Bedingungen und Sicherheitsbestimmungen für das Electronic Banking[1]

Die Bank of China Ltd. in Deutschland[2] bietet Ihren Kunden sichere und komfortable Electronic Banking Services. Zur Gewährleistung der Sicherheit müssen Teilnehmer des Electronic Bankings die folgenden Bedingungen beachten:

1 Leistungsangebot

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

2 Voraussetzungen zur Nutzung des Electronic-Banking

Grundvoraussetzung für die Teilnahme am Electronic Banking ist ein bei der Bank geführtes Standard-Girokonto sowie das Vorliegen eines gültigen Electronic-Banking-Antrags. Für die Abwicklung von Bankgeschäften mittels Electronic-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).

3 Zugang zum Electronic-Banking

Der Teilnehmer erhält Zugang zum Electronic-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 Electronic-Banking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

1 Das Electronic Banking umfasst Personal Online Banking, Personal Mobile Banking und Corporate Online Banking.

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

4 Electronic-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

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

4.2 Widerruf von Aufträgen

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

5 Bearbeitung von Electronic-Banking-Aufträgen durch die Bank

(1) Die Bearbeitung der Electronic-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 Electronic-Banking-Datenformat ist eingehalten
- das gesondert vereinbarte Electronic-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 Electronic-Banking-Aufträge aus.
(3) Liegen die oben genannten Ausführungsbedingungen nicht vor, wird die Bank den Electronic-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 Electronic-Banking eine Information zur Verfügung stellen.

6 Transaktionslimite

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

- Privatkunden:
  - maximal 30.000 EUR pro Überweisung
  - maximal 30.000 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.

7 Information des Kontoinhabers über Electronic-Banking-Verfügungen

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

8 Zugang zum Electronic 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

Der Teilnehmer verpflichtet sich, die Mobile Banking App nur über Google Play Store or Apple App Store herunterzuladen.

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.
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/ App handeln.

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 Electronic-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.
- Das Passwort darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (zum Beispiel nicht auf Online-Händlerseiten).
- Das Passwort darf nicht außerhalb des Electronic-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.

10 Sicheres Verhalten

Der Teilnehmer darf das Electronic 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 Electronic-Banking nie einen Link in einer Mail.
Wenn der Teilnehmer den Computer während einer Electronic-Banking Session verlässt, oder die Electronic-Banking-Session beendet, muss er sich durch Click auf den Exit-Button ausloggen und den Browser schließen.
Der Kontostand ist vor und nach der Durchführung von Transaktionen zu prüfen. Wir empfehlen auch einen regelmäßigen Check der Kontostände. Bei Auffälligkeiten ist die Hotline der Bank

unverzüglich zu informieren.

11 Sicherheit des Kundensystems

Wir empfehlen, ein Passwort für Ihren Computer/ Smart Phone 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 Electronic-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.

12 Kommunikationskanäle der Bank

Bei akuten Bedrohungen wird die Bank Sie über den Begrüßungstext im Login des Electronic-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.

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[2]: +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.
Bitte informieren Sie uns auch falls Sie Phishing-Mails erhalten oder gefälschte Internetseiten sehen, die den Namen unserer Bank verwenden.

14 Nutzungssperre

14.1 Sperre auf Veranlassung des Teilnehmers

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

- den Electronic-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 Electronic-Banking-Zugang für einen Teilnehmer sperren, wenn
• sie berechtigt ist, den Electronic-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 Electronic-Banking-Zugang für den Rest des Tages gesperrt. Nach insgesamt 15 falschen Eingaben des Passworts wird der Electronic-Banking-Zugang dauerhaft gesperrt, eine Entsperrung kann dann nur durch die Bank erfolgen.

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.

[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.

15 Haftung

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

Die Haftung der Bank bei einer nicht autorisierten Electronic-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Electronic-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 Zahlungsvorgänge 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 50,– Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigen Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

(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 50,– 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 50,– 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 Sicherheitsmerkmal im Kundensystem gespeichert hat,
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde,

- das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat,
- das personalisierte Sicherheitsmerkmal außerhalb des Electronic Banking-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 Electronic-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.