Online Banking
Special Terms and Conditions

The present translation is furnished for the customer's convenience only. The original German text is binding in all respects.

In the event of any divergence between the English and the German texts, constructions, meanings, or interpretations, the German text, construction, meaning or interpretation shall govern exclusively.

1 Service Offer

(1) The account/securities deposit holder and their representatives may perform online banking transactions to the extent offered by Bank. In addition, they may call off information provided by Bank this way.
The holder of a payment account and his/her representatives shall also be entitled to employ a payment initiation service provider in terms of sec. 1 para. 33 of the German Financial Services Supervision Act [*Zahlungsdiensteaufsichtsgesetz*] to initiate a transaction and an account information service provider in terms of sec. 1 para. 34 of the same Act for providing payment account information.

(2) The account/securities deposit holder and their representatives are hereinafter jointly referred to as "Participants", the account and the securities deposit shall be hereinafter jointly referred to as "Account", unless the below expressly provides otherwise.

(3) Cash limits separately agreed upon with Bank shall apply to online banking usage and Participant may separately agree upon limit modifications with Bank.

2 Online Banking Usage Requirements

For online banking usage, Participant requires both the personalised security features agreed upon with Bank and the payment instruments for identifying themselves to Bank as an authorised participant (see no. 3) and to authorise transactions (see no. 4). Instead of personalised security features, the Parties may also agree upon biometric features of Participant to be used for authentication and/or authorisation purposes.

2.1 Personalised Security Features

Personalised security features describe personal identifiers which Bank provides to Participant for authentication and/or authorisation purposes. These include, without limitation:

– the personal identification number (PIN) or the usage code for electronic signatures; and
– one-time transaction numbers (TAN).

2.2 Payment Instruments

Payment instruments describe personalised instruments or procedures which Bank and the Account holder agreed to use and which Participant uses for executing online banking transactions. A TAN and/or the electronic signature can be provided to Participant in particular based on the below payment instruments:

– a TAN generator which is a component of a chip card or any other electronic device to generate TANs;
– an online banking application on a mobile terminal (such as mobile phones) for receiving or generating TANs;
– a mobile terminal (such as mobile phones) for receiving or generating TANs;
– a chip card with a signature function; or
– any other payment instrument providing for signature keys.

3 Online Banking Access

Participant is provided with online banking access if:

– they transmitted their account number or their individual participant identification code and their PIN or their electronic signature or used their biometric identifier;
– the review of these data by Bank showed that Participant is authorised to access; and
– access is not blocked in any way (see no. 9).

After Participant was granted online banking access, they can call off information or execute transactions. Sent. 1 and 2 shall also apply if Participant initiates payment transactions via payment initiation service providers and if they request payment account information through an account information service provider (see no. 1 para. 1 sent. 3).

4 Online Banking Transactions

4.1 Order Placing and Authorisation

For online banking transactions (such as wire transfers) to be effective, Participant must authenticate themselves through the personal security features (such as TANs or electronic signatures) provided by Bank or the biometric security feature and transmit this to Bank via online banking, unless they agreed otherwise with Bank. Bank shall confirm order receipt via online banking, too. Sent. 1 and 2 shall also apply if the owner of the payment account and his/her representatives initiate and transmit payment orders via a payment initiation service provider (see no. 1 para. 1 sent. 3).

4.2 Order Revocation

Online banking order revocability shall depend on the relevant special terms and conditions for the relevant type of order (such as the Transfer Transaction Terms and Conditions). Orders may be exclusively revoked outside online banking activities, unless Bank expressly provides the possibility to revoke them in this framework.

5 Online Banking Order Processing by Bank

(1) Online banking transactions shall be processed, in the framework of ordinary business processes, on those days which Bank's online banking website or "Prices and Services Schedule" identifies as business days for the relevant types of transaction (such as transfers). Should Bank receive transactions after the time indicated on Bank's online banking website or in the "Prices and Services Schedule" ("Acceptance Period") or should the time of receipt be no business day in terms of Bank's "Prices and Services Schedule", such transactions shall be deemed to be received on the subsequent business day. Processing shall only commence on that day.

(2) Bank shall process transactions provided that the below execution requirements are fulfilled:

– Participant authorised the transactions;
– Participant submitted an authorisation for the relevant type of transaction (such as securities transactions);
– The online banking data format was complied with;
– The online banking cash limit separately agreed upon was not exceeded; and
– Any other execution requirements in terms of special terms and conditions applicable to the relevant type of transaction (such as sufficient funds in terms of the Transfer Transaction Special Terms and Conditions) were fulfilled.

Provided that the execution requirements under sent. 1 were fulfilled, Bank shall execute online banking transactions pursuant to the provisions under the special terms and conditions applicable to the relevant type of transaction (such as transfer/securities transactions terms and conditions).
(3) If the execution requirements under para. 2 sent. 1 were not fulfilled, Bank shall not execute the online banking order, inform Participant about non-execution and provide – if possible and on the online banking platform – both the reasons and possibilities to correct any errors which led to non-execution.

6 Online Banking Transaction Information Provided to Account Holder

Bank shall inform the Account holder at least once a month about transactions executed on the online banking platform in the manner which they had agreed upon for account information provision.

7 Participant's Duty of Care

7.1 Technical Connection to the Online Banking Platform

Participant shall be obligated to establish technical connection to the online banking platform via the online banking access channels (such as internet addresses) which Bank separately communicated. For initiating payment transactions and requesting payment account information, the payment account holder and their representatives may establish technical connection to the online banking platform also via any payment initiation or account information service providers selected by them (see no. 1 para. 1 sent. 3).

7.2 Non-Disclosure of Personalised Security Features and Safe Payment Instruments Storage

(1) Participant shall be obligated to:

– not disclose their personalised security features (see no. 2.1); and

– safely store and protect their payment instrument (see no. 2.2) from third-party access.

This is due to any individual disposing of the payment instrument being able, in connection with the related personalised security feature, to misuse the online banking platform.
The non-disclosure duty concerning personalised security features under sent. 1 shall not apply to the payment account holder and their representatives towards payment initiation and account information service providers (see no. 1 para. 1 sent. 3) if they initiate payment transactions via payment initiation service providers and call of account information via account information service providers.
(2) In particular the following must be considered for protecting personalised security features and payment instruments: – Personalised security features must never be electronically stored without any protection;

– When entering the personalised security feature, it must be ensured that other individuals are prevented from spying this out;

– The personalised security feature must never be communicated by e-mail or any other means of telecommunication;

– The personalised security feature (such as PINs) must not be stored together with the payment instrument;

– Participant must not use more than one TAN for authorisation of, including, without limitation, transactions or for de-blocking purposes; and

– The device used for TAN receipt (such as mobile phones) must not be used for online banking purposes with regard to the mobileTAN procedure.

7.3 Bank's Security Advices

Participant must comply with Bank's online banking security advices, in particular in relation to protection measures for employed hardware and software components (customer systems).

7.4 Transaction Data Review Based on Data Displayed by Bank

Should Bank display any data to Participant on the customer system or through any other of Participant's devices (such as mobile phones, chip card reading devices with a display) resulting from their online banking transactions (such as amounts, payment recipient account numbers, securities identification numbers) for confirmation purposes, Participant must check them for correctness in relation to data required for the transaction; in the case of deviation, the transaction must be cancelled.

8 Notification and Information Provision Duty

8.1 Blocking Notification

(1) If Participant notices that they lost their payment instrument, that is was stolen or misused or that this or their personalised security feature was used in any other unauthorised manner, they must immediately notify Bank of this ("Blocking Notification"). Participant may submit such Blocking Notification, at any time, also through their contact information which they provided separately.

(2) Also, they must immediately report any card loss or theft with the police.

(3) If Participant has reason to believe that any other individual illegally

– gained possession of their payment instrument or became aware of their personalised security feature or

– used the payment instrument or personalised security feature,

they must also submit a Blocking Notification.

8.2 Notification of Unauthorised or Incorrectly Executed Transactions

The Account holder shall notify Bank of any unauthorised or incorrectly executed transactions immediately after he/she became aware of this.

9 Usage Blockage

9.1 Blockage upon Participant's Request

Upon Participant's request, Bank shall block, particularly in the case of Blocking Notifications in terms of no. 8.1,

– online banking access for Participant or each individual participant; or

– their payment instrument.

9.2 Blockage upon Bank's Request

(1) Bank may block online banking access for participants if:

– they are entitled to online banking contract cancellation for cause;

– factual reasons relating to payment instrument or personalised security feature security justify this; or

– there is reason to believe that unauthorised or fraudulent payment instrument usage occurred.

(2) Bank shall inform the account/security deposit holder about this by indicating the relevant reasons prior to – if possible – and not later than immediately after establishing a block.

9.3 De-Blocking

Bank shall deblock or replace the personalised security feature and/or payment instrument if the reasons for blocking no longer exist and inform the account/security deposit holder about his as quickly as possible.

9.4 Automatic Blocking of Chip-Based Payment Instruments

(1) Chip cards providing for a signature function block themselves if the electronic signature usage code was entered incorrectly three times in a row.

(2) A TAN generator as chip card component requiring the entry of a separate usage code blocks itself if the code was entered incorrectly three times in a row.

(3) In this case, the payment instruments under para. 1. and 2 can no longer be used for online banking purposes. Participant may contact Bank to restore online banking access.

10 Liability

10.1 Bank's Liability for Unauthorised, Failed, Incorrect or Delayed Online Banking Transactions

Bank's liability for unauthorised, failed, incorrect or delayed online banking transactions shall depend on the special terms and conditions (such as transfer/security transactions special terms and conditions) applicable to the relevant type of transaction.

10.2 Liability of the Account/Security Deposit Holder for Personalised Security Feature or Payment Instrument Misuse

10.2.1 Liability of the Account Holder for Unauthorised Payments Prior to Blocking Notifications

(1) If unauthorised payment orders prior to Blocking Notifications are based on lost or stolen payment instruments or any other misuse of payment instruments, the Account holder shall be liable for any damage which Bank incurred as a result of this up to the amount of EUR 50, regardless of whether or not Participant is culpable of this.

(2) The Account holder shall not be obligated to damage compensation in terms of para. 1 if:

– it was impossible for him/her to become aware of having lost the payment instrument, it being stolen or gone astray in any other manner or it being misused prior to the relevant unauthorised payment transaction; or

– such payment instrument loss was caused by a payment service provider employee, agent or branch or any other offices which were commissioned with activities to be performed by such payment service provider.

(3) If unauthorised payment transactions occur prior to Blocking Notifications, if Participant engaged in fraud or intentionally or grossly negligently violated their contractual duty of care under these Terms and Conditions, the Account holder shall bear, in deviation from para. 1 and 2, the full extent of the damage. Cases of gross negligence for Participant shall particularly exist if they:

– fail to notify Bank of payment instrument and/or personalised security feature loss, theft or misuse immediately after they became aware of this (see no. 8.1 para. 1);

– electronically stored the personalised security feature without any protection (see no. 7.2 para. 2 first bullet point);

– disclosed the personalised security feature which then causes a misuse (see no. 7.2 para. 1);

– communicated the personalised security feature by e-mail or any other means of telecommunication (see no. 7.2 para. 2 third bullet point);

– indicated the personalised security feature on the payment instrument or stored those elements together (see no. 7.2 para. 2, fourth bullet point);

– use more than one TAN for order authorisation purposes (see no. 7.2 para. 2 fifth bullet point); or

– use the device used for TAN receipt (such as mobile phones) also for online banking purposes with regard to the mobileTAN procedure (see no. 7.2 para. 2 sixth bullet point).

(4) In deviation from para. 1 and 3, the Account holder needs not pay damages if Bank failed to request strong customer authentication in terms of sec. 1 para. 24 of the German Payment Service Supervision Act from Participant although Bank was obligated to strong customer authentication in terms of sec. 68 para. 4 of the same Act. Strong customer authentication particularly requires the use of two independent elements from the "knowledge" (something which Participant knows, such as PINs), "possession" (something which Participant possesses, such as TAN generators) or "inherence" (something which Participant is, such as finger prints) categories.

(5) Liability for damage caused during the cash limit period shall be limited to the communicated cash limit.

(6) The Account holder shall not be obligated to compensate the damage in terms of para. 1 and 3 if Participant was unable to submit a Blocking Notification under no. 8.1 due to Bank not ensuring acceptance of such notification.

(7) Para. 2 and para. 4 through 6 shall not apply if Participant engaged in fraud.

(8) If the Account holder is no consumer, the following shall additionally apply:

– The Account holder shall be liable for damage resulting from unauthorised payment transactions exceeding the cash limit of EUR 50 in terms of para. 1 and 3 if Participant negligently or intentionally violated their duty of notification and care under these Terms and Conditions;

– liability restrictions under para. 2 first bullet point shall not apply.

10.2.2 Liability of the Security Deposit Holder for Unauthorised Securities Transactions Prior to Blocking Notifications

Should unauthorised securities transactions prior to Blocking Notifications be based on the usage of lost or stolen payment instruments or on personalised security features or payment instruments misuse and should Bank incur any damage as a consequence of this, the securities deposit holder and Bank shall be liable based on the statutory contributory negligence principles.

10.2.3 Bank's Liability from Blocking Notifications

Once Bank received a Blocking Notification from Participant, they shall be responsible for any subsequent damage caused by unauthorised online banking transactions. This shall not apply if Participant intentionally engaged in fraud.

10.2.4 Exclusion of Liability

Liability claims shall be excluded if the circumstances establishing a claim are based on unreasonable and unforeseeable events beyond the control of the Party invoking such events and if it would have been impossible to prevent the consequences despite applying a reasonable level of diligence.

11 Amicable Dispute Resolution and Other Possibilities for Complaints

For resolving any disputes with Bank, Participant may apply to the dispute resolution or complaints office indicated in the "Prices and Services Schedule" in more detail.