COMMERZBANK
Die Bank an Ihrer Seite

Bedingungen für die Abwicklung von Bankgeschäften über das Firmenkundenportal und HBCI/FinTS-Service

(Stand: 14. September 2019)

1. Leistungsangebot

(1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels Firmenkundenportal oder den HBCI/FinTS-Service in dem von der Bank angebotenen Umfang abwickeln. Für die Abwicklung gelten die Bedingungen für die jeweiligen Bankgeschäfte (z. B. Firmenkundenbedingungen für Zahlungsdienste, Sonderbedingungen für das Commerzbank Onlinebanking, Wertpapierbedingungen, Sonderbedingungen für Wertpapiergeschäfte). Zudem können sie Informationen der Bank abrufen.

(2) Kunde und Bevollmächtigte werden einheitlich als „Teilnehmer" oder „User" bezeichnet. Hierzu gehört auch der „Nutzer" gemäß den Bedingungen für die Datenfernübertragung, der die Datenfernübertragung im Rahmen des Firmenkundenportals nutzt. Konto und Depot werden einheitlich als „Konto" bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

(3) Kunde und Bank können Verfügungslimite für bestimmte Servicearten gesondert vereinbaren.

2. Voraussetzungen zur Nutzung des Firmenkundenportals und des HBCI/FinTS-Service

(1) Der Teilnehmer/User kann das Firmenkundenportal oder den HBCI/FinTS-Service 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/Users, oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers/Users prüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer/User sich gegenüber der Bank als berechtigter Teilnehmer/User ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).

(3) Authentifizierungselemente sind
- Wissenselemente, also etwas, das nur der Teilnehmer/User weiß (z. B. persönliche Identifikationsnummer [PIN]),
- Besitzelemente, also etwas, das nur der Teilnehmer/User besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN], die den Besitz des Teilnehmers/Users nachweisen, wie mobile Endgeräte) oder
- Seinselemente, also etwas, das der Teilnehmer/User ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

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

3. Zugang zum Firmenkundenportal

(1) Der Teilnehmer/User erhält Zugang zum Firmenkundenportal, wenn
- er seine individuelle Teilnehmernummer/seinen Anmeldenamen angibt und
- sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (siehe Nummern 9.1 und 10 dieser Bedingungen) vorliegt.

Nach Gewährung des Zugangs zum Firmenkundenportal 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/User auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Firmenkundenportal nur ein Authentifizierungselement angefordert wurde. Der Name des Kontoinhabers und die Kontonummer sind für die vom Teilnehmer/User genutzten Zahlungsauslösedienste und Kontoinformationsdienste keine sensiblen Zahlungsdaten (§ 1 Abs. 26 Satz 2 ZAG).

4. Aufträge

4.1 Auftragserteilung

Der Teilnehmer/User muss einem über das Firmenkundenportal oder HBCI/FinTS-Service erteilten Auftrag (z. B. einer Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z. B. Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden.

4.2 Ergänzende Regelungen für die Datenfernübertragung im EBICS-Standard bei Einsatz des photoTAN-Verfahrens

4.2.1 Der Kunde beauftragt die Bank mit der Speicherung des persönlichen Schlüssels des Teilnehmers/Users in einer technischen Umgebung, die vor unautorisiertem Zugriff geschützt ist. Die Bank ist berechtigt, hierfür auch einen zuverlässigen Dienstleister zu beauftragen. Das zur Freigabe des persönlichen Schlüssels erforderliche Kennwort wird durch eine TAN im photoTAN-Verfahren ersetzt.

4.2.2 Die Bedingungen für die Datenfernübertragung werden wie folgt ergänzt:

- Ergänzend zu Ziffer 4 (2) der Bedingungen für die Datenfernübertragung gilt, dass die Aufbewahrung der elektronischen Schlüssel in einer von der Bank (oder von einem von der Bank zugelassenen Dienstleister) zur Verfügung gestellten technischen Umgebung (vgl. Ziffer 2.2.1 (5) der Anlage 1a der Bedingungen für die Datenfernübertragung) erlaubt ist.
- Zu Ziffer 8 (3) der Bedingungen für die Datenfernübertragung wird vereinbart, dass die Bank die Legitimation auch daraufhin prüft, ob die richtige TAN eingegeben wurde.

4.2.3 Die Anlage 1a der Bedingungen für die Datenfernübertragung wird wie folgt ergänzt:

- Die Authentifikationssignatur kann in Ziffer 1.1.2 der Anlage 1a der Bedingungen für die Datenfernübertragung beim photoTAN-Verfahren auch in der technischen Umgebung der Bank oder des zugelassenen Dienstleisters geleistet werden. Diese nehmen für den Kunden die erforderliche Prüfung vor.
- Zu Ziffer 2.2.1 (5) der Anlage 1a der Bedingungen für die Datenfernübertragung wird vereinbart, dass die TAN anstelle des Passworts verwendet wird, wenn das Sicherungsmedium des Teilnehmers/Users bankseitig in einer technischen Umgebung gespeichert ist, die vor unautorisiertem Zugriff geschützt ist.

4.3 Meldung nach AWV

Bei Zahlungen zugunsten Gebietsfremder ist vom Teilnehmer/User die Meldung gemäß Außenwirtschaftsverordnung (AWV) zu beachten.

4.4 Widerruf von Aufträgen

Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen. Der Widerruf von Aufträgen kann nur außerhalb des Firmenkundenportals und des HBCI/FinTS-Service erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Firmenkundenportal oder beim HBCI/FinTS-Service 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 der vereinbarten Serviceart.

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

- Der Teilnehmer/User hat den Auftrag autorisiert (vgl. Nummer 4.1 dieser Bedingungen).
- Die Berechtigung des Teilnehmers/Users für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das für die vereinbarte Serviceart erforderliche Datenformat wurde eingehalten.
- Das für die Serviceart gesondert vereinbarte Verfügungslimit ist nicht überschritten.
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Firmenkundenbedingungen für Zahlungsdienste) liegen vor.

Liegen die Ausführungsbedingungen nach Absatz (2) Satz 1 vor, führt die Bank die Aufträge nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen aus.

Liegen die Ausführungsbedingungen nach Absatz (2) Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird den Teilnehmer/User hierüber informieren und, soweit möglich, dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6. Information des Kunden über erteilte Verfügungen

Die Bank unterrichtet den Kunden mindestens einmal monatlich über die im Rahmen des Firmenkundenportals oder des HBCI/FinTS-Service getätigten Verfügungen auf dem für Konto- und Depotinformationen vereinbarten Weg und gemäß den für den Auftrag geltenden Bedingungen.

7. Sorgfaltspflichten des Teilnehmers/Users

7.1 Schutz der Authentifizierungselemente

Der Teilnehmer/User ist dafür verantwortlich, dass er für seine eigenen Systeme eine angemessene Datensicherung unterhält und stets nach dem Stand der Technik ausreichende Vorkehrungen gegen Viren und andere schädliche Programme (z. B. Trojaner, Würmer) trifft. Apps der Bank dürfen nur von App-Anbietern bezogen werden, die die Bank dem Kunden mitgeteilt hat. Der Teilnehmer/User hat eigenverantwortlich die landesspezifischen Regelungen für die Nutzung des Internets zu beachten.

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

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer/User 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 Verfahrens in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden,
- nicht ungesichert elektronisch gespeichert werden (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Onlinebanking und Fingerabdrucksensor) dient.

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

- ist die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
- ist sicherzustellen, dass andere unberechtigte Personen auf das mobile Endgerät des Teilnehmers/Users (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 Firmenkundenportal (z. B. Anwendungs-App, Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für das Firmenkundenportal (z. B. Anwendungs-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers/Users zu deaktivieren, bevor der Teilnehmer/User 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 Firmenkundenportals und des HBCI/FinTS-Service 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 Firmenkundenportal) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Firmenkundenportal des Teilnehmers/Users aktivieren.

(c) Seinselemente wie z. B. Fingerabdruck des Teilnehmers dürfen auf einem mobilen Endgerät des Teilnehmers/Users für das Firmenkundenportal 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 Firmenkundenportal genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Firmenkundenportal das von der Bank ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(d) Des Weiteren ist zu beachten:

- Der vom Teilnehmer/User erzeugte persönliche elektronische Schlüssel darf sich nur in der alleinigen Verfügungsgewalt des Teilnehmers/Users oder in einer von der Bank (oder von einem von der Bank zugelassenen Dienstleister) zur Verfügung gestellten technischen Umgebung, die vor unautorisiertem Zugriff geschützt ist, befinden.
- Wird im Rahmen einer voll automatisierten Übertragung ein sogenannter „Technischer User“ eingesetzt, ist die elektronisch gespeicherte Signatur in einer sicheren und entsprechend geeigneten technischen Umgebung zu speichern. Der „Technische User“ ist nicht berechtigt, die Auftragserteilung selbst vorzunehmen. Er übermittelt lediglich die Auftragsdaten.
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Die Signatur-PIN/das Kennwort für die elektronische Signatur darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer/User darf zur Autorisierung eines Auftrags nicht mehr als eine TAN verwenden.

(3) Die App der Bank zur Entschlüsselung der TAN-Grafik ist direkt von der Bank oder von einem dem Kunden von der Bank benannten Anbieter zu beziehen.

7.2 Sicherheitshinweise der Bank

Der Teilnehmer/User muss die Sicherheitshinweise auf der Internetseite der Bank, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten und aktuelle, dem Stand der Technik entsprechende Virenschutz- und Firewall-Systeme installieren. Insbesondere dürfen das Betriebssystem und die Sicherheitsvorkehrungen des mobilen Endgeräts nicht modifiziert oder deaktiviert werden.

7.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer/User die von ihr empfangenen Auftragsdaten (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers/Users an (z. B. mittels eines mobilen Endgeräts). Der Teilnehmer/User ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

7.4 Weitere Sorgfaltspflichten des Kunden

Der Kunde trägt dafür Sorge, dass die Sorgfaltspflichten aus diesen Bedingungen auch von den Bevollmächtigten (also von allen Teilnehmern/Usern) eingehalten werden.

8. Verschlüsselungstechnik im Ausland

In den Ländern, in denen Nutzungs-, Einfuhr- und/oder Ausfuhrbeschränkungen für Verschlüsselungstechniken bestehen, darf der von der Bank zur Verfügung gestellte Onlinezugang nicht genutzt werden. Ggf. hat der Teilnehmer/User die erforderlichen Genehmigungen, Anzeigen oder sonst erforderlichen Maßnahmen zu veranlassen. Der Teilnehmer/User hat die Bank über ihm bekannt gewordene Verbote, Genehmigungs- und Anzeigepflichten zu informieren.

9. Anzeige- und Unterrichtungspflichten

9.1 Sperranzeige

(1) Stellt der Teilnehmer/User
- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. eines mobilen Endgeräts) oder
- die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung eines Authentifizierungselements

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

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

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

9.2 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.

10. Nutzungssperre

10.1 Sperre auf Veranlassung des Teilnehmers/Users

Die Bank sperrt auf Veranlassung des Teilnehmers/Users, insbesondere im Fall der Sperranzeige nach Nummer 9.1 dieser Bedingungen,
- den Zugang für ihn oder alle Teilnehmer/User oder
- sein Authentifizierungselement zur Nutzung des Firmenkundenportals und HBCI/FinTS-Service.

10.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Zugang für einen Teilnehmer/User sperren, wenn
- sie berechtigt ist, den Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Teilnehmers/Users dies rechtfertigen,
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht,
- der Kontrollwert zur Freigabe der HBCI-Signatur dreimal falsch eingegeben wird. Der Teilnehmer/User muss dann eine neue elektronische Signatur erstellen und diese erneut an die Bank übermitteln,
- die PIN dreimal in Folge falsch eingegeben wurde oder
- fünfmal hintereinander die TAN falsch eingegeben wurde.

(2) Die Bank wird den Kunden 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. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

10.3 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.

10.4 Automatische Sperre eines Chip-basierten Besitzelements

(1) Eine Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur falsch eingegeben wurde. Eine Wiederfreischaltung bzw. Entsperrung der Chipkarte durch die Bank ist nicht möglich. Der Teilnehmer/User muss mit einer neuen Chipkarte eine neue elektronische Signatur erstellen und diese erneut an die Bank übermitteln sowie mittels eines INI-Briefs bei der Bank freischalten lassen.

(2) Das Besitzelement kann dann nicht mehr für das Firmenkundenportal oder den HBCI/FinTS-Service genutzt werden. Der Teilnehmer/User kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten wiederherzustellen.

11. Haftung

11.1 Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Bank bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen.

11.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

11.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden, wenn den Teilnehmer/User an dem Verlust, Diebstahl, sonstigem Abhandenkommen oder der sonstigen missbräuchlichen Verwendung des Authentifizierungselements ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer/User nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers/Users nach diesen Bedingungen nicht regelmäßig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens,

in welchem Umfang Kunde und Bank den Schaden zu tragen haben. Soweit es sich beim Kunden um einen Unternehmer gemäß § 14 BGB handelt, findet die Haftungsbegrenzung auf 50 Euro gemäß § 675v Abs. 1 BGB keine Anwendung.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach 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/User 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/Users kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach
- Nummer 7.1 Absatz 2,
- Nummer 7.1 Absatz 3,
- Nummer 7.3,
- Nummer 9.1 Absatz 1 oder
- Nummer 9.2

dieser Bedingungen verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadenersatz verpflichtet, wenn die Bank vom Teilnehmer/User eine starke Kundenauthentifizierung im Sinne des § 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 mit dem Kunden vereinbarte Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf dieses Limit.

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

(7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer/User in betrügerischer Absicht gehandelt hat.

11.2.2 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 verloren gegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haftet der Kunde für den der Bank hierdurch entstandenen Schaden, wenn den Teilnehmer/User an dem Verlust, Diebstahl, sonstigem Abhandenkommen oder der sonstigen missbräuchlichen Nutzung des Authentifizierungselements ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer/User nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers/Users nach diesen Bedingungen nicht regelmäßig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Kunde und Bank den Schaden zu tragen haben.

11.2.3 Haftung ab der Sperranzeige

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

11.2.4 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.

12. Verfügbarkeit

Die Bank strebt an, die angebotenen Services möglichst umfassend verfügbar zu halten. Eine garantierte Verfügbarkeit ist damit nicht verbunden. Insbesondere aufgrund technischer Probleme, Wartungsarbeiten und aufgrund von Netzproblemen (z. B. Nichtverfügbarkeit von Servern Dritter), auf welche die Bank keinen Einfluss hat, kann es zu zeitweiligen Störungen kommen, die den Zugriff verhindern.

13. Verweis auf Internetseiten Dritter

Falls im Rahmen des Internetauftritts der Zugriff auf die Seiten Dritter ermöglicht wird, geschieht dies nur, um dem Kunden und dem Teilnehmer/User einen leichteren Zugriff auf das Informationsangebot im Internet zu ermöglichen. Die Inhalte der Seiten dieser Anbieter stellen nicht eigene Aussagen der Bank dar. Sie werden von der Bank auch nicht überprüft.

14. Nutzungsrechte

Dem Kunden wird durch diesen Vertrag nicht gestattet, Links oder Framelinks auf seinen Webseiten ohne vorherige schriftliche Zustimmung der Bank zu setzen. Der Kunde verpflichtet sich, die Webseiten und deren Inhalt nur für eigene

Zwecke zu verwenden. Insbesondere ist der Kunde nicht berechtigt, ohne Zustimmung der Bank die Inhalte Dritten zur Verfügung zu stellen, in andere Produkte oder Verfahren einzubetten oder den Quellcode der einzelnen Webseiten zu entschlüsseln. Hinweise auf Rechte der Bank oder Dritter dürfen nicht entfernt oder unkenntlich gemacht werden. Der Kunde wird Marken, Domainnamen und andere Kennzeichen der Bank oder Dritter nicht ohne vorherige Zustimmung der Bank verwenden. Der Kunde erhält nach diesen Bedingungen keine unwiderruflichen, ausschließlichen und übertragbaren Nutzungsrechte.

15. Hotline (Helpdesk)

Die Bank bietet eine telefonische Hotline (sog. Helpdesk) für die Bearbeitung von Fragen zu Technik, Bedienung und Funktionalitäten der angebotenen Services an. Die Bank besetzt die Hotline während der für das deutsche Bankgewerbe geltenden Bankarbeitstage. Telefonnummern und Geschäftszeiten werden in den Zugangswegen kommuniziert.

16. Sonstiges

(1) Im Hinblick auf die ordnungsgemäße Abwicklung der Zusammenarbeit behält sich die Bank Änderungen im technischen bzw. organisatorischen Bereich vor, die auf einer allgemeinen, handelsüblichen Änderung der technischen Standards, der Vorgaben der Kreditwirtschaft oder der gesetzlichen bzw. aufsichtsbehördlichen Regelungen beruhen. Eine darüber hinausgehende wesentliche technische bzw. organisatorische Änderung, die erhebliche Auswirkungen auf die Rechte und Pflichten des Kunden oder der Bank hat, teilt die Bank dem Kunden mindestens sechs Wochen vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens mit. Die Zustimmung des Kunden gilt als erteilt, wenn er seine Ablehnung nicht innerhalb von sechs Wochen nach Erhalt der Mitteilung angezeigt hat.

(2) Diese Bedingungen richten sich nach deutschem Recht.

(3) Sollte dieser Vertrag eine Regelungslücke enthalten, eine Bestimmung unwirksam oder undurchführbar sein, so bleibt die Rechtswirksamkeit der übrigen Bestimmungen hiervon unberührt. Die Vertragsparteien verpflichten sich, in einem derartigen Fall eine wirksame oder durchführbare Regelung zu treffen, die dem Geist und Zweck der zu ergänzenden bzw. zu ersetzenden Bestimmung so weit wie möglich entspricht.

Commerzbank AG