HAUCK AUFHÄUSER LAMPE

More detailed information about the bank can bei found in the „List of Prices and Services“

Terms and Conditions of Online Banking (Version 09/2019)

1. Range of Services

(1) The Customer and his/her authorized agent(s) shall be able to conduct banking transactions by means of online banking within the scope of the services offered by the Bank. Furthermore, the Customer may use the online banking platform to retrieve information provided by the Bank. In addition, pursuant to section 675f (3) of the BGB [Civil Code], he/she is entitled to use payment initiation services and account information services in accordance with section 1 (33) and (34) of the Zahlungsdiensteaufsichtsgesetz (ZAG) [Payment Services Supervision Act]. In addition, he/she may use other third-party services of his/her choosing.

(1) The Customer and the authorized agent(s) shall hereinafter collectively be referred to as “Participant(s)”. The bank account and the securities account shall hereinafter collectively be referred to as “Account.”

(2) The use of online banking services shall be subject to the transaction limits separately agreed with the Bank. The Participant may separately agree a change to these limits with his/her Bank.

2. Conditions for Using the Online Banking Platform

(1) The Participant may use the online banking platform provided he/she has been authenticated by the Bank.

(2) Authentication is the procedure separately agreed with the Bank through which the Bank is able to verify the identity of the Participant or the authorized use of an agreed payment instrument, including the use of the Participant’s personalized security features. Through the use of the authentication elements agreed for this purpose, the Participant is able to identify him/herself to the Bank as an authorized participant, to access information (see Section 3 of these Terms and Conditions) and to place orders (see Section 4 of these Terms and Conditions).

(3) Authentication elements are

- Knowledge elements, i.e., something that the Participant knows (such as a personal identification number (PIN)),
- Possession elements, i.e., something that only the Participant possesses (e.g. a device for generating or receiving single-use transaction numbers (TANs) that provides proof of possession of the Participant, such as a debit card combined with a TAN generator or a mobile terminal, or
- Inherent elements, i.e., something that the Participant is (inherence, e.g. fingerprint used as a biometric identifier of the Participant).

(3) The Participant authenticates him/herself through transmitting to the Bank upon request either the knowledge element, proof of the possession element and/or proof of the inherent element.

3. Access to Online Banking

(1) The Participant will be granted access to the online banking services when

- he/she enters his/her individual user ID (e.g. account number, login name) and
- provides proof of identity through using the authentication element(s) requested by the Bank, and
- access has not been blocked (see Sections 8.1 and 9).

After access to the online banking services has been granted, the Participant shall be able to retrieve information or submit orders (see sectio 4).

(2) For access to sensitive payment data within the meaning of section 1 (26) sentence 1 of the ZAG (e.g. for the purpose of making changes to the Customer’s address), the Bank shall request that the participant identify him/herself using an additional authentication element if only one authentication element has been required for access to online banking. For the payment initiation service and the account information service used by the Participant, the account holder’s name and the account number are not deemed to be sensitive payment data (section 1 (26) sentence 2 of the ZAG).

4. Order Submitted via Online Banking

4.1 Submission of Orders

For orders (e.g. credit transfers) to become effective, the Participant must give his/her consent to them (authorization). Where requested, the Participant must use authentication elements (e.g. by entering a TAN as proof of the possession element). The Bank confirms receipt of the order via the online banking platform.

4.2 Cancellation of Orders

The ability to cancel an order shall be governed by the special terms and conditions applicable to the type of order in question (e.g. Terms and Conditions for Credit Transfers). Orders can only be canceled outside the online banking platform, unless the Bank expressly provides for the possibility of cancellation within the online banking platform.

5. Order Processing by the Bank

(1) Online banking orders will be processed in the course of ordinary business on the business days specified on the online banking website of the Bank or in its List of Prices and Services for the processing of the respective order type (e.g. credit transfer). If the order is received at a point in time (acceptance period) stipulated on the online banking website of the Bank or in its List of Prices and Services or if the order is received on any day which is not a business day of the Bank as stipulated on the online banking website of the Bank or in the Bank’s List of Prices and Services, the order will be deemed to have been received on the following business day. Processing of the order will only commence on that day.

(2) The Bank will execute the order if the following conditions for execution are met:

- The Participant has authorized the order (see Section 4.1);
- The Participant is authorized to submit the respective order type (e.g. securities order);
- The order adheres to the online banking data format;
- The separately agreed online banking transaction limit has not been exceeded (cf. Section 1 (3));
- The conditions for execution as stipulated in the special terms and conditions applicable to the relevant type of order (e.g. sufficient funds held in the account pursuant to the Terms and Conditions for Credit Transfers) are met.

If the conditions for execution under sentence 1 above are met, the Bank will execute the online banking orders in accordance with the provisions of the special terms and conditions applicable to the respective order type (e.g. Terms and Conditions for Credit Transfers, Terms and Conditions for Securities Transactions).

(3) If the conditions for execution as stipulated in Section 2 sentence 1 are not met, the Bank will not execute the order and will inform the Participant via the online banking platform that the order has not been executed and, if possible, the reasons for non-execution and the possibilities for correcting the errors that led to the order being rejected.

6. Information for the Account holder regarding Online Banking Transactions

The Bank will inform the account holder at least once a month using the channel agreed for providing account information on the transactions performed via the online banking platform.

7. The Participant´s Duty of Care

7.1 Protection of the Authentication Elements

(1) The Participant shall take all reasonable precautions to protect against unauthorized access to his/her authentication elements (see Section 2). Should he/she not do so, there is a danger that the online banking

(2) In order to protect the individual authentication elements, the Participant must observe the following:

a) Kowledge elements, such as the PIN, are tob e kept secret; in particular, they must not be

- communicated orally (e.g. by telephone or in person),
- disclosed outside the online banking platform in text form (e.g. by email, messenger service),
- stored in an insecure electronic form (e.g. storing the PIN in plain text on a computer or in a mobile terminal), and
- noted on a device or written down and stored together with a device that is used as a possession element (e.g. debit card with TAN generator, mobile terminal, digital signature card) or for verifying the inherent element (e.g. mobile terminal with an online banking app and a fingerprint sensor).

b) Possession elemenets, such as a debit card with a TAN generater or a mobile terminal, are tob e protected against misuse, in particular

- The debit card and the TAN generator or the digital signature card must be kept safe from unauthorized access by other individuals,
- It must be ensured that unauthorized individuals cannot gain access to the Participant’s mobile terminal (e.g. mobile telephone),

- It must be ensured that other people are not able to use the online banking application (e.g. online banking app, authentication app) on the mobile terminal (e.g. mobile telephone),
- The online banking application (e.g. online banking app, authentication app) on the Participant's mobile terminal is to be deactivated before the Participant relinquishes ownership of said mobile terminal (e.g. through sale or disposal of the mobile telephone),
- It is not permitted to disclose the proof of the possession element (e.g. TAN) orally (e.g. by telephone) or in text form (e.g. by email, messenger service) outside the online banking platform, and
- The Participant who has received a code from the Bank to activate the possession element (e.g. mobile phone with online banking app) must keep it safe from unauthorized access by other individual; should he/she not do so, there is a risk that other persons will activate their device as the possession element for the Participant's online banking service.

c) Inherent elements, such as the Participant's fingerprint, may only be used on a mobile terminal of the Participant for online banking if no inherent elements of other individuals are stored on this mobile terminal. If inherent elements of other individuals are stored on the mobile terminal used for online banking, the knowledge element (e.g. PIN) issued by the Bank, and not the inherent element stored on the mobile terminal, is to be used for online banking.

(3) For the mobileTAN system, the device receiving the TAN (e.g. mobile phone) must not be used concurrently for online banking.

(4) The telephone number registered for the mobileTAN system is to be deleted or to be changed if the Participant no longer uses this telephone number for online banking.

(5) Notwithstanding the obligation to protect set out in paragraphs 1 to 4, the Participant may use his/her authentication elements with regard to a payment initiation service and account information service of his/her choice and any other third-party service (see Section 1 (1), sentences 3 and 4). The Participant must ensure the requisite due diligence when selecting other third-party services.

7.2 Security Instructions provided by the Bank

The Participant must observe the security instructions provided on the Bank's website regarding online banking, in particular, the measures put in place to protect the hardware and software deployed (customer system).

7.3 Checking of Order Details against the Details displayed by the Bank

Where, in order to confirm an online banking order, the Bank displays the details of the Participant's order it has received (such as the amount, account number of the creditor, securities registration number) in the customer system or via any other device in the possession of the Participant (such as a mobile phone, chip-card reading device with display), prior to confirming such transaction, the Participant is required to verify that the details shown are identical to the details intended for the order.

8. Obligation to Notify and Inform

8.1 Blocking Notification

(1) If the Participant discovers
- that a possession element used for authentication purposes (such as a mobile terminal, digital signature card) has been lost or stolen, or
- his/her authentication element has been misused or used in any other unauthorized manner,

the Participant must immediately inform the Bank thereof (blocking notification). The participant may also notify the Bank at any time that access is to be blocked by using the separately provided contact details.

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

(3) If the Participant suspects that his/her authentication elements have been used in an unauthorized or fraudulent manner, he/she must also provide notification that the account is to be blocked.

8.2 Notification of unauthorized or incorrectly executed Orders

The Participant must immediately notify the Bank upon discovery of any unauthorized or incorrectly executed order.

9. Blocking of Use

9.1 Blocking Initiated by the Participant

At the Participant's request, including, without limitation, in the event of a blocking notification pursuant to Section 8.1, the Bank will block
- access to online banking for the Participant or for all participants, or
- his/her authentication elements used for online banking.

9.2 Blocking Initiated by the Bank

(1) The Bank may block access to online banking for any Participant if
- it is entitled to terminate the online banking agreement for cause,
- to do so is justified on factual grounds connected to the security of the authentication elements, or
- it suspects unauthorized or fraudulent use of an authentication element.

(2) The Bank will notify the Customer via the agreed channel, if possible, prior to but at the latest immediately subsequent to the blocking, stating the grounds for blocking. It shall be entitled to not state the grounds for the block provided that doing so would not violate any statutory obligations.

9.3 Removal of the Block

The Bank will remove the block or exchange the authentication elements affected if there are no longer any grounds for blocking. It will immediately inform the Customer thereof.

9.4 Automatic Blocking of a Chip-Based Authentication Instrument

(1) The chip card equipped with a signature function automatically blocks if the usage code for the electronic signature is entered incorrectly three times in a row.

(2) A TAN generator that requires the entry of a separate usage code automatically blocks if the code is entered incorrectly three times in a row.

(3) In this event, the authentication instruments specified in Sections 1 and 2 can no longer be used for online banking. The Participant can make contact with the Bank in order to restore usage of the online banking service.

10. Liability

10.1 Liability of the Bank for Unauthorized Online Banking Transactions or for Online Banking Transactions that are not, or incorrectly, Executed

The liability of the Bank for unauthorized order or for an order that is not, or incorrectly, executed is governed by the agreed separate terms and conditions applicable to the relevant type of order (e.g. Terms and Conditions for Credit Transfers, Terms and Conditions for Securities Transactions).

10.2 Liability of the Bank Account/Securities Account Holder for Misuse if his/her Authentication Elements

10.2.1 Liability of the Customer for Unauthorized Payment Transactions which occur prior to the Blocking Notification

(1) If any unauthorized payment transactions made prior to the blocking notification are attributable to the use of a lost, stolen or otherwise missing authentication element, or to any other form of misuse of an authentication element, the Customer shall be liable for any damage incurred by the Bank as a result thereof up to an amount of EUR 50.00, regardless of whether the Participant is at fault.

(2) The account holder shall not be obliged to compensate the loss pursuant to paragraph 1 if
- he/she not able to detect the loss, theft, disappearance or other misuse of the authentication element prior to the unauthorized payment transaction, or
- the loss of the authentication element was caused by an employee, agent, branch office of a payment service provider or any other agency to which the activities of the payment service provider have been outsourced.

(3) In cases where unauthorized payment transactions are made prior to the blocking notification and the Participant has acted with fraudulent intent, or willfully or gross negligently breached his/her duties to ensure due diligence and to provide notification under these Terms and Conditions, by way of derogation from paragraphs 1 and 2, the Customer shall be fully liable for any losses incurred as a consequence thereof. In particular, gross negligence on the part of the Participant may exist, if he/she has breached his/her duties of care pursuant to
- Section 7.1 (2),
- Section 7.1 (4),
- Section 7.3 oder
- Section 8.1 (1),

(4) By way of derogation from paragraphs 1 and 3, the Customer shall not be obliged to pay damages if the Bank has not demanded strong customer authentication from the Participant within the meaning of section 1 (24) of the ZAG. Strong customer authentication requires, in particular, the use of two separate, independent authentication elements from the categories of knowledge, possession or inherence (see Section 2 (3

(5) Liability for losses incurred within the period in which the transaction limit applies shall be limited to the amount of the respective agreed transaction limit.

(6) The account holder shall not be obliged to compensate for any losses under paragraphs 1 to 3 if the Participant was unable to submit the blocking notification under Section 8.1 because the Bank had not ensured that the notification could be delivered and the loss has arisen as a consequence thereof

(7) Paragraphs 2, 4 to 6 shall not apply if the cardholder has acted with fraudulent intent.

(8) If the Customer is not a consumer, the following shall additionally apply:

- The Customer shall be liable for damages resulting from unauthorized payment transactions in excess of the liability limit of EUR 50.00 as set forth in paragraphs 1 and 3 if the Participant has negligently or intentionally breached his/her duty of notification and due diligence under these Terms and Conditions.
- The limitation of liability in the first indent of paragraph 2 shall not apply.

10.2.2 Liability of the Customer for Unauthorized Transactions Outside Payment Services Providers (e.g. Securities Transaction) prior to the Blocking Notification

If any unauthorized transactions outside payment services providers (e.g. securities transaction) made prior to the blocking notification are attributable to the use of a lost or stolen authentication instrument, or to any other form of misuse of the authentication element, and this results in damage being incurred by the Bank, the Customer and the Bank shall be liable in accordance with the statutory principles of contributory negligence.

10.2.3 Liability of the Bank subsequent to the Blocking Notification

As soon as the Bank has received a blocking notification from the Participant, it shall bear all subsequent losses arising from unauthorized online banking transactions. This shall not apply if the Participant acted with fraudulent intent.

10.2.4 Exclusion of Liability

Any liability claim shall be excluded if the circumstances giving rise to such claim are the result of an unusual and unforeseeable event that is beyond the control of the party evoking such event and the consequences of which such party could not have prevented despite ensuring the requisite due diligence.

11. Multibanking

The Multibanking function offered by the Bank is an option that can be used by the Customer to integrate accounts, credit cards and securities accounts of domestic third-party providers. For this purpose, the respective third-party provider must provide the possibility for exchanging data via a corresponding interface. The third-party provider must also allow the Participant to participate in online banking using a PIN/TAN procedure or to use its online services in conjunction with a comparable security procedure supported by the provider. The Bank shall have access to the Customer's account information and transactions and shall process them continuously and regularly for the purpose of providing its services under the Multibanking function, to use them for selected advisory activities and to submit individual offers to the Customer. The Bank shall only transmit personal data to third parties if it is legally obliged to do so or if the Participant has given the Bank its consent thereto

The data displayed via the Multibanking function in the Bank's online banking platform relating to the accounts, credit cards and securities accounts managed by third-party providers will be retrieved from the third-party providers via the corresponding interfaces. The Bank shall not assume any liability for the accuracy and completeness of the data provided by third parties via their interfaces. The Bank shall not bear any liability 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 giving prior notice. It shall only be liable for damage resulting from the malfunction or loss of such function if it is guilty of willful intent or gross negligence.