COMMERZBANK

Antrag zum photoTAN- und mobileTAN-Verfahren

Unser technischer Support am Telefon:
☎ 069 98 66 00 33
Wir sind jeden Tag 24 h für Sie da.
www.commerzbank.de

Persönlich/Vertraulich

Commerzbank AG
Geschäftsabwicklung Online Banking
59067 Hamm

Weitere Informationen unter
www.commerzbank.de/TAN-Verfahren

Daten des DigitalBanking-Teilnehmers

Vorname Nachname _____ Geburtsdatum _____

Straße, Hausnummer _____

PLZ _____ Ort _____

Teilnehmernummer _____ Kontonummer _____ BLZ _____

Bitte führen Sie die unten angekreuzten Aufträge für mich aus. Die Ausführung soll alle bestehenden und zukünftigen Konten und Depots zu allen Kundennummern umfassen, auf die ich unter der o.g. Teilnehmernummer als Kontoinhaber oder Bevollmächtigter zugreife.
Falls ich bisher für das iTAN-Verfahren freigeschaltet bin, wird dieses nach 30 Tagen gesperrt, sobald ich die photoTAN oder die mobileTAN beantragt habe.

photoTAN-Verfahren

Anmeldung zur photoTAN oder erneute Aktivierung

☐ Ich möchte das **kostenlose photoTAN-**Verfahren nutzen. Senden Sie mir dazu den entsprechenden Aktivierungsbrief zu.
Für das Verfahren ist ein unterstütztes Smartphone mit der photoTAN-App der Commerzbank (www.commerzbank.de/photoTAN) oder ein separates Commerzbank-Lesegerät erforderlich.

Bestellung eines Lesegeräts für das photoTAN-Verfahren (falls gewünscht)

☐ Ich bestelle _____ **Lesegeräte** für das photoTAN-Verfahren zum Stückpreis von 29,90 Euro inkl. MwSt. und Versand an die bei der Bank hinterlegte Postanschrift. Der Gesamtbetrag soll von folgendem Commerzbank-Konto, über das ich alleine verfügen kann, abgebucht werden:

BLZ/BIC: _____ Kontonummer/IBAN: _____

Als Rechnung dient die Umsatzanzeige auf dem Kontoauszug. Bis zur vollständigen Bezahlung des Kaufpreises bleibt die Ware im Eigentum der Bank. Versand und Reklamationsbearbeitung erfolgen durch die Bank-Verlag GmbH, Wendelinstr. 1, 50933 Köln.

Sperrung/Entsperrung/Deaktivierung des photoTAN-Verfahrens

☐ **Sperren** Sie bis auf Widerruf meine **photoTAN.** ☐ **Entsperren** Sie meine **photoTAN.**
☐ **Deaktivieren** Sie meine photoTAN, ich möchte diese nicht länger nutzen.

mobileTAN-Verfahren

Anmeldung zur mobileTAN oder Änderung Ihrer Mobilfunknummer

☐ Ich möchte das **mobileTAN**-Verfahren mit meinem Handy nutzen. Senden Sie mir dazu den entsprechenden Aktivierungsbrief. Für die mobileTAN möchte ich folgende Mobilfunknummer verwenden:

Mobilfunknummer Vorwahl _____ Rufnummer _____

Sperrung/Entsperrung/Deaktivierung des mobileTAN-Verfahrens

☐ **Sperren** Sie bis auf Widerruf meine **mobileTAN.** ☐ **Entsperren** Sie meine **mobileTAN.**
☐ **Deaktivieren** Sie meine **mobileTAN,** ich möchte diese nicht länger nutzen.

Es gelten die Bedingungen für das DigitalBanking und die Sonderbedingungen für Commerzbank Online Banking Wertpapiergeschäfte.

Unterschrift des Teilnehmers:

Ort, Datum _____ _____

Unterschrift X _____

Vermerke für Bank

Unterschrift(en) geprüft
oder Sicherungsstempel _____

6838/09/25 – HD0418

COMMERZBANK

Antrag zum photoTAN- und mobileTAN-Verfahren

Unser technischer Support am Telefon:
☎ 069 98 66 00 33
Wir sind jeden Tag 24 h für Sie da.
www.commerzbank.de

Persönlich/Vertraulich

Commerzbank AG
Geschäftsabwicklung Online Banking
59067 Hamm

Weitere Informationen unter
www.commerzbank.de/TAN-Verfahren

Daten des DigitalBanking-Teilnehmers

Vorname Nachname _____ Geburtsdatum _____

Straße, Hausnummer _____

PLZ _____ Ort _____

Teilnehmernummer _____ Kontonummer _____ BLZ _____

Bitte führen Sie die unten angekreuzten Aufträge für mich aus. Die Ausführung soll alle bestehenden und zukünftigen Konten und Depots zu allen Kundennummern umfassen, auf die ich unter der o.g. Teilnehmernummer als Kontoinhaber oder Bevollmächtigter zugreife.
Falls ich bisher für das iTAN-Verfahren freigeschaltet bin, wird dieses nach 30 Tagen gesperrt, sobald ich die photoTAN oder die mobileTAN beantragt habe.

photoTAN-Verfahren

Anmeldung zur photoTAN oder erneute Aktivierung

☐ Ich möchte das **kostenlose photoTAN-**Verfahren nutzen. Senden Sie mir dazu den entsprechenden Aktivierungsbrief zu.
Für das Verfahren ist ein unterstütztes Smartphone mit der photoTAN-App der Commerzbank (www.commerzbank.de/photoTAN) oder ein separates Commerzbank-Lesegerät erforderlich.

Bestellung eines Lesegeräts für das photoTAN-Verfahren (falls gewünscht)

☐ Ich bestelle _____ **Lesegeräte** für das photoTAN-Verfahren zum Stückpreis von 29,90 Euro inkl. MwSt. und Versand an die bei der Bank hinterlegte Postanschrift. Der Gesamtbetrag soll von folgendem Commerzbank-Konto, über das ich alleine verfügen kann, abgebucht werden:

BLZ/BIC: _____ Kontonummer/IBAN: _____

Als Rechnung dient die Umsatzanzeige auf dem Kontoauszug. Bis zur vollständigen Bezahlung des Kaufpreises bleibt die Ware im Eigentum der Bank. Versand und Reklamationsbearbeitung erfolgen durch die Bank-Verlag GmbH, Wendelinstr. 1, 50933 Köln.

Sperrung/Entsperrung/Deaktivierung des photoTAN-Verfahrens

☐ **Sperren** Sie bis auf Widerruf meine **photoTAN.** ☐ **Entsperren** Sie meine **photoTAN.**
☐ **Deaktivieren** Sie meine photoTAN, ich möchte diese nicht länger nutzen.

mobileTAN-Verfahren

Anmeldung zur mobileTAN oder Änderung Ihrer Mobilfunknummer

☐ Ich möchte das **mobileTAN**-Verfahren mit meinem Handy nutzen. Senden Sie mir dazu den entsprechenden Aktivierungsbrief. Für die mobileTAN möchte ich folgende Mobilfunknummer verwenden:

Mobilfunknummer Vorwahl _____ Rufnummer _____

Sperrung/Entsperrung/Deaktivierung des mobileTAN-Verfahrens

☐ **Sperren** Sie bis auf Widerruf meine **mobileTAN.** ☐ **Entsperren** Sie meine **mobileTAN.**
☐ **Deaktivieren** Sie meine **mobileTAN,** ich möchte diese nicht länger nutzen.

Es gelten die Bedingungen für das DigitalBanking und die Sonderbedingungen für Commerzbank Online Banking Wertpapiergeschäfte.

Unterschrift des Teilnehmers:

Ort, Datum _____ _____

Unterschrift X _____

6838/09/25 – HD0418

Digital Banking Bedingungen

(Stand: 14.09.2019)

1. Leistungsangebot

(1) Der Kunde 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 Digital Banking abrufen. Des Weiteren sind sie gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absätze 33 und 34 Zahlungsdiensteaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen. Die Bank ist berechtigt, dem Kunden 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) Kunde und Bevollmächtigte werden einheitlich als „Teilnehmer", Konto und Depot einheitlich als „Konto" bezeichnet, es sei denn dies ist ausdrücklich anders bestimmt.

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

2. Voraussetzungen zur Nutzung des Digital Banking

(1) Der Teilnehmer kann das Digital Banking nutzen, wenn die Bank ihn authentifiziert hat.

(2) Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers prüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummern 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen

(3) Authentifizierungselemente sind

- Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer [PIN])
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN]) oder,
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

(4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelements und / oder den Nachweis des Seinselements an die Bank übermittelt.

3. Zugang zum Online Banking

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

- er seine individuelle Teilnehmernummer (z. B. Kontonummer, Anmeldename) angibt und
- er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (siehe Nummern 10.1 und 11 dieser Bedingungen) vorliegt. Nach Gewährung des Zugangs zum Online Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge erteilt werden.

(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Abs. 26 Satz 1 ZAG (z. B. zum Zweck der Änderung der Anschrift des Kunden) fordert die Bank den Teilnehmer auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Online Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kontoinhabers und die Kontonummer sind für den vom Teilnehmer genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Zahlungsdaten (§ 1 Abs. 26 Satz 2 ZAG).

4. Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss einen Auftrag (zum Beispiel Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (zum Beispiel Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden. Die Bank bestätigt mittels Online Banking den Eingang des Auftrags.

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 Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Allgemeine Bedingungen für Zahlungsdienste). 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 Aufträge erfolgt nach den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung oder Wertpapierauftrag) geltenden Regelungen.

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

- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1. dieser Bedingungen.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (zum Beispiel Wertpapierorder) liegt vor.
- Das Online Banking Datenformat ist eingehalten.
- Das gesondert vereinbarte Digital Banking Verfügungslimit oder das Standardlimit ist nicht überschritten (vgl. Nummer 1 Absatz 3 dieser Bedingungen).
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Allgemeinen Bedingungen für Zahlungsdienste) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel gemäß den Allgemeinen Bedingungen für Zahlungsdienste, Bedingungen für Wertpapiergeschäft) aus. Die Ausführung darf nicht gegen sonstige Rechtsvorschriften verstoßen.

(3) Liegen die Ausführungsbedingungen nach Satz 1 nicht vor, wird die Bank den 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.

22/67/20 – HD0322-01

7. Information des Kunden über Digital Banking Verfügungen

Die Bank unterrichtet den Kunden mindestens einmal monatlich 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 Schutz der Authentifizierungselemente

(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungelemente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Digital Banking Verfahren missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummer 3 und 4 dieser Bedingungen).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

(a) Wissenselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere

- nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden
- nicht außerhalb des Digital Banking in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben werden
- nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. mobiles Endgerät) oder zur Prüfung des Seinselementes (z. B. mobiles Endgerät mit Anwendung für das Online Banking und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z. B. ein mobiles Endgerät sind vor Missbrauch zu schützen

- ist sicherzustellen, dass unberechtigte Personen auf dem mobilen Endgerät (z. B. Mobiltelefon) nicht zugreifen können,
- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für das Online Banking (z. B. Online-Banking-App, Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für das Online Banking (z. B. Online-Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons),
- dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und
- muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das Online Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online Banking des Teilnehmers aktivieren.

(c) Seinselemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Online Banking das von der Bank ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (z. B. Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden. Die für das mobileTAN-Verfahren hinterlegte Telefonnummer ist zu löschen
oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Online Banking nicht mehr nutzt.

(4) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 4 darf der Teilnehmer seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden (siehe Nummer 1 Absatz 1 Sätze 4 und 5 dieser Bedingungen). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

(5) 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.

(6) 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.

8.2 Sicherheitshinweise der Bank

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

8.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (zum Beispiel mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag 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 eines Besitzelements zur Authentifizierung (z. B. mobiles Endgerät) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungselements

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

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

(3) Hat der Teilnehmer den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente,
muss er ebenfalls eine Sperranzeige abgeben.

10.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Kunde 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 dieser Bedingungen,

- den Digital Banking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument zur Nutzung des Digital Banking.

11.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Digital Banking-Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den Digital Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungselements des Teilnehmers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des eines Authentifizierungselements besteht.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre schriftlich, in Textform (z. B. mittels, Telefax oder E-Mail) oder telefonisch unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

11.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

11.4 Automatische Sperre eines chip-basierten Besitzelements sowie des Digital Banking-Zugang mittels PIN und TAN

(1) Eine 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 Digital Banking-Zugangs.

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

11.5 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Kunden verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Bank wird den Kunden über eine solche Zugangsverweigerung auf dem vereinbarten Weg unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Bank die Zugangssperre auf. Hierüber unterrichtet sie den Kunden unverzüglich.

12. Haftung[1]

12.1 Haftung der Bank bei Ausführung eines nicht autorisierten Online Banking Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Bank bei einem nicht autorisierten Auftrag und einer nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich vorrangig nach Nummer 12.2 und nachrangig nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Allgemeine Bedingungen für Zahlungsdienste und Bedingungen für das Wertpapiergeschäft).

12.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

12.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kunde 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 Kunde 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 Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Authentifizierungselements 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 Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang.

Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach

- Nummer 8.1 Absatz 2
- Nummer 8.1 Absatz 4
- Nummer 8.1 Absatz 6
- Nummer 8.3 oder
- Nummer 10.1 Absatz 1

dieser Bedingungen verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung im Sinne von § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Sein (siehe Nummer 2 Absatz 3 dieser Bedingungen).

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

(6) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz (1) und (3) verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 10.1 dieser Bedingungen 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 Kunde kein Verbraucher, gilt ergänzend Folgendes:

- Der Kunde haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro in Absatz (1) und (3) hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich 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 Kunden bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige

Beruhen nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

12.2.3 Haftung ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach über das Digital Banking 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 Digital Banking 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

Im Rahmen der Ordererteilung wird dem Teilnehmer eine Auswahl der zum jeweiligen Zeitpunkt bei der Commerzbank verfügbaren Ausführungsplätze angeboten. Der Teilnehmer kann auf dieser Basis einen Ausführungsplatz für seinen Auftrag bestimmen. 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 – HD0322-01