wirecard

Terms and Conditions for Online Banking

1. Services

(1) The customer and authorised representatives of the latter may conduct banking transactions by means of the online banking services offered by the bank. They may also retrieve information from the bank through its online banking services. They are also entitled, under section 675f (3) of the German Civil Code (Bürgerliches Gesetzbuch - BGB), to use payment order services and account information services pursuant to section 1 (33) and (34) of the German Supervision of Payment Services Act (Zahlungsdiensteaufsichtsgesetz - ZAG). They may also select other third-party services for use.

(2) Unless expressly stated otherwise, customers and authorised representatives are referred to collectively as “subscribers”, and accounts and securities accounts are referred to collectively as “accounts”.

(3) The drawing limits agreed separately with the bank shall apply to the use of the online banking services.

2. Requirements for the use of online banking

(1) The subscriber may use the online banking services if authorised by the bank in an authentication process.

(2) Authentication is the procedure agreed separately with the bank by means of which the bank can verify the identity of the subscriber or the authorised use of an agreed payment instrument, including the use of the personal security feature of the subscriber. Subscribers may use the agreed authentication elements to identify themselves to the bank as the authorised users, to access information (cf. section 3 of these terms & conditions) and to place orders (cf. section 4 of these terms & conditions).

(3) Authentication elements are as follows:

- knowledge, i.e. something that is known only to the subscriber (e.g. personal identification number (PIN));
- possession, i.e. something which is possessed only by the subscriber (e.g. device used to generate or receive single-use transaction numbers (TANs) which proves the ownership of the subscriber, such as the girocard with TAN generator or the mobile terminal), or
- inherence, i.e. something which is inherent to the subscriber (e.g. fingerprint as a biometric feature of the subscriber).

(4) The subscriber will be authenticated by complying with the request of the bank to provide the bank with proof of knowledge, possession and/or inherence.

3. Access to the online banking service

(1) Access can be gained to the online banking services of the bank in the following way:

- subscribers enter their individual details (e.g. account number, login name) and
- subscribers provide the authentication element(s) requested by the bank by way of identification and
- there is no block on access (cf. sections 8.1 and 9 of these terms & conditions)

Once access to the online banking service has been granted, information may be accessed or orders may be issued in accordance with section 4 of these terms & conditions.

(2) For access to sensitive payment data, as defined in section 1 (26) clause 1 ZAG (e.g. to change the address of the customer), the bank will ask the subscriber for an additional authentication element for identification if only one authentication element is requested for access to the online banking service.

The name of the account holder and the account number will not be classed as sensitive payment data for the payment order service and account information service used by the subscriber (cf. section 1 (26) clause 2 ZAG).

4. Orders

4.1.1. Placing of orders

The subscriber must agree to an order (e.g. transfer instruction) in order for it to be effective (authorisation). The subscriber must use authentication elements in this connection on request (e.g. enter a TAN as proof of possession). The bank will confirm receipt of the order by means of online banking.

4.1.2. Revocation of orders

The revocability of an order will depend on the special conditions applicable to the respective type of order (e.g. conditions for transfer transactions). Orders may only be cancelled outside the online banking service unless the bank expressly provides a facility for cancellation in the online banking service.

5. Processing of orders by the bank

(1) Orders will be processed in the ordinary course of business on the days specified for the execution of the various types of order (e.g. bank transfer) on the bank’s online banking page or in the “List of Prices and Services”. If the order is received after the date specified on the bank’s online banking page or in the “List of Prices and Services” (acceptance deadline) or if the date of receipt does not fall on a business day in accordance with the bank’s online banking page or the bank’s "List of Prices and Services", the order will be deemed to have been received on the following business day. Processing will not commence until this business day.

(2) The bank will execute the order if the following conditions are met:

- The subscriber has authorised the order (cf. section 4.1 of these terms & conditions).
- The subscriber has the relevant authorisation for the type of order (e.g. securities).
- The online banking data format has been adhered to.
- The separately agreed online banking drawing limit has not been exceeded (cf. section 1 (3) of these terms & conditions).
- The additional terms of execution set out in the special conditions applicable to the respective type of order (e.g. sufficient funds in the account in accordance with the conditions for transfer transactions) have been met.

If the conditions pursuant to sentence 1 have been met, the bank will execute the orders in accordance with the provisions set out in the special conditions applicable to the type of order in any given case (e.g. conditions for transfer transactions; conditions for securities transactions).

(3) If the conditions pursuant to paragraph 2 sentence 1 have not been met, the bank will not execute the order. It will provide the subscriber with information through the online banking service on the action which it takes and, as far as possible, explain the reasons why the transaction was not executed and the ways in which the relevant errors can be corrected.

6. Statements of online banking transactions

The bank will inform the customer at least once a month of the transactions made through the online banking service in the manner agreed for providing such statements.

Version 5.0.0 | Status 01.01.2020

7. Duties of care of the subscriber

7.1. Protection of authentication elements

(1) The subscriber must take all reasonable precautions to protect its authentication elements (cf. section 2 of these terms & conditions) from unauthorised access. Otherwise there is a risk that online banking rights may be misused or used in some other unauthorised way (cf. sections 3 and 4 of these terms & conditions).

(2) The subscriber must pay particular attention to the following safeguards in seeking to protect the individual authentication elements:

(a) Knowledge elements, such as the PIN, must be kept secret and due note must be taken of the following requirements:
- they must not be communicated verbally (e.g. by telephone or in person);
- they must not be forwarded in text form outside the online banking service (e.g. by email, messenger service);
- they must not be stored electronically without taking security precautions (e.g. storage of the PIN in plain text in the computer or in the mobile device) and
- they must not be noted on a device or copied and kept with a device which serves as an element of possession (e.g. girocard with TAN generator, mobile terminal, signature card) or to verify the element of inherence (e.g. mobile terminal with application for online banking and fingerprint sensor).

(b) Ownership elements, e.g. the girocard with TAN generator or a mobile terminal, must be protected from misuse in the following ways in particular:
- the girocard with TAN generator or the signature card must be protected from third-party unauthorised access;
- measures must be taken to ensure that unauthorised persons cannot access the mobile device of the subscriber (e.g. mobile phone);
- steps must be taken to ensure that third parties cannot use the application on the mobile device (e.g. mobile phone) for online banking (e.g. online banking app, authentication app);
- the application for online banking (e.g. online banking app, authentication app) on the mobile device of the subscriber must be deactivated before the subscriber cedes ownership of this mobile device (e.g. by selling or disposing of the mobile phone);
- the proof of ownership (e.g. TAN) may not be passed on verbally (e.g. by telephone) or in text form (e.g. by email, messenger service) outside the online banking service, and
- the subscriber who has received a code from the bank to activate the possession element (e.g. mobile phone with application for online banking) must keep the code safe from unauthorised third-party access, otherwise there is a risk that third parties may use their device as a possession element for the subscriber's online banking.

(c) Inherence elements, such as the fingerprints of the subscriber, may only be used as an authentication element for online banking on a mobile device belonging to the subscriber if no inherence elements of other persons are stored on the mobile device. If inherence elements of other persons are stored on the mobile device used for online banking, the knowledge element issued by the bank (e.g. PIN) must be used for online banking and not the inherence element stored in the mobile device.

(3) When using the mobileTAN system, 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 subscriber no longer uses this telephone number for online banking.

(5) Notwithstanding the duties of care set out in paragraphs 1 to 4, subscribers may use their authentication elements in relation to a payment order service and account information service selected by them as well as to any other third-party services (cf. section 1 (1) sentences 3 and 4 of these terms & conditions). The subscriber must select other third-party services with due diligence.

7.2. Bank security instructions

The subscriber must observe the security instructions on the bank's online banking page, especially the measures required to protect the relevant hardware and software (customer system).

7.3. Checking the order data against data displayed by the bank

The bank will display the order data it has received to the subscriber (e.g. amount, account number of the payee, securities identification number) on the device agreed separately with the subscriber (e.g. mobile device, chip card reader with display). Prior to confirmation, the subscriber must check that the data displayed concur with the data intended for the order.

8. Duties of disclosure and notification

8.1. Notice of cancellation

(1) The subscriber must inform the bank immediately (issue notice of cancellation) on becoming aware of the following circumstances:
- the loss or theft of a possession element for authentication (e.g. girocard with TAN generator, mobile device, signature card) or
- the misuse or other unauthorised use of an authentication element.

The subscriber may also issue such notice of cancellation at any time through the communication channels arranged separately.

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

(3) Subscribers must also submit notice of cancellation if they suspect unauthorised or fraudulent use of one of their authentication elements.

8.2. Notification of unauthorised orders or incorrectly executed orders

The customer must notify the bank immediately on finding that an order was unauthorised or was executed incorrectly.

Wirecard Bank AG | Einsteinring 35 | 85609 Aschheim | Germany
Register Court Munich HRB Number: 161 178 | VAT ID: DE 207 567 674
Managing Board: Daniel Heuser, Alexander von Knoop | Chairman of the Supervisory Board: Wulf Matthias
Phone +49 (0)89 4424 2000 | Fax +49 (0)89 4424 2100 | service@wirecardbank.com | www.wirecardbank.com

9. Prevention of use

9.1. Blocks at the request of the subscriber

The bank will disable the following at the request of the subscriber, especially if notice of cancellation has been issued pursuant to section 8.1 of these terms & conditions:

- the online banking access for this subscriber or all subscribers, or
- the authentication elements of this subscriber for the use of the online banking service.

9.2. Blocks at the instigation of the bank

(1) The bank may block access to the online banking service to a subscriber in the following cases:

- if it is entitled to terminate the online banking contract for good cause;
- if this is justified for objective reasons in connection with the security of the authentication elements of the subscriber, or
- if there is a suspicion of unauthorised or fraudulent use of an authentification element.

(2) The bank will notify the customer through the agreed channels of the action being taken and the relevant reasons for its decision, in advance if at all possible but immediately afterwards at the latest. The bank may refrain from giving reasons if it would violate its statutory obligations in doing so.

9.3. Lifting a block

The bank will lift the block or replace the relevant authentication elements if the reasons for the block no longer apply. The bank will notify the customer hereof without undue delay.

9.4. Automatic block on a chip-based possession element

(1) A chip card with a signature function will be blocked automatically if the code for the electronic signature is entered incorrectly three times in succession.

(2) A TAN generator forming part of a chip card and requiring the entry of a code will lock automatically if the code is entered incorrectly three times in succession.

(3) It will then no longer be possible to use the possession elements referred to in paragraphs 1 and 2 for online banking. The subscriber may contact the bank to ask for the facility of online banking to be restored.

9.5. Block on access to payment order services and account information services

The bank may refuse account information service providers or payment order service providers access to an account used for payments by a customer if the refusal is justified by objective and duly substantiated reasons in connection with unauthorised or fraudulent access by the account information service provider or payment order service provider to the account used for payments, including unauthorised or fraudulent initiation of a payment transaction. The bank will inform the customer through the agreed channels of any such course of action, preferably before refusing access but at the latest immediately afterwards. The bank may refrain from giving reasons if it would violate its statutory obligations in doing so. The bank will lift the block on access as soon as the reasons for refusing access cease to apply. It will also inform the customer hereof without delay.

10. Liability

10.1. Liability of the bank in executing unauthorised orders, failing to execute orders, or failing to execute orders correctly or on time

The liability of the bank in executing unauthorised orders, failing to execute orders, or failing to execute orders correctly or on time will be dictated by the special terms & conditions agreed for the respective type of order (e.g. conditions for transfer transactions, conditions for securities transactions).

10.2. Liability of customers in the event of misuse of their authentication elements

10.2.1. Liability of customers for unauthorised payment transactions prior to the notice of cancellation

(1) If unauthorized payment transactions prior to the notice of cancellation involve the use of a lost, stolen or otherwise misplaced authentication element of any other improper use of an authentication element stolen or otherwise misplaced, the customer will be liable for any losses incurred by the bank as a result up to an amount of 50 euro, irrespective of whether the subscriber is at fault.

(2) The customer will not be obliged to compensate for the losses under paragraph 1 in the following cases:

(a) it was not possible for the customer to notice the loss, theft, misplacement or other improper use of the authentication element prior to the unauthorised payment transaction, or

(b) the loss of the authentication element was caused by an employee, agent or branch of a payment service provider or by another agency to which the services of the payment service provider have been outsourced

(3) If unauthorised payment transactions are carried out before the notice of cancellation is issued, and if the subscriber acted with fraudulent intent or violated the relevant duties of care and notification under these terms & conditions with deliberate intent or gross negligence, the customer will bear the resulting losses in full, contrary to the provisions set out in paragraphs 1 and 2. The subscriber may most notably be guilty of gross negligence if the latter has failed to comply with one of the relevant duties of care under the following sections of these terms & conditions:

- section 7.1 (2);
- section 7.1 (4);
- section 7.3 or
- section 8.1 (1).

(4) By way of derogation from paragraphs 1 and 3, the customer shall not be liable to pay damages if the bank did not ask the subscriber to provide strong authentication as defined in section 1 (24) ZAG. Strong customer authentication most notably requires the use of two independent elements categorised as knowledge, possession or inherence (cf. section 2 (3) of these terms & conditions).

(5) Liability for losses incurred within the period to which the drawing limit applies shall be restricted to the drawing limit agreed in any given case.

(6) The customer will not be held liable for the losses pursuant to paragraphs 1 and 3 if the subscriber was unable to issue the notice of cancellation pursuant to section 8.1 of these terms & conditions because the bank had not put measures in place to ensure receipt of the notice of cancellation.

(7) Paragraphs 2 and 4 to 6 shall not apply if the subscriber acted with fraudulent intent.

Wirecard Bank AG | Einsteinring 35 | 85609 Aschheim | Germany
Register Court Munich HRB Number: 161 178 | VAT ID: DE 207 567 674
Managing Board: Daniel Heuser, Alexander von Knoop | Chairman of the Supervisory Board: Wulf Matthias
Phone +49 (0)89 4424 2000 | Fax +49 (0)89 4424 2100 | service@wirecardbank.com | www.wirecardbank.com

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

- The customer will be liable for damages due to unauthorised payment transactions exceeding the liability limit of 50 euro pursuant to paragraphs 1 and 3 if the subscriber was negligent or acted with intent in breaching the relevant duties of notification and due diligence under these terms & conditions.
- The limitation of liability in the first bullet point in paragraph 2 shall not apply.

10.2.2. Liability of the customer in the event of unauthorised transactions not classed as payment services (e.g. securities transactions) prior to the notice of cancellation

If unauthorised transactions not classed as payment services (e.g. securities transactions) prior to the notice of cancellation involve the use of a lost or stolen authentication element or any other improper use of the authentication element, and if the bank has suffered losses as a result, both the customer and the bank will be liable in accordance with the statutory principles of contributory negligence.

10.2.3. Liability after notice of cancellation

As soon as the bank has received notice of cancellation from a subscriber, it will assume all the losses incurred thereafter as a result of unauthorised online banking transactions. This shall not apply if the subscriber acted with fraudulent intent.

10.2.4. Exclusion of liability

No liability claims may be made if the circumstances giving rise to a claim involve an unusual and unforeseeable event over which the party citing said event has no control and the consequences of which could not have been avoided by said party despite exercising due care.

Wirecard Bank AG | Einsteinring 35 | 85609 Aschheim | Germany
Register Court Munich HRB Number: 161 178 | VAT ID: DE 207 567 674
Managing Board: Daniel Heuser, Alexander von Knoop | Chairman of the Supervisory Board: Wulf Matthias
Phone +49 (0)89 4424 2000 | Fax +49 (0)89 4424 2100 | service@wirecardbank.com | www.wirecardbank.com