

## Bedingungen für das InternetBanking & Ordering

Fassung 1. November 2009

### 1. Leistungsangebot

(1) Die Bank bietet durch das SEB InternetBanking & Ordering (im Folgenden Online-Banking) den Konto-/Depotinhabern den elektronischen Zugang zu den Kontoinformationen und zur Abwicklung von Bankgeschäften in dem von der Bank vorgegebenen Umfang per Internet unter Verwendung verschiedener Zugangsmedien an. Zudem kann er Informationen der Bank mittels Online-Banking abrufen.

(2) Die Konto-/Depotinhaber sowie deren Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.

(3) Zur Nutzung des Online-Banking gelten die mit der Bank gesondert vereinbarten Verfügungsmittele.

(4) Die Bank ist berechtigt, den Leistungsumfang der angebotenen Bankgeschäfte zu erweitern oder einzuschränken.

(5) Die Bank nimmt keinerlei Beratung vor und gibt für den Verkauf und Kauf von Wertpapieren keinerlei Empfehlungen. Das dem Teilnehmer im Internet zur Verfügung gestellte Informationsmaterial stellt keine individuelle Anlageberatung dar, sondern soll lediglich die selbständige Anlageentscheidung des Teilnehmers erleichtern. Bevor ein Teilnehmer davon Gebrauch macht, sollte der Teilnehmer eingehend prüfen, ob die Informationen mit seinen persönlichen Anlagezielen vereinbar sind.

### 2. Zugangsmedien und Verfahren

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels Online-Banking die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen und Aufträge zu autorisieren.

(1) *Personalisierte Sicherheitsmerkmale*  
Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN) oder
- der Nutzungscode für die elektronische Signatur.

(2) *Authentifizierungsinstrumente*  
Die TAN bzw. die elektronische Signatur können dem Teilnehmer auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:

- auf einer indizierten Liste mit einmal verwendbaren TAN,
- mittels eines TAN-Generators, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist,
- mittels eines mobilen Endgerätes (z.B. Mobiltelefon) zum Empfang von TAN per SMS (mobile TAN),
- auf einer Chipkarte mit Signaturfunktion oder
- auf einem sonstigen Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden.

(3) Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

#### 2.1 InternetBanking & Ordering mit PIN/TAN

(1) Zur Abwicklung von Bankgeschäften per Internet erhält der Teilnehmer von der Bank jeweils einen Aktivierungs-Code sowie eine TAN-Liste.

(2) Der Aktivierungs-Code dient zur erstmaligen Anmeldung und ist ausschließlich für die Vergabe einer vom Teilnehmer zu wählenden PIN geeignet. In den von der Bank im Einzelnen angegebenen Fällen hat der Teilnehmer jeweils zusätzlich eine TAN einzugeben.

(3) Der Teilnehmer hat mittels InternetBanking & Ordering mit PIN/TAN Zugang zum Konto, wenn er zuvor seine Personennummer sowie seine PIN eingegeben hat.

(4) Der Teilnehmer ist berechtigt, seine PIN unter Verwendung einer TAN jederzeit zu ändern. Bei Änderung der PIN wird seine bisherige PIN ungültig.

#### 2.2 InternetBanking & Ordering mit Chipkarte

(1) Die Bank teilt dem Teilnehmer die zur Aufnahme der Verbindung per Online-Banking erforderlichen Zugangsdaten mit. Dabei handelt es sich um

- die Benutzerkennung und
- die Zugangsadresse.

Der Teilnehmer erhält von der Bank als Authentifizierungsinstrument eine Chipkarte. Der Zugriff auf die Chipkarte wird durch eine Chipkarten-PIN (Nutzungscode) geschützt, die vom Teilnehmer im Rahmen der Initialisierung der Karte vergeben wird. Die Chipkarte dient der Speicherung des privaten Schlüssels des Teilnehmers und zur Generierung der digitalen Signatur im Public/Private Key-Verfahren mit Hilfe des Nutzungscode (Chipkarten-PIN). Alle Aufträge, die an die Bank gesandt werden, sind mit dieser digitalen Signatur zu unterschreiben.

(2) Der Teilnehmer muss bei der Initialisierung die Benutzerkennung und die Zugangsadresse auf der Chipkarte speichern. Die Art und Weise der Initialisierung ist abhängig vom eingesetzten Kundenprodukt und Chipkartenleser.

### 3. Zugang zum Online-Banking

(1) Der Teilnehmer erhält Zugang zum Online-Banking, wenn

- dieser seine individuelle Kundenkennung (Personennummer) und seine PIN oder elektronische Signatur übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs vorliegt.

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

### 4. Erteilung, Widerruf und Bearbeitung von Aufträgen im Online-Banking

#### 4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Online-Banking-Aufträge (z.B. Überweisungen) zu deren Wirksamkeit mit den vereinbarten personalisierten Sicherheitsmerkmalen (TAN oder elektronischer Signatur) autorisieren und der Bank mittels Online-Banking übermitteln. Die Bank bestätigt mittels 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 (z.B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Online-Banking ausdrücklich vor.

#### 4.3 Auftragsbearbeitung

(1) Die Bearbeitung der mittels Online-Banking eingereichten Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z.B. Überweisung) auf der Online-Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank angegebenen oder im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat sich mit seinen personalisierten Sicherheitsmerkmalen legitimiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z.B. Wertpapierorder) liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert für die Auftragsart vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z.B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 vor, führt die Bank die Online-Banking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(4) Andernfalls wird die Bank den Online-Banking-Auftrag nicht ausführen und den Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtet werden können, informieren.

## 5. Information des Kontoinhabers 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. Kontoinhaber, die keine Verbraucher sind, informiert die Bank zum vereinbarten Zeitpunkt auf dem vereinbarten Rechnungsabschluss.

## 6. Finanzieller Nutzungsrahmen

(1) Der Teilnehmer darf Verfügungen nur im Rahmen des Kontoguthabens oder eines vorher für das Konto eingeräumten Kredites vornehmen. Auch wenn der Teilnehmer diese Nutzungsgrenze bei seinen Verfügungen nicht einhält, ist die Bank berechtigt, den Ersatz der Aufwendungen zu verlangen, die aus der Nutzung des Online-Banking entstehen. Die Buchung solcher Verfügungen auf dem Konto führt lediglich zu einer geduldeten Kontoüberziehung. Die Bank ist berechtigt, in diesem Fall den höheren Zinssatz für geduldete Kontoüberziehungen zu verlangen.

(2) Bei ausgeführten Wertpapierkaufaufträgen ohne entsprechende Kontodeckung ist die Bank zum Verkauf der erworbenen Wertpapiere berechtigt. Die Bank wird dabei auf die berechtigten Belange des Teilnehmers Rücksicht nehmen.

## 7. Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

Der Teilnehmer hat seine personalisierten Sicherheitsmerkmale geheim zu halten und nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln sowie sein Authentifizierungsinstrument vor dem Zugriff anderer Personen sicher zu verwahren. Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit den dazugehörigen personalisierten Sicherheitsmerkmalen das Online-Banking-Leistungsangebot einschließlich der dem Teilnehmer eingeräumten Anwendungen missbräuchlich nutzen und damit Aufträge zu Lasten des Kontos erteilen.

### 7.1 Geheimhaltung von PIN/TAN

Insbesondere ist Folgendes zur Geheimhaltung von PIN und TAN zu beachten:

- Aktivierungs-Code, PIN und TAN dürfen nicht elektronisch gespeichert werden.
- Die dem Teilnehmer zur Verfügung gestellte TAN-Liste ist sicher und getrennt von der PIN zu verwahren; bei der Eingabe des Aktivierungs-Codes, der PIN und der TAN ist sicherzustellen, dass Dritte diese nicht ausspähen können.
- Der Teilnehmer darf zur Autorisierung z.B. eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung einer neuen TAN-Liste nicht mehr als eine TAN verwenden.
- Aktivierungs-Code, PIN und TAN dürfen nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- PIN und TAN dürfen nicht außerhalb der Online-Banking-Seiten der Bank eingegeben werden (z.B. nicht auf Online-Händlerseiten).
- Beim mobile TAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z.B. Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.

### 7.2 Geheimhaltung von ChipKarte und Nutzungscodes

Insbesondere Folgendes ist zur Geheimhaltung der Chipkarte und des Nutzungscodes (Chipkarten-PIN) zu beachten:

- Die den Teilnehmer identifizierenden Daten dürfen nicht außerhalb der Chipkarte, z.B. auf der Festplatte des Rechners, gespeichert werden.
- Der Nutzungscodes darf nicht notiert oder elektronisch abgespeichert werden.
- Der Nutzungscodes darf nicht zusammen mit der Chipkarte verwahrt werden.
- Duplikate der Chipkarte dürfen nicht erstellt werden.
- Bei Eingabe des Nutzungscodes ist sicherzustellen, dass Dritte dieses nicht ausspähen können.
- Die Chipkarte ist nach Beendigung des Online-Banking aus dem Lesegerät zu entnehmen und sicher zu verwahren.

## 8. Sorgfalts- und Mitwirkungspflichten des Teilnehmers

(1) Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online-Banking nur über die Internetseite der Bank ([www.seb-bank.de](http://www.seb-bank.de)) oder die ihm gesondert mitgeteilten Kommunikationswege herzustellen.

(2) Der Teilnehmer hat sich Gewissheit über die Sicherheit der von ihm benutzten Technik und Software zu verschaffen und Risiken (z.B. Computerviren, Trojaner) im Rahmen des Möglichen (z.B. durch die Installation und Aktualisierung eines handelsüblichen Virenschutzprogramms, einer Firewall und der regelmäßigen Sicherheits-Updates für den von ihm verwendeten Browser) auszuschließen. Weitere zu beachtende Sicherheitshinweise zum Online-Banking erhält der Teilnehmer über die Internetseiten der Bank.

(3) Bei jedem Login in das Online-Banking hat der Teilnehmer das Sicherheitszertifikat zu überprüfen, um sicherzustellen, dass er auch tatsächlich mit der Bank kommuniziert. Bei Auffälligkeiten und Zweifeln an der Echtheit hat der Teilnehmer die Bank unverzüglich hierüber zu informieren.

(4) Der Teilnehmer hat alle von ihm eingegebenen Daten auf Vollständigkeit und Richtigkeit zu überprüfen. Soweit die Bank dem Teilnehmer Daten aus seinem Online-Banking-Auftrag (z.B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

(5) Stellt der Teilnehmer den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seiner personalisierten Sicherheitsmerkmale fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige).

(6) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seiner personalisierten Sicherheitsmerkmale erlangt hat oder das Authentifizierungsinstrument oder die personalisierten Sicherheitsmerkmale verwendet, so muss er ebenfalls eine Sperranzeige abgeben.

(7) Der Teilnehmer hat die Bank unverzüglich nach Feststellung eines nicht autorisierten Auftrags hierüber zu unterrichten.

(8) Der Teilnehmer ist verpflichtet, jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen und dies der Bank nachzuweisen.

## 9. Sperre des Online-Banking-Zugangs

(1) Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige, den Online-Banking-Zugang für ihn. Diese Sperre kann nicht mittels Online-Banking aufgehoben werden. Der Teilnehmer muss sich zur Aufhebung der Sperre mit der Bank in Verbindung setzen.

(2) Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilte zentrale Sperr-Rufnummer abgeben.

(3) 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 Authentifizierungsinstruments oder der personalisierten Sicherheitsmerkmale dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.

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

Auch diese Sperre kann nicht mittels Online-Banking aufgehoben werden. Der Teilnehmer muss sich zur Aufhebung der Sperre mit der Bank in Verbindung setzen.

(4) Die Bank wird eine Sperre aufheben oder die personalisierten Sicherheitsmerkmale beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Teilnehmer unverzüglich.

### 9.1 Automatische Sperre des Authentifizierungsinstruments Chipkarte

Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscodes für die elektronische Signatur falsch eingegeben wird. Die Chipkarte kann dann nicht mehr für das Online-Banking genutzt werden. Der Teilnehmer muss sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

### 9.2 Automatische Sperre des PIN/TAN-Zugangsweges

Wird dreimal hintereinander eine falsche PIN eingegeben, so sperrt die Bank den Internetzugang zum Konto/Depot. Der Teilnehmer kann diese Sperre aufheben, indem er neben der richtigen PIN eine gültige TAN eingibt. Wird viermal hintereinander eine falsche PIN eingegeben, kann der Zugang zum Online-Banking nicht durch den Teilnehmer entsperrt werden. Die Bank sendet dem Teilnehmer in diesem Fall automatisch einen neuen Aktivierungs-Code und eine neue TAN-Liste zu.

Wird dreimal hintereinander eine falsche TAN eingegeben, so werden alle noch nicht verbrauchten TAN für das betreffende Konto/Depot gesperrt. In diesem Fall wird dem Teilnehmer automatisch eine neue TAN-Liste zugesendet.

## 10. Haftung

### 10.1 Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung 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 (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

### 10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

#### 10.2.1 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 abhandengekommenen Authentifizierungsinstruments, 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.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen, gestohlen oder sonst abhandengekommen 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 der personalisierten Sicherheitsmerkmale 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 1-3 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 der personalisierten Sicherheitsmerkmale der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat,
- eines der personalisierten Sicherheitsmerkmale im Kundensystem gespeichert hat,
- eines der personalisierten Sicherheitsmerkmale einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde,

- eines der personalisierten Sicherheitsmerkmale erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat,
- eines der personalisierten Sicherheitsmerkmale außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat,
- eines der personalisierten Sicherheitsmerkmale auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat,
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat,
- beim mobile TAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z.B. Mobiltelefon), auch für das Online-Banking nutzt.

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

#### 10.2.2 Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung der personalisierten Sicherheitsmerkmale oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften der Kontoinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

#### 10.2.3 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.

#### 10.2.4 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.

## 11. Allgemeine Geschäftsbedingungen

Ergänzend zu diesen Bestimmungen, insbesondere in Bezug auf die Änderung der Geschäftsbedingungen und die außergerichtliche Streit-schlichtung und sonstigen Beschwerdemöglichkeiten, gelten die Allgemeinen Geschäftsbedingungen der Bank sowie die für einzelne Geschäftsbeziehungen vorgesehenen Sonderbedingungen und Bedingungen der Bank, insbesondere die Bedingungen für Wertpapiergeschäfte, die Bedingungen für den Scheckverkehr, die Reisescheckbedingungen der American Express Travel Related Services Company Inc. und die Bedingungen für den Überweisungsverkehr.