COMMERZBANK

Business Conditions for Remote Communication

(Stand 31.10.2009)

1. Scope of services

(1) The account/securities account holder may execute banking transactions by means of Remote Communication within the scope offered by the Bank. The execution shall be subject to the conditions for the relevant banking transactions (e.g. general conditions for payment services, conditions for the use of Dresdner OnlineDepot, special conditions for securities transactions). In addition, he/she may retrieve information provided by the Bank by means of Remote Communication. The Bank may notify the account/securities account holder of any amendment of its Business Conditions in electronic form and make them available for download. With respect to the effectiveness of such amendments, the regulation in No. 1 (2) of its General Business Conditions or differing conditions which may have been agreed with the customer shall remain valid.

(2) Account/securities account holders and authorised persons are hereinafter collectively referred to as "User". The account and securities account is hereinafter collectively referred to as "Account".

(3) For the use of Remote Communication, the standard limits or drawing limits agreed with the Bank for Remote Communication separately shall apply.

2. Preconditions for the use of Remote Communication

For the execution of banking transactions by means of Remote Communication, the User requires the personalised security features and authentication instruments agreed with the Bank in order to prove his identity to the Bank as authorised User (see No. 3) and to authorise orders (see No. 4).

2.1 Personalised security features

Personalised security features which may also be alphanumerical are:
- the personal identification number (PIN)
- transaction authorisation numbers (TAN), usable once only (not applicable for telephone banking)
- the signature PIN / code word and the data of the personal electronic key for the electronic signature
- any other authentication instrument agreed by the Bank with the User

2.2 Authentication instruments

The TAN may be made available to the User on a list containing TANs usable once only. The Users may use further authentication instruments to store the electronic signature data:
- chipcard with signature function
- other authentication instrument containing the signature key or
- any other security feature agreed by the Bank with the User.

In connection with a chipcard, the User additionally requires an adequate card reader.

3. Access to Remote Communication

The User is allowed access to Remote Communication, if
- the User has transmitted his personal customer identification („Banking ID") and his/hers PIN or electronic signature,
- the verification of this/her data by the Bank has shown that an access authorisation for the User exists, and
- access has not been blocked (see nos. 9.1 and 10).

After access to Remote Communication has been enabled, the User can retrieve information or give orders.

4. Execution of orders within the scope of Remote Communication

4.1 Giving of orders and authorisation

The User must authorise an order given within the scope of Remote Communication (e.g. a credit transfer) by means of the agreed personalised security feature (for example PIN and TAN or signature PIN / code word and the electronic signature) in order to be effective and transmit it to the Bank via Remote Communication. The Bank confirms the receipt of the order by means of Remote Communication.

4.2 Report according to the German Foreign Trade and Payments Ordinance (AWV)

In connection with payments in favour of non-residents, the report according to the German Foreign Trade and Payments Ordinance (AWV) is to be observed.

4.3 Revocation of orders

The revocability of an order shall be subject to the special conditions applicable for the relevant order type. Orders can only be revoked outside the Remote Communication service, unless the Bank expressly provides for a revocation option in its Remote Communication system.

5. Processing of orders by the Bank

(1) The orders given within the scope of Remote Communication shall be processed according to the regulations applicable for the processing of the relevant order type (e.g. credit transfer or securities order).

(2) Payment orders (credit transfer, direct debit) shall be subject to the following special regulations:

The Bank will execute the order subject to the following conditions:
- the User has proved his identity by means of his personalised security feature
- the User's authorisation for the relevant order type has been verified
- the Remote Communication data format is adhered to
- the separately agreed Remote Communication drawing limit or the standard limit is not exceeded
- the preconditions for execution according to the special conditions applicable to the relevant order type are complied with
- sufficient cover in the account (credit balance or granted credit) is available.

If the preconditions for execution according to sentence 1 are complied with, the Bank will execute the order. Such execution shall not be in breach of any other legal provisions.

(3) If the preconditions for execution according to para. (2), sentence 1, bullet points 1–5, are not complied with, the Bank will not execute the payment order. If it does not execute the payment order, it will provide an information to the User via Remote Communication on the non-execution and, as far as possible, the reasons for the non-execution as well as the possibilities of correcting any errors which have caused the non-execution. This shall not apply if the statement of reasons is in breach of any other legal provisions. If the Bank executes the order in the absence of sufficient cover in the account, a tolerated account overdraft arises for which an increased interest rate shall be payable.

6. Notification to the account holder on drawings made by means of Remote Communication

The Bank shall notify the account holder of the drawings made by means of Remote Communication in the form agreed for account and securities account information and in accordance with the conditions applicable for the order.

7. Duties of care of the User

7.1 Technical connection to Remote Communication

The User shall be obliged to establish the technical connection to Remote Communication only through the Remote Communication access channels (e.g. Internet address) notified by the Bank separately.

7.2 Keeping the personalised security features secret and careful safekeeping of the authentication instruments

(1) The User shall
- keep his/her personalised security features (see No. 2.1) secret and transmit them to the Bank only via the Remote Communication access channels notified by the Bank separately, and
- keep his/her authentication instrument carefully (see No. 2.2) to prevent access by other persons.

This is because any other person who is in possession of the authentication instrument can misuse the Remote Communication procedure in combination with the related personalised security feature.

(2) In particular, the following is to be observed for the protection of the personalised security feature and the authentication instrument:
- The personalised security features PIN and TAN as well as the signature PIN / code word may not be stored electronically (e.g. in the customer system). The personal electronic key generated by the User shall be under the control of the User alone.
- When entering the personalised security feature, it is to be ensured that no other person can spy it out.
- The personalised security features may not be entered outside the separately agreed Internet pages (e.g. not on online pages of traders).
- The personalised security features may not be transmitted outside the Remote Communication procedure, for instance not by e-mail.
- The signature PIN / code word for the electronic signature may not be kept together with the authentication instrument.
- The User may not use more than one TAN for the authorisation of an order.

7.3 Verification of the order data by means of the data displayed by the Bank
If the Bank displays data to the User contained in his Remote Communication order (e.g. amount, account number of payee, securities identification no.) in the customer system or via another device of the User (e.g. mobile phone, chipcard reader with display) for confirmation, the User shall be obliged to verify that the displayed data conform with the data of the intended transaction prior to confirmation.

8. Import of software from and export to foreign countries

A software made available by the Bank may not be used in countries where restrictions of use or import and export restrictions for encryption techniques exist.

9. Notification and information duties

9.1 Blocking request
(1) If the User detects
– the loss or theft of the authentication instrument,
– the misuse thereof, or
– any other unauthorised use of his/her authentication instrument or personal security feature,
the User shall notify the Bank thereof without delay (blocking request). The User may give a blocking request to the Bank whenever required also by means of the contact details notified to him separately.
(2) The User shall report any theft or misuse to the police without delay.
(3) If the User has the suspicion that another person
– has come into the possession of his/her authentication instrument in an unauthorised manner or has gained unauthorised knowledge of his personalised security feature otherwise, or
– uses the authentication instrument or personalised security feature,
he must also give a blocking request.

9.2 Notification on unauthorised or incorrectly executed orders
The account holder shall notify the Bank as soon as he/she detects an unauthorised or incorrectly executed order.

10. Blocking of access

10.1 Blocking of access at the request of the User
At the request of the User, especially in the event of a blocking request according to No. 9.1 above, the Bank will block
– the Remote Communication access for that User or for all Users, or
– the User's authentication instrument.

10.2 Blocking of access at the request of the Bank
(1) The Bank may block the Remote Communication access for a User if
– the Bank is entitled to terminate the Remote Communication agreement for good 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 suspicion of an unauthorised or fraudulent use of the authentication instrument.
(2) The Bank will notify the account/securities account holder by stating the relevant reasons for blocking the access, if possible, before the access is blocked, but at the latest immediately afterwards.

10.3 Unblocking of access
The Bank will unblock the access or exchange the personalised security feature or authentication instrument, if the reasons for blocking the access are no longer applicable. It will notify the account/securities account holder thereof without delay.

10.4 Automatic blocking of a chip-based authentication instrument
(1) The chipcard with signature function blocks itself automatically, if an incorrect signature PIN / code word for the electronic signature is entered three times in succession. The chipcard cannot be enabled by the Bank.
(2) If the check value to enable the HBCI signature is entered incorrectly three times in succession, a blocking of the transmitted signature occurs. The User must generate a new electronic signature and transmit the same to the Bank again.
(3) The incorrect entry of the PIN three times in succession results in the blocking of the access.
(4) The authentication instrument mentioned in para. (1) can then no longer be used for Remote Communication. The User may contact the Bank to restore the possibility of using the Remote Communication.

11. Liability

11.1 Liability of the Bank for an unauthorised drawing via Remote Communication and a non-executed or incorrectly executed drawing via Remote Communication
(1) The Bank's liability for an unauthorised drawing via Remote Communication and a non-executed or incorrectly executed drawing via Remote Communication shall be subject in the first place to No. 11.2 and in the second place to the special conditions applicable for the relevant order type.

11.2 Liability of the account holder in the event of misuse of his authentication instrument
11.2.1 Liability of the account holder for unauthorised payment transactions before a blocking request is given
(1) If unauthorised payment transactions occur before a blocking request is given due to the use of an authentication instrument which has been lost or stolen or become missing otherwise, the account holder shall be liable for the loss incurred by the Bank up to the amount of 150 euros. In this connection it is of no consequence whether or not the loss or theft of the authentication instrument is the User's fault.
(2) If unauthorised payment transactions occur before a blocking request is given due to the misuse of an authentication instrument although the same has been neither lost nor stolen or become missing otherwise, the account holder shall be liable for the loss incurred by the Bank as a result up to an amount of 150 euros, if the User has culpably breached his duty to keep the personalised security features carefully.
(3) If the account holder is not a consumer, he shall be liable for losses due to unauthorised payment transactions in excess of the liability limit of 150 euros specified in para. (1) and (2) up to a maximum of half the amount drawn, provided that the User has negligently or wilfully breached his duties of notification and care in accordance with these Conditions.
(4) The account holder shall not be obliged to refund the loss according to para. (1), (2) and (3) above, if the User was unable to give the blocking request according to No. 9.1 because the Bank had failed to ensure that the blocking request could be received and the loss was incurred as a result.
(5) If unauthorised payment transactions occur before the blocking request is given and the User has breached his/hers duties of care according to these conditions wilfully or by gross negligence or has acted with fraudulent intent, the account holder shall bear the loss resulting therefrom in the full amount. Gross negligence of the User shall exist particularly, if he/she
– fails to notify the Bank of the loss or theft of the authentication instrument or the misuse of the authentication instrument or the personalised security feature as soon as he obtains knowledge thereof (see No. 9.1, para. (1)),
– has stored the personalised security feature in the customer system (see No. 7.2, para. (2), 1st bullet point),
– has disclosed the personalised security feature to another person or made the authentication instrument accessible to a third party and this has caused the misuse (see No. 7.2, para. (1), 2nd bullet point),
– has entered the personalised security feature visibly outside the separately agreed Internet pages (see No. 7.2, para. (2), 3rd bullet point),
– has passed on the personalised security feature outside the Remote Communication procedure, for instance by e-mail (see No. 7.2, para. (2), 4th bullet point),
– has noted the personalised security feature on the authentication instrument or kept it together with it (see No. 7.2, para. (2), 5th bullet point),
– has used more than one TAN for the authorisation of an order (see No. 7.2, para. (2), 6th bullet point), or
– fails to check the order data displayed on his authentication instrument.
(6) The liability for losses caused during the period for which the standard limit or the Remote Communication drawing limit agreed with the customer applies, shall be limited to the amount of the relevant limit.

11.2.2 Liability for unauthorised securities transactions before a blocking request is given
If unauthorised securities transactions occur before a blocking request is given due to the use of a lost or stolen authentication instrument or other misuse of the personalised security feature or authentication instrument, and the Bank has incurred a loss as a result, the account/securities account holder and the Bank shall be liable according to the statutory principles of contributory negligence.

11.2.3 Liability of the Bank after the blocking request is given
As soon as the Bank receives a blocking request by a User, it will bear all losses incurred after the date of the blocking request arising from unauthorised Remote Communication drawings. This shall not apply if the User has acted with fraudulent intent.

11.2.4 Exclusion of liability
Liability claims shall be excluded if the circumstances constituting a claim are due to an extraordinary and unforeseeable event beyond the control of the party which invokes this event and the consequences of which could not have been avoided by it in spite of due and reasonable care being exercised.

12. Data protection

All personal data arising within the scope of the Remote Communication are collected and processed by the Bank and by CommerzService GmbH (CSG)/Dresdner Direkt Service for the purpose of implementing the agreement only within the European Union.