otherwise missing authentication element or due to the other misuse of an authentication element, the customer is liable for any loss incurred by the Bank as a result up to an amount of EUR 50, irrespective of whether the participant is at fault.

(2) The account holder is not obliged to compensate for the loss pursuant to paragraph 1 if
- he/she has not been able to detect the loss, theft, misappropriation or other misuse of the authentication element before the unauthorized payment transaction, or
- the loss of the authentication element has been caused by an employee, an agent, a branch of a payment service provider or any other entity to which activities of the payment service provider have been outsourced

(3) If unauthorized payment transactions occur prior to the lock notification and if the participant has acted fraudulently or has violated his/her duties of care and notification under these terms and conditions intentionally or through gross negligence, the customer must, notwithstanding paragraphs 1 and 2, bear the resulting loss in full. Gross negligence on the part of the participant may be deemed to have occurred in particular if he/she has breached one of his/her due diligence obligations under:
- No. 7.1 Paragraph 2,
- No. 7.1 Paragraph 4,
- No. 7.3 or
- No. 8.1 Paragraph 1

(4) Notwithstanding paragraphs 1 and 3, the customer is not obliged to pay damages if the bank has not required the participant to provide strong customer authentication within the meaning of Section 1 (24) ZAG. Strong customer authentication requires in particular the use of two independent authentication elements from the categories knowledge, ownership or being (see No. 2 paragraph 3).

(5) Liability for damages caused within the period to which the order limit applies are limited in each case to the agreed order limit.

(6) The account holder is not obliged to compensate for the loss pursuant to paragraphs 1 and 3 if the participant was unable to submit the lock notification pursuant to No. 8.1 because the bank had not ensured that it was possible to receive the lock notification and the loss occurred as a result.

(7) Paragraphs 2 and 4 to 6 do not apply if the participant has acted fraudulently.

(8) If the customer is not a private consumer, the following applies in addition:
- The customer is liable for losses resulting from unauthorized payment transactions exceeding the liability limit of EUR 50 under paragraphs 1 and 3 if the participant has negligently or intentionally failed to fulfil his obligations to notify and exercise due care under these conditions.
- The limitation of liability in paragraph 2 first bullet point does not apply.

10.2.2 Liability of the customer for unauthorized orders outside payment services (e.g. securities transactions) before the lock notification

If unauthorized dispositions outside payment services (e.g. securities transactions which do not apply to the use of Signature Folder) prior to the lock notification are due to the use of a lost or stolen authentication element or other misuse of an authentication element, and if the bank has suffered damage as a result, the customer and the bank are liable in accordance with the statutory principles of contributory negligence.

10.2.3 Liability of the Bank after the lock notification

As soon as the bank has received a lock notification from a participant, it will bear all losses arising thereafter from unauthorized online banking transactions. This does not apply if the participant has acted with fraudulent intent.

10.2.4 Disclaimer of Liability

Liability claims are excluded if the circumstances substantiating a claim are based on an unusual and unforeseeable event over which the party invoking this event has no influence and the consequences of which could not have been avoided by it despite exercising due care.

11. Multibanking

The Multibanking function offered by the bank is an optional feature that can be used by the customer to integrate accounts, credit cards and securities accounts from domestic third-party providers. The respective third-party provider must provide the possibility of data exchange via a corresponding interface. At the third-party provider, the participant must also participate in online banking with a PIN/TAN procedure or use their online service with a comparable security procedure supported by the provider. The bank has access to the customer's account information and transactions, and processes them on an ongoing and regular basis in order to provide its services as part of its Multibanking function, to use them in selected advisory processes and to submit individual offers to the customer. The bank only transfers personal data to third parties if there is a legal obligation to do so or if the participant has given the bank his/her consent.

The data displayed via the Multibanking function in the bank's online banking system for accounts, credit cards and securities accounts held with third-party providers are requested from the third-party providers via appropriate interfaces. The bank is not liable for the accuracy and completeness of the data provided by the third-party providers via their interfaces. In addition, the bank is not liable for the availability of the Multibanking function. The bank provides the functionality in its current form and reserves the right to further develop, restrict or terminate it at any time and without prior notice. It is only liable for damages resulting from its malfunction if it has acted with intent or gross negligence.