Terms, Conditions and Security Advice for Electronic Banking[1]

Bank of China Ltd. in Germany[2] offers secure and comfortable electronic banking services to the customers. For ensuring security, the electronic banking participant must adhere to the following conditions:

1 Service Offer

The account holder and authorized persons (hereafter: participants) can conduct banking business through electronic banking to the extent offered by the bank. Furthermore they can enquire banking information through electronic banking. The use of electronic banking is subject to the transaction limits agreed with the bank.

2 Conditions for the use of electronic banking

The precondition for participation in the bank's electronic banking is a standard current payment account held at our bank and a valid electronic banking application handed to the bank. To conduct banking business online, the participant requires the personalized security feature (password) and authentication media (e-token) agreed with the bank, in order to identify himself/herself as authorized participant (see no 3.) and to authorize orders (see no.4).

3 Electronicbanking access

The participant is granted access to electronic banking, if

- he/she has submitted the customer ID, the password, the e-token and a captcha verification code
- the evaluation of these data by the bank has proven an access authorization and
- the electronic banking access is not blocked

After the access has been granted, the participant can enquire information or make orders.

1 The Electronic Banking includes Personal Online Banking, Personal Mobile Banking and Corporate Online Banking.

2 Bank of China Ltd. in Germany (hereafter: the bank) includes Bank of China Ltd. Frankfurt, Düsseldorf, Hamburg, Berlin and München Branches.

4 Electronic banking orders

4.1 Placing and authorization of orders

The participant has to authorize electronic banking orders (e.g. remittances) with his password and e-token and submit them to the bank to become effective. The bank confirms the receipt of the order on the electronic banking platform.

4.2 Revocability of orders

The revocability of orders follows the special conditions for the respective order type. Orders can only be revoked outside the electronic banking.

5 Processing of electronic banking orders by the bank

(1) Electronic banking orders are processed on business days within the ordinary course of business for settlement of the respective transaction (e.g. remittance). If the order is received after the acceptance period, or if the order is not received on a business day, then the order is considered to be received on the following business day. Only on this day, the processing takes place.
(2) If the following execution conditions are fulfilled:

- The participant has identified himself by means of the personalized security feature and authentication media
- The participant is entitled for the type of transaction
- The electronic banking data format is adhered to
- The separately agreed electronic banking transaction limit is not breached and
- The conditions for execution applicable to the relevant type of order (e.g. sufficient account balance, correct entry of IBAN and BIC, etc.) have been met

then the bank executes the order.
(3) If the above mentioned conditions for execution are not met, then the bank will not process the electronic banking order and notify the participant through electronic banking of the non-execution and as far as possible about the reasons and possible ways of correcting the errors leading to the non-execution.

6 Transaction limits

For electronic banking orders through which money is transferred to an account outside of the bank the following general transaction limits are established:

- Private customers
  - Maximum EUR 30.000 per transfer
  - Maximum EUR 30.000 per day
- Corporate customers (per transaction type)
  - Maximum EUR 2 million per transfer
  - Maximum EUR 5 million per day

Below these maximum limits, corporate customers can agree individual limits with the bank.

7 Customer information on electronic banking transactions

The bank notifies the customer at least monthly on electronic banking transactions through the agreed channel for account information. Furthermore, the transaction status can be enquired through electronic banking.

8 Electronic banking access

The participant is obliged, to connect to the online banking service exclusively via the internet addresses stated below:

http://www.boc.cn/de ,

http://www.bankofchina.com/de oder

https://ea.ebs.bankofchina.com/login.html?bn=FRA

The participant is obliged, to download the Mobile Banking App only in Google Play Store or Apple App Store.

Note:
If the online banking page is stored as favorite in your browser, please check that really the correct page is displayed.
The certificate of the webpage can be verified by clicking “Tools” >> “Internet Options” >> “Content” >> “Certificates” in the internet explorer.
Please be cautious with regard to fake web pages. If you have any doubt, please immediately contact our below stated service hotline.
Identification methods for fake web pages:
Malicious internet pages use various tricks to appear genuine, e.g.

- Usage of pictures of the real internet page
- Redirection to the real internet page, while the data stream between participant and bank is directed through the malicious page
- Usage of a similar domain name, that can be easily confused with the name stated above

After successful login, a welcome message is displayed. Please make a plausibility check of the displayed last login time. If the time is not as you remember, it could be a fake website/ App.

9 Confidentiality of password and e-token

The participant is obliged to

- Keep his password secretly and only use the above stated access channels to submit it to the bank
- Keep the e-token safe from any access of other persons

Every other person, who has access to the e-token, can in connection with the respective password

abuse the electronic banking services.
In particular, the following shall be respected:

- The password may not be saved electronically (e.g. in the customer's system).
- When entering the password, is must be ensured, that it is not spied out by other persons.
- The password may not be entered on any internet pages outside the online banking (e.g. on pages of online merchants).
- The password may not be transmitted outside from electronic banking, e.g. via email.
- The password may not be stored together with the e-token.
- Easy to guess passwords like birthday, telephone number or car license plate numbers may not be used. Please use hard to guess combinations of numbers and letters as password.
- The participant may not use the same password as for other online services, e.g. email.
- The password must be changed regularly.
- The password should not be written on paper. In case it is written down, the paper must be kept inaccessible for third persons, e.g. in a safe.
- Personal information like user ID and account number may not be disclosed to suspicious or unidentified persons or websites.

10 Safe behavior

The participant may not use the electronic banking service in public places like internet cafés or public libraries. Unknown computers could be infected with malicious software recording your user name and password. Furthermore other persons could spy out your inputs.
Don't open mails with unknown sender. For accessing the online banking page, never use a link contained in an email.
If the participant is leaving the computer during a session or wants to end the session, the log out button must be clicked and the browser must be closed.
The account balance must be checked before and after carrying out a transaction. We recommend checking the account balances regularly. If there are any abnormalities, the service hotline has to be contacted immediately.

11 Security of the customer's system

We recommend setting a password to your PC/ Smart Phone in order to protect the contained information.
The participant has to install a firewall in order to protect the computer against unauthorized access. Furthermore an anti-virus system has to be installed and updated regularly, to protect the computer against viruses.
We recommend downloading only such software from the internet, for which you can be sure, that it is genuine and has not been tampered with. Fraudsters could hide a malicious program within a software, that you download from the internet and install on your computer.
We recommend using Microsoft Internet Explorer as browser.
Updates and security patches of the operating system and the browser have to be installed

regularly.
We recommend deleting the browsing history and the browser cache after ending the electronic banking session, so that your account information is not stored on the computer.
We recommend turning off the "Auto Complete" functionality of your browser, in order to prevent that your access data are stored on the computer:

- Open your internet explorer "Tools" >> "Internet options" >> "Content"
- Choose "Settings" under „Auto Complete"
- Remove the check mark from "User names and passwords on forms"

12 Communication channels of the bank

In case of acute threats, the bank will inform you through the welcome message on the login page of the electronic banking.
In case the bank notices fraudulent transactions or you have reported a suspicion to us, we will inform you by telephone and/or in writing.
The bank will never, except for the above stated login page, ask you in any way to hand over your password.

13 Disclosure and notification obligations of the customer

If the customer notices the loss or theft of his/her e-token or the abuse or other non-authorized usage of the e-token or the password, he/she has to immediately inform the bank about this (Stop Notice).
The participant can give the Stop Notice through the following service hotlines:

- during business hours[3]: +49 69 170090 0
- out of business hours[2]: +49 69 170090 777 (Please connect to a service team member, key combination 1-0-8; the service is available in Chinese and English)

The participant must immediately report any theft or abuse to the police.
In case of suspicions, a Stop Notice has to be given, too.
After becoming aware of any unauthorized or incorrectly executed orders, the customer must inform the bank without undue delay.
Please also inform us, if you become aware of phishing-mails or any fake internet pages using the name of our bank.

14 Blocking

14.1 Blocking at the participant's request

At the participant's request, particularly in the case of a stop notice as set out above, the bank will

- block the electronic banking access for one or all participants of a customer or

[3] Business hours: Monday to Thursday 9:00-12:00 and 13:00-16:00; Friday 9:00-12:00 and 13:00-14:30; closed on Saturday, Sunday and public holidays.

- deactivate the e-token

14.2 Blocking at the bank's request

The bank may block the electronic banking access for a certain participant, if

- the bank is authorized to terminate the electronic banking agreement for good reason
- objective reasons related to the security of the e-token or password are justifying it, or
- an unauthorized or fraudulent transaction is suspected

14.3 Automated blocking

After entering the password incorrectly for 5 times on one day, the electronic banking access will be blocked for the rest of the day. After entering the password incorrectly for a total of 15 times, the electronic banking access is blocked permanently and can only be unblocked by the bank.

14.4 Unblocking

The bank will release the blocking or replace the password or e-token, if the reasons for the blocking are no longer given. On this, the bank informs the account holder without undue delay.
To request unblocking, the participant must contact the above mentioned hotline and hand in the necessary documents in paper.

15 Liabilities

15.1 Liability of the bank for unauthorized or incorrectly executed electronic banking payment transactions

The liability of the bank for unauthorized or incorrectly executed electronic banking payment transactions shall be governed by the agreed special conditions applicable to the type of transaction order.

15.2 Liability of the account holder for misuse of the authentication media

15.2.1 Liability of the account holder for unauthorized transactions prior to the receipt of a Stop Notice

(1) If unauthorized transactions prior to the receipt of a Stop Notice are due to the use of a lost, stolen or otherwise missing e-token, the account holder shall be liable for such damage up to the amount of EUR 50, regardless of whether the participant is at fault for the theft or other loss of the e-token.
(2) If prior to the Stop Notice unauthorized payment transactions are executed without the e-token being lost, stolen or otherwise missing, the account holder shall be liable for such damage up to the amount of EUR 50, if he/she has culpably neglected his/her obligation to safeguard.
(3) If the account holder does not qualify as consumer, he/she is liable for the damages due to unauthorized transactions beyond the limit of 50 EUR according to sub clauses (1) and (2), if the participant has intentionally or negligently violated the obligations to notification and due diligence according to these conditions.
(4) The account holder shall not be obliged to compensate for the damage under sub clauses (1), (2) and (3) if he/she was unable to give the Stop Notice because the bank had not secured the

possibility of receiving the Stop Notice and the damage occurred as a result thereof.
(5) If prior to the Stop Notice unauthorized payment transactions are executed and the participant has intentionally or in gross negligence violated the due diligence obligations according to these conditions or he/she has acted fraudulently, the account holder shall be fully liable for any damages resulting there from.
Gross negligence can exists, if he/she

- has not notified the bank on the loss or theft of the authentication media or on the misuse of the authentication media or the personalized security feature without delay after becoming aware of it,
- has saved the personalized security feature in the customer system,
- has disclosed the personalized security feature to another person and the misuse has been caused by this,
- has entered the personalized security feature recognizably outside the specifically agreed internet pages,
- has transmitted the personalized security feature outside the electronic banking process, e.g. by email, or
- has written the password on the e-token or kept both together.

(6) The liability for losses caused within the period in which a transaction limit is applicable is limited to the respective transaction limit.

15.2.2 Liability of the bank after the Stop Notice

As soon as the bank has received the Stop Notice of a participant, the bank will bear all losses caused by unauthorized electronic banking transactions. This does not apply, if the participant has acted fraudulently.

15.3 Exclusion of liability

Liability claims are excluded, if the circumstances on which the claim is based relate to an abnormal and unforeseeable event beyond the control of the party invoking the event and the consequences could not have been avoided in spite of the exercise of all due diligence.

16 Other

In order to comply with new legal requirements, these terms, conditions and security advices may from time to time be updated. The latest version can always be enquired on the internet page of Bank of China Ltd. Frankfurt Branch. Please read these terms and conditions often, in order to increase your security awareness.
For your information, these terms, conditions and security advices are available in German and Chinese language, too. In case of differences, the German version shall prevail.