wirecard bank

Terms and Conditions for eBanking

The following translation is provided for the customer's convenience only. The original German text of the respective Terms and Conditions is binding in all respects. In the event of any divergence between the English and the German texts, constructions, meanings or interpretations, those of the German original shall govern exclusively

1. Services offered

1.1 The holder of an account/securities account can process banking transactions via eBanking, to the extent offered by the Bank. Furthermore, he/she can access information from the Bank via eBanking.

1.2 Account/securities account holders and authorised persons shall hereinafter be referred to as "Participants". Accounts and securities accounts shall hereinafter be referred to as "Accounts".

1.3 With regard to the usage of eBanking, the credit limits agreed separately with the Bank shall apply.

2. Conditions for the use of eBanking

In order to be able to process banking transactions via eBanking, the Participant requires the Personalised Security Features and Authentication Instruments agreed with the Bank in order to prove to the Bank his/her identity as a legitimate Participant (see clause 3) and in order to authorise orders (see clause 4).

2.1 Personalised Security Features

Personalised Security Features, which can also be alphanumerical, are the following:

- the personal identification number (PIN),
- transaction numbers which can each only be used once (TAN),
- the usage code for the electronic signature.

2.2 Authentication Instruments

The TAN and/or the electronic signature can be made available to the Participants via the following Authentication Instruments:

- as a list with TANs which can each only be used once,
- via a TAN generator which is a component of a chip card or of another electronic device for the generation of TANs,
- via a mobile device (e.g. mobile telephone) for receipt of TANs via text message (mobile TAN),
- on a chip card with signature function, or
- on another Authentication Instrument on which a signature key is stored.

For the chip card, Participants additionally require a suitable card reading device.

3. Access to eBanking

Participants are provided with access to eBanking

- after having transmitted the account number or the individualised customer identifier and the PIN or electronic signature,
- when the verification of these data by the Bank has shown that the Participant is authorised to access eBanking, and
- provided that access is not blocked (see clauses 8.1 and 9).

Once access to eBanking has been granted, the Participant will be able to retrieve information or to place orders.

4. eBanking orders

4.1 Placement of orders and authorisation

In order for eBanking orders (e.g. bank transfers) to be valid, the Participants have to authorise them with the agreed Personalised Security Feature (TAN or electronic signature), and transmit them to the Bank via eBanking. The Bank confirms receipt of the order via eBanking.

4.2 Withdrawal of orders

Whether an eBanking order can be withdrawn depends on the special terms applicable to the relevant type of order (for instance, terms for bank transfers). Orders can only be withdrawn outside the eBanking system, except if the Bank expressly offers a withdrawal option within the eBanking system.

5. Processing of eBanking orders by the Bank

5.1 eBanking orders are processed on the business days specified for the processing of the relevant type of order (e.g. bank transfer) on the Bank's eBanking site or in the List of Prices and Services, within the framework of regular work processes. If the order is received after the time specified on the Bank's eBanking site or set out in the "List of Prices and Services" (receipt deadline), or, if the time of receipt is not a business day in accordance with the Bank's "List of Prices and Services", such orders shall be deemed to have been received on the following business day. Processing will only commence on this day.

5.2 The Bank will execute the order if the following conditions are fulfilled:

- the Participant has proven his/her identity by means of the Personalised Security Feature;
- the authorisation for the Participant for the relevant type of order (e.g. securities order) has been issued;
- the eBanking data format is being complied with;
- the separately agreed eBanking credit limit is not being exceeded;
- the processing conditions according to the special terms applicable to the relevant type of order (e.g. sufficient deposit on the account, in accordance with the terms for bank transfers) are being fulfilled.

If the processing conditions under sentence 1 are fulfilled, the Bank will process the eBanking orders in accordance with the provisions of the special terms applicable to the relevant type of order (e.g. terms for bank transfers, terms for securities transactions).

5.3 If the processing conditions under sub-clause 2 sentence 1 are not fulfilled, the Bank will not process the eBanking order, and will provide the Participant with information via eBanking regarding the fact that the order will not be processed and, if possible, of the reasons for this decision and the options of correcting the mistake which led to the rejection.

6 Information for the Account Holder on eBanking transactions

The Bank will inform the Account Holder at least once per month of the transactions made via eBanking, via the means of communication agreed for account information.

7 Participant's diligence obligations

7.1 Technical connection to eBanking

The Participant is obligated to only technically connect to eBanking via the eBanking access channels (e.g. internet address) provided separately by the Bank.

7.2 Confidentiality of Personalised Security Features and secure storage of Authentication Instruments

The Participant shall be obligated

- to keep confidential his/her Personalised Security Features (see clause 2.1), and to only transmit these to the Bank via the eBanking access channels stipulated separately by the Bank, and
- to store his/her Authentication Instrument (see clause 2.2) secured against access by third parties

The reason for this is that any person who is in possession of the Authentication Instrument can, in combination with the associated Personalised Security Feature, use the eBanking procedure in an abusive manner.

The following will in particular have to be observed in order to protect the Personalised Security Feature and the Authentication Instrument:

- The Personalised Security Feature must not be stored electronically (e.g. in the customer system).
- When entering the Personalised Security Feature, it must be ensured that other persons cannot spy out such features.
- The Personalised Security Feature must not be entered outside the internet pages agreed separately (for instance not on online merchants' websites).
- The Personalised Security Feature must not be forwarded outside the eBanking procedure, i.e. for instance not by e-mail.
- The PIN and the user code for the electronic signature must not be stored together with the Authentication Instrument.
- The Participant must not use more than one TAN when authorising, for instance, an order, the lifting of a blocking or when activating a new TAN list.

Version: 1.0.0 | Status 3.11.2016

Wirecard Bank AG Serviceteam | P.O. Box 31 05 44 | 04163 Leipzig, Germany
Phone +49 (0) 30 / 300 110 600* | Fax +49 (0) 30 / 300 110 650 | service@wirecardbank.com | **www.wirecardbank.com**
Executive Board: Alexander von Knoop, Burkhard Ley, Rainer Wexeler | Chairman of Supervisory Board: Wulf Matthias
HRB number: 161178 (Munich District Court) | VAT identification number: DE 207567674 | IBAN DE75 7004 0041 0512 4805 00 | BIC COBADEFF700
* You will be charged by your telephone company for a call in the German landline.

- Within the context of the mobileTAN procedure, the device which is used to receive TANs (e.g. the mobile telephone) must not simultaneously be used for eBanking.

7.3 Safety of the customer system

The Participant must comply with the safety instructions on the Bank's internet pages relating to eBanking, in particular the measures for the protection of the hardware and software used (customer system).

7.4 Verification of order data with the data displayed by the Bank

In as far as the Bank displays data from an eBanking order (e.g. amount, recipient's account number, securities ID) in the customer system or via another device used by the Participant (e.g. mobile telephone, chip card reader with display) to the Participant for confirmation, the Participant shall be obligated to verify prior to confirming such data that the displayed data correspond to the data required for the transaction.

8 Notification and information obligations

8.1 Blocking notification

Should the Participant detect

- the loss or theft of the Authentication Instrument, an improper use or
- otherwise unauthorised use of his/her Authentication Instrument,

the Participant shall inform the Bank thereof immediately (blocking notification). The Participant can issue a blocking notification to the Bank at any time, also via the contact data provided separately to him/her.

The Participant shall immediately report any theft or improper use to the police.

Should the Participant suspect that another person

- is in possession of his/her Authentication Instrument or has knowledge of his/her Personalised Security Feature, or
- uses the Authentication Instrument or the Personalised Security Feature

without authorisation, he/she shall also issue a blocking notification.

8.2 Information on unauthorised or incorrectly processed orders

The Account/Securities Account Holder shall inform the Bank immediately should he/she detect that an order was processed without authorisation or incorrectly.

9 Blocking

9.1 Blocking upon the Participant's request

The Bank, upon a request by the Participant, in particular in the event of a blocking notification pursuant to clause 8.1, will block

- eBanking access for him/her or all participants, or
- his/her Authentication Instrument.

9.2 Blocking upon the Bank's initiative

1) The Bank may block eBanking access for a Participant if
- it has the right to terminate the eBanking contract for cause,
- this is justified due to objective reasons in connection with the security of the Authentication Instrument or the Personalised Security Feature, or
- there is a suspicion that the Authentication Instrument is being used in an unauthorised or abusive manner.

2) The Bank will inform the Account/Securities Account Holder of such blocking, including the reasons for such blocking, prior to, or at the latest immediately after the blocking.

9.3 Lifting a blocking

The Bank will lift the blocking or exchange the Personalised Security Feature or Authentication Instrument when the reasons for the blocking have ceased to apply. It shall inform the Account/Securities Account Holder thereof without delay.

9.4 Automatic blocking of a chip-based Authentication Instrument

The chip card with signature function will block itself automatically if the user code for the electronic signature is entered incorrectly three times in a row.

10 Liability

10.1 The Bank's liability for unauthorised eBanking transactions and eBanking transactions which are not carried out or not carried out correctly

The Bank's liability for unauthorised eBanking transactions and eBanking transactions not carried out or not carried out correctly shall be governed by the special terms agreed for the relevant type of order (e.g. terms for bank transfer transactions, terms for securities transactions).

10.2 Account/Securities Account Holder's liability in the event of an abuse of his/her Authentication Instrument

Account Holder's liability for unauthorised payment transactions prior to the blocking notification

a) If unauthorised payment transactions prior to the blocking notification are due to the usage of an Authentication Instrument which has been lost, stolen or has otherwise disappeared, the Account Holder will be liable to the Bank for any damage caused to the Bank, up to an amount of 150.00 Euro, irrespective of whether or not the Participant is responsible for the loss, theft or disappearance of the Authentication Instrument.

b) Should unauthorised payment transaction occur prior to the blocking notification due to an abuse of an Authentication Instrument without this instrument having been lost, stolen or having otherwise disappeared, the Account Holder will be liable to the Bank up to an amount of 150.00 Euro for the damage incurred by the Bank through this if the Participant has culpably breached his/her obligation to store the Personalised Security Features in a safe place.

c) If the Account Holder is not a consumer, he/she shall be liable for damage beyond the liability limit of 150.000 Euro pursuant to clauses 1 and 2 incurred due to unauthorised payment transactions if the Participant has negligently or intentionally failed to fulfil his/her notification and diligence obligations under these Terms and Conditions.

d) The Account Holder is not obligated to reimburse damage under clauses 1, 2 and 3 if the Participant was unable to file the blocking notification pursuant to clause 8.1 due to the Bank not having provided the possibility of receiving the blocking notification, and if the damage has incurred due to this.

e) If unauthorised payment transactions occur prior to the blocking notification, and if the Participant has intentionally or in a grossly negligent manner failed to fulfil the diligence obligations under these Terms and Conditions, or has acted in a fraudulent manner, the Account Holder shall bear the full damage incurred. The Participant may in particular be deemed to have acted in a grossly negligent manner if he/she

- has failed to inform the Bank of the loss or theft of the Authentication Instrument or the abuse of the Authentication Instrument or the Personalised Security Feature immediately after obtaining knowledge thereof (see clause 8.1 paragraph 1),
- has stored the Personalised Security Feature in the customer system (see clause 7.2 paragraph 2 item 1),
- has informed a third person of the Personalised Security Feature, and if the abuse was caused by this (see clause 7.2 paragraph 1 item 2),
- has recognisably entered the Personalised Security Feature outside the internet pages agreed separately (see clause 7.2 paragraph 2 item 3),
- has forwarded the Personalised Security Feature outside the eBanking procedure, e.g. via email (see clause 7.2 paragraph 2 item 4),
- has stored the Personalised Security Feature on the Authentication Instrument, or has stored it together with the Authentication Instrument (see clause 7.2 paragraph 2 item 5),
- has used more than one TAN in order to authorise an order (see clause 7.2 paragraph 2 item 6),
- in the mobile TAN procedure, uses the device through which the TAN is received (e.g. mobile telephone) also for eBanking (see clause 7.2 paragraph 2 item 7).

f) The liability for damage caused during the period for which the credit limit applies shall be limited to the agreed credit limit.

The Securities Account Holder's liability for unauthorised securities transactions prior to the blocking notification

Wirecard Bank AG Serviceteam | P.O. Box 31 05 44 | 04163 Leipzig, Germany
Phone +49 (0) 30 / 300 110 600* | Fax +49 (0) 30 / 300 110 650 | service@wirecardbank.com | **www.wirecardbank.com**
Executive Board: Alexander von Knoop, Burkhard Ley, Rainer Wexeler | Chairman of Supervisory Board: Wulf Matthias
HRB number: 161178 (Munich District Court) | VAT identification number: DE 207567674 | IBAN DE75 7004 0041 0512 4805 00 | BIC COBADEFF700
* You will be charged by your telephone company for a call in the German landline.

If unauthorised securities transactions prior to the blocking notification are due to the use of a lost or stolen Authentication Instrument or a different abuse of the Personalised Security Feature or of the Authentication Instrument, and if the Bank has incurred damage due to this, the Securities Account Holder and the Bank shall be liable in accordance with the statutory principles of contributory negligence.

Bank's liability after blocking notification

As soon as the Bank has received a blocking notification from a Participant, the Bank shall assume any damage incurred after this time due to unauthorised eBanking transactions. This shall not apply if the Participant has acted with fraudulent intentions.

Exclusion of liability

Liability claims shall be excluded if the circumstances which give rise to a claim are due to unusual and unforeseeable events which the Party invoking such event cannot influence, and the consequences of which could not have been avoided even if the required level of diligence had been applied

Version: 1.0.0 | Status 3.11.2016