Bedingungen und Sicherheitsbestimmungen für das Online Banking

Die Bank of China Ltd. in Deutschland[1] bietet Ihren Kunden sichere und komfortable Online Banking Services. Zur Gewährleistung der Sicherheit müssen Teilnehmer des Online Bankings die folgenden Bedingungen beachten:

1 Leistungsangebot

Der Kontoinhaber und Bevollmächtigte (im Folgenden: Teilnehmer) können Bankgeschäfte mittels Online-Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online-Banking abrufen. Zur Nutzung des Online-Banking gelten die mit der Bank vereinbarten Verfügungslimite.

2 Voraussetzungen zur Nutzung des Online-Banking

Grundvoraussetzung für die Teilnahme am Online Banking ist ein bei der Bank geführtes Standard-Girokonto sowie das Vorliegen eines gültigen Online-Banking-Antrags. Für die Abwicklung von Bankgeschäften mittels Online-Banking benötigt der Teilnehmer das mit der Bank vereinbarte personalisierte Sicherheitsmerkmal (Passwort) und Authentifizierungsinstrument (E-Token), um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4).

[1] Die Bank of China Ltd. in Deutschland (im Folgenden kurz: die Bank) umfasst die Bank of China Ltd. Zweigniederlassungen Frankfurt, Düsseldorf, Hamburg, Berlin, München und Stuttgart.

Terms, Conditions and Security Advice for Online Banking

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

1 Service Offer

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

2 Conditions for the use of online banking

The precondition for participation in the bank's online Banking is a standard current payment account held at our bank and a valid online 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).

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

3 Zugang zum Online-Banking

Der Teilnehmer erhält Zugang zum Online-Banking, wenn

- dieser seine individuelle Kundenkennung, sein Passwort, das E-Token und einen Kaptcha-Verifizierungscode übermittelt hat
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs vorliegt.

Nach Gewährung des Zugangs zum Online-Banking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

3 Online banking access

The participant is granted access to online 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 online banking access is not blocked

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

4 Online-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Online-Banking-Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit mit Passwort und E-Token autorisieren und der Bank mittels Online-Banking übermitteln. Die Bank bestätigt im Online-Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Online-Banking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen. Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen.

4 Online banking orders

4.1 Placing and authorization of orders

The participant has to authorize online 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 online 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 online banking.

5 Bearbeitung von Online-Banking-Aufträgen durch die Bank

(1) Die Bearbeitung der Online-Banking-Aufträge erfolgt an den Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufs für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung). Geht der Auftrag nach der Annahmefrist ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung erfolgt erst an diesem Tag.

(2) Wenn folgende Ausführungsbedingungen vorliegen:

- der Teilnehmer hat sich mit seinem personalisierten Sicherheitsmerkmal und Authentifizierungsinstrument legitimiert
- die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor
- das Online-Banking-Datenformat ist eingehalten
- das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten
- die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung, korrekte Angabe IBAN & BIC) liegen vor

führt die Bank - die Online-Banking-Aufträge aus.

(3) Liegen die oben genannten Ausführungsbedingungen nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen und dem Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Online-Banking eine Information zur Verfügung stellen.

5 Processing of online banking orders by the bank

(1) Online 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 online banking data format is adhered to
- The separately agreed online 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 online banking order and notify the participant through online 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 Transaktionslimite

Für Online-Banking Aufträge, bei denen Geld auf ein Konto außerhalb der Bank überwiesen wird, gelten die folgenden Transaktionslimite:

- Privatkunden:
  - maximal 5.000 EUR pro Überweisung
  - maximal 20.000 EUR pro Tag
- Unternehmenskunden (pro Transaktionsart):
  - maximal 2 Mio. EUR pro Überweisung
  - maximal 5 Mio. EUR pro Tag

Unterhalb von diesen Maximalbeträgen können für Unternehmenskunden kundenindividuelle Limite eingerichtet werden.

6 Transaction limits

For online 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 5.000 per transfer
  - Maximum EUR 20.000 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 Information des Konto-inhabers über Online-Banking-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg. Zudem kann der Status von Online-Banking-Transaktionen im Online-Banking abgefragt werden.

7 Customer information on online banking trans-actions

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

8 Zugang zum Online Banking

Der Teilnehmer verpflichtet sich, die technische Verbindung zum Online Banking nur über die folgenden Internetadressen herzustellen:

http://www.boc.cn/de ,
http://www.bankofchina.com/de oder
https://ea.ebs.bankofchina.com/login.html?bn=FRA

Hinweis:
Sofern Sie die Adresse als Favorit in Ihrem Browser gespeichert haben, prüfen Sie bitte, dass wirklich die korrekte Internetseite angezeigt wird.
Sie können das Zertifikat der Internetseite überprüfen, indem Sie im Internet Explorer „Extras“ >> „Internetoptionen“ >> „Inhalte“ >> „Zertifikate“ auswählen.

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

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.

Bitte nehmen Sie sich in Acht vor gefälschten Internetseiten. Im Zweifelsfall kontaktieren Sie uns bitte sofort durch die unten genannte Hotline.
Identifizierungsmöglichkeiten gefälschter Internetseiten:
Schädliche Internetseiten nutzen verschiedene Tricks, um echt zu erscheinen, z.B.

- Benutzung von Bildern der echten Internetseite
- Umleitung auf die echte Internetseite, wobei der Datenfluss zwischen dem Teilnehmer und der Bank über die gefälschte Internetseite umgeleitet wird
- Benutzung eines ähnlichen Domain-Namens, der leicht mit dem oben angegebenen Domain-Namen verwechselt werden kann

Nach erfolgreichem Login sehen Sie den Begrüßungstext. Bitte prüfen Sie die Plausibilität des angezeigten Zeitpunkts des letzten Logins. Falls der Zeitpunkt nicht Ihrer Erinnung entspricht, könnte es ich um eine gefälschte Internetseite handeln.

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.

9 Geheimhaltung von Passwort und E-Token

Der Teilnehmer hat

- sein Passwort geheim zu halten und nur über oben aufgeführten Internetseiten zur Authentifizierung an die Bank zu übermitteln sowie
- sein E-Token vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des E-Tokens ist, kann in Verbindung mit dem dazugehörigen Passwort das Online-Banking-Verfahren missbräuchlich nutzen.

Insbesondere ist folgendes zu beachten:

- Das Passwort darf nicht elektronisch gespeichert werden (zum Beispiel im Kundensystem).
- Bei Eingabe des Passworts ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.

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 online 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.

- Das Passwort darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (zum Beispiel nicht auf Online-Händlerseiten).
- Das Passwort darf nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Das Passwort darf nicht zusammen mit dem E-Token verwahrt werden.
- Es dürfen keine einfach zu erratenden Passwörter verwendet werden, wie z.B. Geburtstag, Telefonnummer oder Auto-Kennzeichen. Bitte nutzen Sie schwer zu erratende Kombinationen von Buchstaben und Zahlen als Passwort.
- Es darf nicht das gleiche Passwort wie für andere Internet Services, wie z.B. Email, verwendet werden.
- Das Passwort muss regelmäßig geändert werden.
- Das Passwort sollte nicht auf Papier aufgeschrieben werden. Falls das Passwort aufgeschrieben wird, muss das Papier für Dritte unzugänglich verwahrt werden (z.B. Tresor).
- Persönliche Informationen, wie z.B. Benutzerkennung und Kontonummer dürfen nicht verdächtigen oder unidentifizierten Personen oder Internetseiten gegenüber preisgegeben werden.

- 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 online 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 Sicheres Verhalten

Der Teilnehmer darf das Online Banking nicht an öffentlichen Orten wie z.B. Internetcafes oder öffentlichen Bibliotheken benutzen. Fremde Computer könnten mit Schadsoftware infiziert sein, die Ihren Nutzernamen und Ihr Passwort aufzeichnet. Auch Fremde könnten Ihre Eingaben einsehen.
Öffnen Sie keine Mails mit unbekanntem Absender und nutzen Sie für den Zugang zum Online-Banking nie einen Link in einer Mail.
Wenn der Teilnehmer den Computer während einer Online-Banking Session verlässt, oder die Online-Banking-Session beendet, muss er sich durch Click auf den Exit-Button ausloggen und den Browser schließen.

10 Safe behavior

The participant may not use the online 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.

Der Kontostand ist vor und nach der Durchführung von Online Transaktionen zu prüfen. Wir empfehlen auch einen regelmäßigen Check der Kontostände. Bei Auffälligkeiten ist die Hotline der Bank unverzüglich zu informieren.

11 Sicherheit des Kunden-systems

Wir empfehlen, ein Passwort für Ihren Computer zu setzen, um die darin enthaltenen Informationen zu schützen.
Der Teilnehmer muss eine Firewall installieren, um den Computer vor unauthorisiertem Zugriff zu schützen. Außerdem muss ein Anti-Viren-Programm installiert und regelmäßig aktualisiert werden, um den Computer vor Viren zu schützen.
Wir empfehlen, über das Internet nur Software herunterzuladen, von der Sie mit hinreichender Sicherheit feststellen können, ob die Software echt ist und nicht manipuliert wurde. Betrüger könnten eine Schadsoftware in einem anderen Programm, das Sie aus dem Internet herunterladen und auf Ihrem Computer installieren, verbergen.
Wir empfehlen, als Browser Microsoft Internet Explorer zu verwenden.
Updates für das Betriebssystem und Sicherheitspatches des Browsers müssen regelmäßig installiert werden.
Wir empfehlen, bei Beendigung des Online-Bankings den Cache und den Verlauf Ihres Browers zu löschen, so dass Ihre Konteninformationen nicht auf dem Computer gespeichert bleiben.
Wir empfehlen die Funktion „Autovervollständigen“ auszuschalten, um zu verhindern, dass Ihre Zugangsdaten im Computer gespeichert werden:

1. Öffnen Sie den Internet Explorer und wählen Sie Extras >> Internetoptionen >> Inhalte
2. Wählen Sie “Einstellungen“ under “Autovervollständigen ”
3. Löschen Sie in dem Menü das Häkchen vor “Nutzername und Passwort” und klicken Sie „Passwort löschen“ an.

The account balance must be checked before and after carrying out an online 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 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 online 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 Kommunikationskanäle der Bank

Bei akuten Bedrohungen wird die Bank Sie über den Begrüßungstext im Login des Online-Bankings warnen.
Für den Fall, dass die Bank betrügerische Transaktionen feststellt, oder Sie uns gegenüber einen Verdacht angezeigt haben, werden wir Sie telefonisch und/oder schriftlich informieren.
Die Bank wird Sie, außer über die oben angegebene Login-Seite, nie zur Herausgabe Ihres Passworts auffordern.

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 online 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 Anzeige- und Unterrichtungspflichten des Kunden

Stellt der Teilnehmer den Verlust oder den Diebstahl des E-Tokens, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung des E-Tokens oder seines Passwortes fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige).
Der Teilnehmer kann der Bank eine Sperranzeige über die folgenden Hotlines abgeben:

- während der Geschäftszeiten[3]: +49 69 170090 0
- außerhalb der Geschäftszeiten[3]: +49 69 170090 777 (Bitte lassen Sie sich mit einem Mitarbeiter verbinden, Tastenkombination 1-0-8, Service in Englisch und Chinesisch verfügbar.)

Der Teilnehmer hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen.
Bei Verdachtsfällen ist ebenfalls eine Sperranzeige abzugeben.
Nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags ist die Bank unverzüglich hierüber zu unterrichten.

[3] Geschäftszeiten: Montag bis Donnerstag: 09:00 – 12:00 und 13:00 – 16:00; Freitag: 09:00 – 12:00 und 13:00 – 14:30; geschlossen an Samstagen, Sonntagen und gesetzlichen Feiertagen.

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 [4] : +49 69 170090 0
- out of business hours[4]: +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.

[4] 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.

Bitte informieren Sie uns auch falls Sie Phishing-Mails erhalten oder gefälschte Internetseiten sehen, die den Namen unserer Bank verwenden.

Please also inform us, if you become aware of phishing-mails or any fake internet pages using the name of our bank.

14 Nutzungssperre

14.1 Sperre auf Veranlassung des Teilnehmers

Die Bank kann auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige,

- den Online-Banking-Zugang für einen oder alle Teilnehmer eines Kunden sperren oder
- den E-Token deaktivieren.

14.2 Sperre auf Veranlassung der Bank

Die Bank darf den Online-Banking-Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des E-Tokens oder des Passworts dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Transaktion besteht.

Die Bank wird den Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

14.3 Automatisierte Sperre

Bei 5-maliger falscher Eingabe des Passworts am selben Tag wird der Online-Banking-Zugang für den Rest des Tages gesperrt. Nach insgesamt 15 falschen Eingaben des Passworts wird der Online-Banking-Zugang dauerhaft gesperrt, eine Entsperrung kann dann nur durch die Bank erfolgen.

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 online banking access for one or all participants of a customer or
- deactivate the e-token

14.2 Blocking at the bank's request

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

- the bank is authorized to terminate the online 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

The bank will inform the account holder if possible before, but at least immediately after the blocking, stating the reasons for the blocking.

14.3 Automated blocking

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

14.4 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Passwort beziehungsweise das E-Token austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber unverzüglich. Zur Beantragung der Aufhebung einer Sperre muss der Kunde die oben genannte Hotline kontaktieren und die erforderlichen Dokumente schriftlich einreichen.

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 Haftung

15.1 Haftung der Bank bei einer nicht autorisierten und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung

Die Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen.

15.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

15.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungs-vorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen E-Tokens, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,– Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigen Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

15. Liabilities

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

The liability of the bank for unauthorized or incorrectly executed online 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 150, regardless of whether the participant is at fault for the theft or other loss of the e-token.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines E-Tokens, ohne dass dieses verlorengegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,– Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung des Passworts schuldhaft verletzt hat.

(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150,– Euro nach Absatz (1) und (2) hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen (1) , (2) und (3) verpflichtet, wenn der Teilnehmer die Sperranzeige nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(5) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang.

Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er

- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat,
- das personalisierte Sicherheits-merkmal im Kundensystem gespeichert hat,
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde,

(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 150, 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 150 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,

- das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat,
- das personalisierte Sicherheitsmerkmal außerhalb des OnlineBanking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat, oder
- das Passwort auf dem E-Token vermerkt oder zusammen mit diesem verwahrt hat.

(6) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

15.2.2 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-Banking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

15.3 Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

16. Sonstiges

Um mit neuen gesetzlichen Entwicklungen konform zu sein, werden diese Sicherheitsbestimmungen von Zeit zu Zeit aktualisiert. Die neueste Version ist immer auf der Internetseite der Bank of China Ltd. Zweigniederlassung Frankfurt einsehbar. Bitte lesen Sie diese Bedingungen öfters durch, um Ihr Sicherheitsbewusstsein zu erhöhen.
Zu Ihrer Information sind diese Bedingungen und Sicherheitsbestimmungen auch in englischer und chinesischer Sprache verfügbar. Bei Abweichungen gilt die deutsche Version.

- has entered the personalized security feature recognizably outside the specifically agreed internet pages,
- has transmitted the personalized security feature outside the online 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 online 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.