DigitalBanking Bedingungen

(Stand: 03.04.2018)

1. Leistungsangebot

(1) Der Konto-/Depotinhaber und dessen Bevollmächtigte können Bankgeschäfte mittels Online Banking und Telefon Banking (beides zusammen „Digital-Banking“) in dem von der Bank angebotenen Umfang abwickeln. Für die Abwicklung gelten die Bedingungen für die jeweiligen Bankgeschäfte (z. B. Allgemeine Bedingungen für Zahlungsdienste, Sonderbedingungen für Commerzbank Online Banking Wertpapiergeschäfte, Sonderbedingungen für Wertpapiergeschäfte). Zudem können sie Informationen der Bank mittels DigitalBanking abrufen. Sie sind zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrags im Rahmen des Online Bankings einen Zahlungsauslösedienst gemäß § 1 Absatz 33 Zahlungsdiensteaufsichtsgesetz und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienstleister gemäß § 1 Absatz 34 Zahlungsdiensteaufsichtsgesetz zu nutzen. Die Bank ist berechtigt, dem Konto-/Depotinhaber die Änderung ihrer Geschäftsbedingungen auf elektronischem Weg anzuzeigen und zum Abruf bereitzustellen. Wegen des Wirksamwerdens der Änderungen verbleibt es bei der Regelung in Nummer 1 Abs. 2 der Allgemeinen Geschäftsbedingungen oder den mit dem Kunden vereinbarten abweichenden Regelungen.

(2) Konto-/Depotinhaber und Bevollmächtigte werden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden einheitlich als „Konto“ bezeichnet, es sei denn dies ist ausdrücklich anders bestimmt.

(3) Zur Nutzung des DigitalBankings gelten die Standardlimite oder die mit der Bank gesondert vereinbarten Verfügungslimite für das DigitalBanking.

2. Voraussetzungen zur Nutzung des DigitalBankings

Der Teilnehmer benötigt für die Nutzung des DigitalBankings die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummern 3 und 6) und Aufträge zu autorisieren (siehe Nummer 4). Statt eines Personalisierten Sicherheitsmerkmals kann auch ein biometrisches Merkmal des Teilnehmers zum Zwecke der Authentifizierung bzw. Autorisierung vereinbart werden.

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind Personalisierte Merkmale, die die Bank dem Teilnehmer zum Zwecke der Authentifizierung bereitstellt. Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind beispielsweise:

- die persönliche Identifikationsnummer (PIN),
- der Nutzungscode für die elektronische Signatur,
- einmal verwendbare Transaktionsnummern (TAN),
- die Signatur-PIN/das Kennwort und die Daten des persönlichen elektronischen Schlüssels für die elektronische Signatur.

2.2 Authentifizierungsinstrumente

Authentifizierungsinstrumente sind Personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurden und die vom Teilnehmer zur Erteilung eines DigitalBanking-Auftrags verwendet werden. Insbesondere mittels folgender Authentifizierungsinstrumente kann das Personalisierte Sicherheitsmerkmal (z. B. TAN) dem Teilnehmer zur Verfügung gestellt werden:

- PIN-Brief,
- Liste mit einmal verwendbaren TANs,
- Online Banking-App auf einem mobilen Endgerät (z. B. Mobiltelefon) zum Empfang oder Erzeugung von TAN,
- mobiles Endgerät (z. B. Mobiltelefon) zum Empfang oder Erzeugung von TAN per SMS (mobile TAN),
- einer Grafik, die mit einem von der Bank zugelassenen Lesegerät oder mit einer auf einem mobilen Endgerät (z. B. ein Smartphone) installierten App der Bank entschlüsselt werden kann,
- Chipkarte mit Signaturfunktion oder
- sonstiges Authentifizierungsinstrument, auf dem sich der Signaturschlüssel befindet.

3. Zugang zum Online Banking

Der Teilnehmer erhält Zugang zum Online Banking, wenn

- dieser die Kontonummer oder seine individuelle Teilnehmernummer und seine PIN oder elektronische Signatur oder sein biometrisches Merkmal eingesetzt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 10.1 und 11) vorliegt.

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

Die Sätze 1 und 2 gelten auch, wenn der Teilnehmer Zahlungsaufträge über einen Zahlungsauslösedienst auslöst und Zahlungskontoinformationen über einen Kontoinformationsdienst anfordert (siehe Nummer 1 Absatz 1 Satz 4).

4. Auftragsabwicklung im Rahmen des Online Bankings

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss einen im Rahmen des Online Bankings erteilten Auftrag (z. B. eine Überweisung) zu dessen Wirksamkeit mit dem von der Bank bereitgestellten Personalisierten Sicherheitsmerkmal (z. B. TAN) oder mit dem vereinbarten biometrischen Sicherheitsmerkmal autorisieren und der Bank mittels Online Banking übermitteln. Die Bank bestätigt mittels Online Banking den Eingang des Auftrags. Die Sätze 1 und 2 gelten auch, wenn der Teilnehmer einen Zahlungsauftrag über einen Zahlungsauslösedienst (siehe Nummer 1 Absatz 1 Satz 4) auslöst und übermittelt.

4.2 Meldung nach AWV

Bei Zahlungen zugunsten Gebietsfremder ist die Meldung gemäß Außenwirtschaftsverordnung (AWV) zu beachten.

4.3 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 Bankings erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Online Banking ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der im Rahmen des Online Bankings erteilten Aufträge erfolgt nach den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung oder Wertpapierauftrag) geltenden Regelungen.

(2) Für Zahlungsaufträge (Überweisung, Lastschrift) gelten folgende Sonderregelungen:

Die Bank wird den Zahlungsauftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat den Auftrag autorisiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor.
- Das Online Banking Datenformat ist eingehalten.
- Das gesondert vereinbarte DigitalBanking Verfügungslimit oder das Standardlimit ist nicht überschritten.
- Die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen liegen vor.
- Es ist eine ausreichende Kontodeckung (Guthaben oder eingeräumter Kredit) vorhanden.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank den Zahlungsauftrag nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen aus. Die Ausführung darf nicht gegen sonstige Rechtsvorschriften verstoßen.

(3) Liegen die Ausführungsbedingungen nach Nr. 5.2 Satz 1 1.– 5. Spiegelstrich nicht vor, wird die Bank den Online Banking-Auftrag nicht ausführen. Sie wird dem Teilnehmer hierüber mittels Online Banking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können. Dies gilt nicht, wenn die Angabe von Gründen gegen sonstige Rechtsvorschriften verstößt. Führt die Bank den Auftrag aus, obwohl keine Kontodeckung vorhanden ist, entsteht eine geduldete Kontoüberziehung, für die ein vereinbarter Zins zu zahlen ist.

6. Telefon Banking

Der Teilnehmer erhält Zugang zum Telefon Banking, wenn

- dieser sich unter der ihm mitgeteilten Rufnummer für das Telefon Banking durch Eingabe von Teilnehmernummer und PIN über die Telefontastatur legitimiert 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 Telefon Banking kann der Teilnehmer Informationen erfragen oder Bankgeschäfte vereinbaren.

Der Teilnehmer erteilt seine Zustimmung und autorisiert eine Vereinbarung im Rahmen des Telefon Bankings durch mündliche Bestätigung nach der Wiederholung der Vereinbarung durch einen Mitarbeiter der Bank oder ein Ansagesystem.

7. Information des Kontoinhabers über mittels DigitalBanking erteilte Verfügungen

Die Bank unterrichtet den Kontoinhaber über die mittels Online Banking getätigten Verfügungen im Zahlungsverkehr oder bei Wertpapiergeschäften auf dem für Konto- und Depotinformationen vereinbarten Weg und gemäß den für den Auftrag geltenden Bedingungen.

8. Sorgfaltspflichten des Teilnehmers

8.1 Technische Verbindung zum DigitalBanking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum DigitalBanking über die von der Bank gesondert mitgeteilten DigitalBanking Zugangskanäle (z. B. Internetadresse, Telefonnummer) herzustellen. Zur Erteilung eines Zahlungsauftrags und zum Abruf von Informationen über ein Zahlungskonto kann der Teilnehmer die technische Verbindung zum Online Banking auch über einen Zahlungsauslösedienst beziehungsweise einen Kontoinformationsdienst (siehe Nummer 1 Absatz 1 Satz 4) herstellen.

8.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer hat
– seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten sowie
– sein Authentifizierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit der Kenntnis des dazugehörigen Personalisierten Sicherheitsmerkmals das DigitalBanking Verfahren missbräuchlich nutzen.

Die Geheimhaltungspflicht bezüglich der Personalisierten Sicherheitsmerkmale nach Satz 1 gilt nicht, wenn der Teilnehmer diese zur Erteilung eines Zahlungsauftrags oder zum Abruf von Informationen über ein Zahlungskonto beim Online Banking an den von ihm ausgewählten Zahlungsauslösedienst beziehungsweise Kontoinformationsdienst übermittelt (siehe Nummer 1 Absatz 1 Satz 4).

(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:
– Das Personalisierte Sicherheitsmerkmal darf nicht ungesichert elektronisch gespeichert werden. Der vom Teilnehmer erzeugte persönliche elektronische Schlüssel darf sich nur in der alleinigen Verfügungsgewalt des Teilnehmers befinden.
– Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
– Das Personalisierte Sicherheitsmerkmal darf nicht per E-Mail weitergegeben werden.
– Das Personalisierte Sicherheitsmerkmal (z. B. PIN) darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
– Der Teilnehmer darf zur Autorisierung eines Auftrags oder zur Aufhebung einer Sperre nicht mehr als eine TAN verwenden. Zwei TANs sind lediglich zu verwenden, wenn die TAN-Liste gewechselt wird. Hier muss der Teilnehmer eine TAN aus der alten TAN-Liste eingeben und eine TAN aus der neuen TAN-Liste.
– Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen wird (z. B. Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.
– Die App der Bank zur Entschlüsselung der TAN-Grafik ist direkt von der Bank oder von einem von der Bank dem Kunden benannten Anbieter zu beziehen.
– Sofern PIN und die Teilnehmernummer vom Telefon des Teilnehmers automatisch gespeichert werden (z. B. Wahlwiederholungsfunktion des Telefons), sind, soweit technisch möglich, die gespeicherten Ziffernfolgen zu löschen oder zu überschreiben.

8.3 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise auf der Internetseite der Bank zum DigitalBanking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

8.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem Online Banking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z. B. Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

9. Ein- und Ausfuhr von Software im Ausland

In Ländern, in denen Nutzungs oder Einfuhr- und Ausfuhrbeschränkungen für Verschlüsselungstechniken bestehen, darf eine von der Bank zur Verfügung gestellte Software nicht verwendet werden.

10. Anzeige und Unterrichtungspflichten

10.1 Sperranzeige

(1) Stellt der Teilnehmer
– den Verlust oder den Diebstahl des Authentifizierungsinstruments,
– die missbräuchliche Verwendung oder
– die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder eines seiner persönlichen Sicherheitsmerkmale fest,

muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen.

(3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt
– den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder
– das Authentifizierungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet,

muss er ebenfalls eine Sperranzeige abgeben.

10.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Konto-/Depotinhaber hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

11. Nutzungssperre

11.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 10.1,
– den DigitalBanking-Zugang für ihn oder alle Teilnehmer oder
– sein Authentifizierungsinstrument.

11.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den DigitalBanking-Zugang für einen Teilnehmer sperren, wenn
– sie berechtigt ist, den DigitalBanking-Vertrag aus wichtigem Grund zu kündigen,
– sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
– der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.

(2) Die Bank wird den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre in Textform (z. B. mittels Brief, Telefax oder E-Mail) oder telefonisch unterrichten.

11.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber unverzüglich.

11.4 Automatische Sperre eines chipbasierten Authentifizierungsinstruments sowie DigitalBanking-Zugang mittels PIN und TAN

(1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur falsch eingegeben wird. Eine Freischaltung der Chipkarte durch die Bank ist nicht möglich.

(2) Wenn der Kontrollwert zur Freigabe der HBCI-Signatur dreimal falsch eingegeben wird, kommt es zur Sperrung der übermittelten Signatur. Der Teilnehmer muss eine neue elektronische Signatur erstellen und diese erneut an die Bank übermitteln.

(3) Die dreimalige Falscheingabe des PIN führt zu einer Sperre des DigitalBanking-Zugangs.

(4) Das im Absatz 1 genannte Authentifizierungsinstrument kann dann nicht mehr für das DigitalBanking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des DigitalBankings wiederherzustellen.

12. Haftung[1]

12.1 Haftung der Bank bei einer nicht autorisierten Online Banking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Online Banking-Verfügung

Die Haftung der Bank bei einer nicht autorisierten Online Banking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Online Banking-Verfügung richtet sich vorrangig nach Nummer 12.2 und nachrangig nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen.

12.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung eines Personalisierten Sicherheitsmerkmals oder eines Authentifizierungsinstruments

12.2.1 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 oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungsinstruments, 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 ein Verschulden trifft.

(2) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach dem Absatz 1 verpflichtet, wenn

- es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungsinstruments vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Authentifizierungsinstruments durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Anzeige und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von den Absätzen 1 und 2 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 (siehe Nummer 10.1 Absatz 1),
- das Personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe Nummer 8.2 Absatz 2 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 8.2 Absatz 1),
- das Personalisierte Sicherheitsmerkmal per E-Mail weitergegeben hat (siehe Nummer 8.2 Absatz 2 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 8.2 Absatz 2 4. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 8.2 Absatz 2 5. Spiegelstrich),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen wird (z. B. Mobiltelefon), auch für das Online Banking nutzt (siehe Nummer 8.2 Absatz 2 6.Spiegelstrich),
- die App der Bank zur Entschlüsselung der TAN-Grafik nicht direkt von der Bank oder von einem Anbieter bezieht, der dem Kunden von der Bank benannt wurde (siehe Nummer 8.2 Absatz 2 7.Spiegelstrich) oder
- die auf seinem Authentifizierungsinstrument angezeigten Auftragsdaten nicht prüft.

(4) Abweichend von den Absätzen 1 und 3 ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt, obwohl die Bank zur starken Kundenauthentifizierung nach § 68 Absatz 4 Zahlungsdiensteaufsichtsgesetz verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, was der Teilnehmer weiß, z. B. PIN), Besitz (etwas, das der Teilnehmer besitzt, z. B. TAN-Generator) oder Inhärenz (etwas, das der Teilnehmer ist, z. B. Fingerabdruck).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Standardlimit oder das mit dem Kunden vereinbarte DigitalBanking-Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf diese Limite.

(6) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz (1) und (3) verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 9.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(7) Die Absätze 2 und 4 bis 6 gelten nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(8) Ist der Kontoinhaber kein Verbraucher, gilt ergänzend Folgendes:

- Der Kontoinhaber haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro in Absatz (1) hinaus, wenn der Teilnehmer fahrlässig gegen seine Anzeige und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- Die Haftungsbeschränkungen in Absatz (2) erster Spiegelstrich finden keine Anwendung.

12.2.2 Haftung des Depotinhabers 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 des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften der Depotinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

12.2.3 Haftung der Bank ab der Sperranzeige

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

12.2.4 Haftung beim Telefon Banking

Bis zur Sperranzeige haftet der Kunde außer in den Fällen nach Absatz 12.1 und 12.2 nach den rechtlichen Regelungen für vorsätzliches und fahrlässiges Verhalten unter Berücksichtigung eines eventuellen Mitverschuldens der Bank.

12.2.5 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.

13. Datenschutz

Alle im Rahmen von Commerzbank DigitalBanking entstehenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und der Commerz Direktservice GmbH nur innerhalb der Europäischen Union erhoben und verarbeitet.

Commerzbank AG

[1] Ergänzend gelten die Regelungen der Sicherheits-Garantie der Bank.

Sonderbedingungen für Commerzbank Online Banking Wertpapiergeschäfte

Ergänzend zu den DigitalBanking Bedingungen gelten für Commerzbank Online Banking Wertpapiergeschäfte die nachfolgenden Sonderbedingungen:

1. Leistungsbeschreibung

Der Teilnehmer kann bei Wertpapiergeschäften mittels Online Banking im Rahmen der bestehenden Geschäftsbeziehung gegenüber der Bank folgende Willenserklärungen abgeben:

– Erteilung von Aufträgen zum Kauf bzw. Verkauf von Wertpapieren über das bei der Bank geführte Depot nach Maßgabe der Ziffer 2. dieser Bedingungen. Zusätzlich kann der Teilnehmer bei Wertpapiergeschäften mittels Online Banking nachstehende Informationen abrufen:
– aktueller Depotbestand
– Wertpapierkennnummer-Orderbuchanzeige

Bei Wertpapiergeschäften mittels Online Banking erbringt die Bank keine individuelle, auf die persönlichen Bedürfnisse des Teilnehmers zugeschnittene Anlageberatung. Der Teilnehmer trifft, ggf. gestützt auf die zur Verfügung gestellten Informationen und Research-Studien, eine selbstständige Anlageentscheidung. Wünscht der Teilnehmer eine individuelle Beratung, so kann er sich an den Kundenbetreuer wenden. Die Bank wird bei Wertpapiergeschäften mittels Online Banking den Auftrag des Teilnehmers nach § 31 Abs. 5 Wertpapierhandelsgesetz lediglich auf seine Angemessenheit hin überprüfen und den Teilnehmer gegebenenfalls vor Auftragsausführung auf die Unangemessenheit der Order hinweisen. Die Verrechnung der Gegenwerte erfolgt ausschließlich über die bei der Bank für die Nutzung von Online Banking vorgesehenen Konten.

2. Kenntnisstufe

Aufgrund seiner Angaben nach § 31 Abs. 5 Wertpapierhandelsgesetz (WpHG-Bogen) erhält der Teilnehmer eine persönliche Kenntnisstufe. Er kann Aufträge nur innerhalb dieser ihm gegenüber bekannt gegebenen Kenntnisstufe erteilen. Über die Kenntnisstufe hinausgehende Aufträge werden systemseitig nicht angenommen. Sofern der Teilnehmer keine oder nur unvollständige Angaben nach § 31 Abs. 5 Wertpapierhandelsgesetz macht, wird die Bank Aufträge zum Kauf von Wertpapieren nur innerhalb der niedrigsten Kenntnisstufe entgegennehmen.

3. Ordererteilung

Aufträge zum Kauf bzw. Verkauf von Wertpapieren sind erst dann vom Teilnehmer erteilt, wenn er die von der Bank erhaltene Rückmeldung im Bildschirmdialog gegenüber der Bank mittels Eingabe einer Transaktionsnummer (TAN) oder Verwendung einer elektronischen Signatur und anschließender Freigabe bestätigt hat.

4. Orderänderung/Orderlöschung

Aufträge zum Kauf bzw. Verkauf von Wertpapieren können vom Teilnehmer nachträglich nur geändert oder gelöscht werden, sofern der ursprüngliche Auftrag zwischenzeitlich noch nicht ausgeführt wurde. Dem Teilnehmer wird systemseitig angezeigt werden, ob eine Orderänderung/Orderlöschung noch akzeptiert werden konnte.

5. Orderhöchstbetrag

Der Teilnehmer kann bei Wertpapiergeschäften mittels Online Banking aus Sicherheitsgründen nur innerhalb eines vereinbarten Höchstbetrages pro Order Wertpapiere erwerben. Auf der Grundlage des zuletzt systemseitig verfügbaren Wertpapierkurses bzw. des vom Kunden erteilten Limits überprüft die Bank bei jeder Wertpapiertransaktion die Ausnutzung des Höchstbetrages. Ist eine Überschreitung des Höchstbetrages pro Order gewünscht, kann sich der Teilnehmer an seinen Kundenbetreuer wenden und seinen Auftrag außerhalb des Online Bankings erteilen.

6. Ausführungsplatz

Bei der Ordererteilung wird dem Teilnehmer ein Ausführungsplatz in Einklang mit den Ausführungsgrundsätzen der Bank vorgeschlagen. Der Teilnehmer hat die Möglichkeit, einen anderen Ausführungsplatz zu bestimmen; in diesem Fall wird die Bank den Auftrag nicht gemäß ihren Ausführungsgrundsätzen ausführen. Der Teilnehmer schließt mit der Bank Wertpapiergeschäfte in Form von Kommissionsgeschäften (dazu Ziffer 7. dieser Bedingungen) oder Festpreisgeschäften (dazu Ziffern 8. und 9. dieser Bedingungen) ab.

7. Preis des Ausführungsgeschäfts im Kommissionsgeschäft

Beauftragt der Teilnehmer die Bank zur Durchführung der Wertpapierorder im Wege des Kommissionsgeschäfts, wird dem Teilnehmer ein Kurswert der disponierten Wertpapiere angezeigt. Dieser angezeigte Betrag beruht auf dem zuletzt verfügbaren Kurs aus den Datenbeständen der Bank und dient lediglich als unverbindliche Orientierungsgröße für den Kunden. Der Preis des Ausführungsgeschäfts wird erst mit der Orderausführung an dem Handelsplatz nach den dort jeweils geltenden Preisfeststellungsregeln bestimmt; der endgültige Abrechnungsbetrag enthält zusätzlich das Entgelt der Bank sowie etwaige ihr in Rechnung gestellte fremde Kosten, soweit diese nach gesetzlichen Vorschriften zu ersetzen sind.

8. Auftragserteilung im Festpreisgeschäft

Vereinbaren Kunde und Bank für ein Geschäft einen festen Preis, so kommt ein außerbörslicher Kaufvertrag zwischen Kunde und Bank zustande. Zu diesem Zweck nennt die Bank für die Wertpapiere Preisindikationen, die laufend kurzfristig aktualisiert werden. Der Teilnehmer kann der Bank auf Grundlage dieser Preisindikationen den Abschluss eines Festpreisgeschäfts antragen. Sofern die Bank dieses Angebot annimmt, wird die Bank dem Teilnehmer eine Annahmeerklärung anzeigen.

9. Korrektur von Festpreisgeschäften durch die Bank (Mistrade-Regelung)

Der Bank steht ein vertragliches Aufhebungsrecht für den Fall zu, dass der außerbörsliche Kaufvertrag zu einem nicht marktgerecht gebildeten Preis zustande kam (Mistrade). Ein Mistrade liegt vor, wenn der Preis erheblich und offenkundig von dem zum Zeitpunkt des Abschlusses des Festpreisgeschäfts marktgerechten Referenzpreis abweicht. Als Ursache für einen Mistrade kommen entweder Fehler im technischen System der Bank sowie ihrer Vertragspartner oder Fehler bei der Eingabe einer Preisindikation in Betracht. Als Referenzpreis des Wertpapieres gilt der Durchschnittspreis der letzten drei vor dem fraglichen Festpreisgeschäft in einem börslichen oder außerbörslichen Handelssystem zustande gekommenen Geschäfte in dem fraglichen Wertpapier. Ist kein Durchschnittspreis zu ermitteln, so ermittelt die Bank den Referenzpreis nach billigem Ermessen mittels allgemein anerkannter und marktüblicher Berechnungsmethoden. Als erhebliche und offenkundige Abweichung von dem marktgerechten Referenzpreis gilt bei Geschäftsabschlüssen

(1) in stücknotierten Wertpapieren bei einem Referenzpreis über EUR 0,40 eine Abweichung von mindestens 10 % oder mehr als EUR 2,50, bei einem anderen Referenzpreis eine Abweichung von mindestens 25 % oder mehr als EUR 0,10;
(2) in Wertpapieren, die in Prozent notiert werden, bei einem Referenzpreis ab 101,50 % eine Abweichung von mindestens 2,5 Prozentpunkten, bei einem Referenzpreis zwischen 60 % und bis zu unter 101,50 % eine Abweichung von mindestens 2 Prozentpunkten, bei einem Referenzpreis zwischen 30 % und bis zu unter 60 % eine Abweichung von mindestens 1,25 Prozentpunkten, bei einem Referenzpreis unter 30 % eine Abweichung von mindestens 1 Prozentpunkt.

Die Bank macht ihr Aufhebungsverlangen am Tage des Mistrades geltend. Die Bank verzichtet auf ihr Aufhebungsrecht, wenn die Schadenssumme EUR 500,– nicht erreicht. Dem Kunden steht kein Anspruch auf Ersatz etwaiger im Vertrauen auf den Bestand des aufgehobenen Festpreisgeschäfts erlittener Schäden zu.

10. Informationen/Research-Studien

Die systemseitig zur Verfügung gestellten Informationen, Wertpapierstammdaten und Wertpapierkurse bezieht die Bank aus öffentlich zugänglichen Quellen und von Dritten, die sie für zuverlässig hält. Eine Garantie für die Richtigkeit oder Vollständigkeit der Angaben kann die Bank nicht übernehmen. Research-Studien geben, soweit sie Meinungsäußerungen enthalten, die Einschätzung eines der Research-Teams der Bank wieder. Eine individuelle Anlageempfehlung ist damit nicht verbunden und sie ersetzen keine Anlageberatung.

Besondere Verpflichtungen des Teilnehmers

– Der Teilnehmer verpflichtet sich, bei Wertpapiergeschäften mittels Online Banking nur innerhalb des Kontoguthabens oder eingeräumter Kreditlinien zu verfügen. Er wird evtl. aus der Ausführung von Wertpapieraufträgen entstandene Überziehungen unverzüglich zurückführen.
– Vor Freigabe der Order hat sich der Teilnehmer zu vergewissern, dass er die Wertpapierkennnummer, die Stückzahl, die Gültigkeit und die betragsmäßige Limitierung seiner Order korrekt in das System eingestellt hat.
– Bei dem Abruf von Research-Studien hat der Teilnehmer das Erstellungsdatum zu beachten. Danach eingetretene Ereignisse sind in der Studie nicht berücksichtigt.

Benötigt der Teilnehmer ergänzende aktuelle Informationen, kann er sich an den Kundenbetreuer wenden.

Ergänzend gelten die „Allgemeinen Geschäftsbedingungen“ und die „Sonderbedingungen für Wertpapiergeschäfte“.

Commerzbank AG

22/67/20 – HD1018