Deutsche Bank
Aktiengesellschaft

Bedingungen für den Zugang zur Deutsche Bank AG (nachstehend Bank) über elektronische Medien

Stand: 10/2018

1. Leistungsangebot

(1) Der Konto-/Depotinhaber und dessen Bevollmächtigte können Bankgeschäfte mittels elektronischer Zugangsmedien, im Einzelnen Online-Banking und Telefon-Banking (jeweils einzeln „Online-Banking" bzw. „Telefon-Banking" sowie gemeinsam „Zugangsmedien" bzw. „elektronische Medien"), in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online- und Telefon-Banking abrufen. Im Rahmen des Online-Bankings sind sie zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrags[1] einen Zahlungsauslösedienst gemäß § 1 Absatz 33 Zahlungsdiensteaufsichtsgesetz und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienst gemäß § 1 Absatz 34 Zahlungsdiensteaufsichtsgesetz zu nutzen.
Hinweis: Im Rahmen von maxblue bietet die Bank keine Anlageberatung an.

(2) Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer" bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto" bezeichnet.

(3) Für die Nutzung der Zugangsmedien gelten die mit der Bank gesondert vereinbarten Verfügungslimite.

2. Voraussetzungen zur Nutzung der elektronischen Medien

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften über elektronische Medien die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge[1] zu autorisieren (siehe Nummer 4). Statt eines Personalisierten Sicherheitsmerkmals kann auch ein biometrisches Merkmal zum Zwecke der Authentifizierung bzw. Autorisierung vereinbart werden.

Dieser Prozess wird als Authentifizierungsverfahren bezeichnet.

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die die Bank dem Teilnehmer zum Zwecke der Authentifizierung bereitstellt. Biometrische Merkmale bzw. Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind beispielsweise:
– die persönliche Identifikationsnummer (PIN) oder das persönliche Passwort,
– einmal verwendbare Transaktionsnummern (TAN),
– der Nutzungscode für die elektronische Signatur,
– der Aktivierungscode für ein Authentifizierungsinstrument oder
– ein von einem von der Bank zugelassenen Authentifizierungsinstrument geprüftes, biometrisches Merkmal wie der eigene Fingerabdruck (Fingerprint).

2.2 Authentifizierungsinstrumente

(1) Authentifizierungsinstrumente sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurde und die vom Teilnehmer zur Erteilung eines Auftrags[1] verwendet werden. Insbesondere mittels folgender Authentifizierungsinstrumente kann das Personalisierte Sicherheitsmerkmal (z. B. PIN oder TAN) dem Teilnehmer zur Verfügung gestellt werden:
– PIN
– auf einer Liste mit einmal verwendbaren TAN (iTAN),
– mittels eines TAN-Generators, der Bestandteil einer Chipkarte oder eines anderen elektronischen Gerätes zur Erzeugung von TAN ist,
– mittels eines mobilen Endgerätes (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN), auf einer Chipkarte mit Signaturfunktion (z. B. HBCI) oder
– auf einem sonstigen Authentifizierungsinstrument, u. a. über eine Softwareanwendung bzw. „App" der Bank auf elektronischen Geräten wie Smartphone, Tablet oder Lesegerät, z. B. für das photoTAN-Verfahren, oder über ein für eine elektronische Signatur ausreichend geeignetes Lesegerät, auf dem sich Signaturschlüssel befinden.

(2) Je nach Authentifizierungsverfahren und -instrument benötigt der Teilnehmer hierfür gegebenenfalls geeignete Hard- und Software. Über das Angebot der bankeigenen Anwendungen hinaus bleibt der Teilnehmer selbst für die Beschaffung, Installation und Pflege dieser Hard- und Software verantwortlich

(3) Bei einer Nutzung einer Hard- bzw. Software von Drittanbietern durch den Teilnehmer übernimmt die Bank keine eigene Gewährleistung oder sonstige Verantwortung für eine andauernde Eignung oder Verfügbarkeit im Zusammenhang mit einem Authentifizierungsverfahren.

(4) Sofern die Bank für einzelne hier aufgeführte Leistungen ein Entgelt verlangt, ist der jeweilige Preis im „Preis- und Leistungsverzeichnis" der Bank bzw. in der jeweiligen Teilnahmevereinbarung ausgewiesen. Für Änderungen und Preise gilt Ziffer 12 der AGB Banken, wenn keine besondere Vereinbarung zwischen Bank und Kunde getroffen wurde.

3. Zugang über elektronische Medien

Der Teilnehmer erhält Zugang zu Online- und Telefon-Banking, wenn
– dieser die Kontonummer oder seinen individuellen Benutzernamen und seine PIN oder seinen Token oder sein Passwort oder seine elektronische Signatur der Bank 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 Nummer 8.1 und 9) vorliegt.

Nach Gewährung des Zugangs zum Online- und Telefon-Banking kann der Teilnehmer Informationen abrufen oder Aufträge[1] erteilen. Im Rahmen des Online-Bankings gelten die Sätze 1 und 2 auch, wenn der Teilnehmer Zahlungsaufträge über einen Zahlungsauslösedienst auslöst und Zahlungskontoinformationen über einen Kontoinformationsdienst anfordert (siehe Nummer 1 Absatz 1 Satz 3).

4. Online- und Telefon-Banking-Aufträge[1]

4.1 Auftragserteilung und Autorisierung

(1) Der Teilnehmer muss Online-Banking-Aufträge zu deren Wirksamkeit mit dem von der Bank bereitgestellten Personalisierten Sicherheitsmerkmal (z. B. TAN oder elektronische Signatur) oder mit einem 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 3) auslöst und übermittelt.

(2) Der Teilnehmer kann Telefon-Banking-Aufträge nur nach erfolgreicher Autorisierung mit von der Bank bereitgestelltem Personalisiertem Sicherheitsmerkmal erteilen. Die Bank bestätigt den Eingang des Auftrags auf dem vom Teilnehmer für den Auftrag gewählten Zugangsweg. Die zwischen der Bank und dem Kontoinhaber übermittelte Telefonkommunikation wird zu Beweiszwecken automatisch aufgezeichnet und gespeichert.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Online- und Telefon-Banking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Online- und Telefon-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Online- und Telefon-Banking ausdrücklich vor.

5. Bearbeitung von Online- und Telefon-Banking-Aufträgen[1] durch die Bank

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

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
– Der Teilnehmer hat den Auftrag autorisiert.
– Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
– Das Online-Banking-Datenformat ist eingehalten.
– Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.

– Im Telefon-Banking wird die Bank Verfügungen über das Konto, die eine Zahlung[1] an einen Dritten (abweichende Kontonummer) enthalten, bis zu einem Betrag von insgesamt unter 50.000 EUR pro Tag ausführen, sofern nicht ein anderer Verfügungshöchstbetrag mit dem Teilnehmer vereinbart ist. Für Überträge (Überweisungen) innerhalb der gleichen Kundennummer oder An- und Verkäufe von Wertpapieren gilt diese Betragsgrenze nicht.
– Die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Online-und Telefon-Banking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Online- bzw. Telefon-Banking-Auftrag nicht ausführen und den Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Online- bzw. Telefon-Banking oder postalisch informieren.

6. Information des Kontoinhabers über Online- und Telefon-Banking-Verfügungen[1]
Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Online- und Telefon-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers
7.1 Technische Verbindung zum Online- und Telefon-Banking
Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online- und Telefon-Banking nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle (z. B. Internetadresse) und Telefon-Banking-Zugangskanäle (Telefonnummern) herzustellen.
Im Rahmen des Online-Bankings kann der Teilnehmer zur Erteilung eines Zahlungsauftrags[1] und zum Abruf von Informationen über ein Zahlungskonto die technische Verbindung zum Online-Banking auch über einen Zahlungsauslösedienst beziehungsweise einen Kontoinformationsdienst (siehe Nr. 1 Absatz 1 Satz 3) herstellen.

7.2 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 dem dazugehörigen Personalisierten Sicherheitsmerkmal das Online- und Telefon-Banking-Verfahren missbräuchlich nutzen. Im Rahmen des Online-Bankings wird die Geheimhaltungspflicht bezüglich der Personalisierten Sicherheitsmerkmale nach Satz 1 nicht verletzt, wenn der Teilnehmer diese zur Erteilung eines Zahlungsauftrags[1] oder zum Abruf von Informationen über ein Zahlungskonto an den von ihm ausgewählten Zahlungsauslösedienst beziehungsweise Kontoinformationsdienst übermittelt (siehe Nummer 1 Absatz 1 Satz 3).

(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:
– Das Personalisierte Sicherheitsmerkmal darf nicht ungesichert außerhalb des zugelassenen Authentifizierungsverfahrens elektronisch gespeichert werden (z. B. im Kundensystem oder auf einem Endgerät).
– Das Authentifizierungsinstrument (z. B. die Softwareanwendung der Bank oder das zugelassene Lesegerät) darf sich ausschließlich in der alleinigen Verfügungsgewalt des Teilnehmers befinden. Ein Zugriff auf Personalisierte Sicherheitsmerkmale durch unberechtigte Dritte (worunter keine Kontoinformationsdienste und Zahlungsauslösedienste zu verstehen sind) über das Authentifizierungsinstrument ist durch angemessene Sicherheitsmaßnahmen des Teilnehmers (z. B. Passwortschutz bei Smartphone) zu unterbinden.
– Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
– Das Personalisierte Sicherheitsmerkmal darf – auch wenn der Teilnehmer sich eines Zahlungsauslösedienstes bzw. eines Kontoinformationsdienstes bedient – nur mittels der von der Bank zugelassenen Authentifizierungsverfahren eingegeben werden.
– Sollte der Teilnehmer im Rahmen eines Authentifizierungsverfahrens Systeme oder Verfahren eines Dritten verwenden, so übernimmt die Bank keine Verantwortung für die Auswahl, Sicherheit oder Überwachung dieser Systeme oder Verfahren. Der Teilnehmer bleibt bei einer Nutzung dieser Dritt-Systeme oder -Verfahren für die Einhaltung seiner Pflichten aus diesen Bedingungen verantwortlich.
– Das Personalisierte Sicherheitsmerkmal darf nicht an unberechtigte Dritte (z. B. per E-Mail oder Telefon) weitergegeben werden.
– Die Personalisierten Sicherheitsmerkmale (z. B. PIN, das Passwort und der Nutzungscode für die elektronische Signatur) dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
– Der Teilnehmer darf zur Autorisierung z. B. eines Auftrags oder zur Aufhebung einer Sperre nicht mehr als eine TAN verwenden oder ein sonstiges Personalisiertes Sicherheitsmerkmal einsetzen.
– Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.
– Der Aufforderung per elektronischer Nachricht (z. B. E-Mail), eine damit übersandte Verknüpfung zum (vermeintlichen) Online-Banking der Bank anzuwählen und darüber persönliche Zugangsdaten einzugeben, darf nicht gefolgt werden.
– Anfragen außerhalb der bankseitig zur Verfügung gestellten originären Zugangswege, in denen nach vertraulichen Daten wie PIN, Geheimzahl oder Passwort/Online-TAN gefragt wird, dürfen nicht beantwortet werden. Die Nutzung von Zahlungsauslösediensten bzw. Kontoinformationsdiensten bleibt hiervon unberührt.
– Der Teilnehmer hat vor seinem jeweiligen Zugang zum Online-Banking sicherzustellen, dass auf dem verwendeten System handelsübliche Sicherheitsvorkehrungen (wie Anti-Viren-Programm und Firewall) installiert sind und diese ebenso wie die verwendete System- und Anwendungssoftware regelmäßig aktualisiert werden. Beispiele handelsüblicher Sicherheitsvorkehrungen kann der Teilnehmer den Internetseiten der Bank entnehmen.
– Die Softwareanwendungen der Bank sind ausschließlich direkt von der Bank oder von einem von der Bank benannten Anbieter zu beziehen.

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

Darüber hinaus hat der Kunde in eigener Verantwortung etwaige Sicherheitshinweise der Anbieter der eingesetzten Kundensysteme zu beachten (z. B. Sicherheitsupdates von Systemsoftware mobiler Endgeräte).

7.4 Kontrolle durch Abgleich der Auftragsdaten mit von der Bank angezeigten Daten
Soweit die Bank dem Teilnehmer Daten aus seinem Online-Banking-Auftrag[1] (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z. B. Mobiltelefon oder Lesegerät) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Autorisierung (z. B. Eingabe der TAN) die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen. Stimmen die angezeigten Daten nicht überein, ist der Vorgang abzubrechen und die Bank unverzüglich zu informieren.

8. Anzeige- und Unterrichtungspflichten
8.1 Sperranzeige
(1) Stellt der Teilnehmer
– den Verlust, den Diebstahl oder die missbräuchliche Verwendung des Authentifizierungsinstruments oder des zugehörigen Gerätes (z. B. Smartphone mit installierter Banksoftwareanwendung zur Authentifizierung) 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
– Besitz an seinem Authentifizierungsinstrument oder Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder
– das Authentifizierungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet,

muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Kontoinhaber hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1,
– den vom Teilnehmer bezeichneten Banking-Zugang für ihn oder alle Teilnehmer oder
– sein Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Online- und Telefon-Banking-Zugang für einen Teilnehmer sperren oder ein Authentifizierungsinstrument nicht mehr zulassen, wenn
– sie berechtigt ist, den Online- und Telefon-Banking-Vertrag aus wichtigem Grund zu kündigen,
– sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen,
– der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht oder
– ein genutzter Zugangsweg bzw. ein im Zusammenhang mit einem Authentifizierungsverfahren zugelassenes Gerät von der Bank als unsicher eingestuft wird. Als Zugangsweg gelten auch Softwareanwendungen der Bank in allen zur Verfügung stehenden Versionen.

(2) Die Bank wird den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre postalisch, telefonisch oder online unterrichten.

9.3 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. Der Teilnehmer kann eine von ihm veranlasste Sperrung nur postalisch oder mit telefonisch legitimiertem Auftrag aufheben lassen.

9.4 Automatische Sperre eines chipbasierten Authentifizierungsinstruments

(1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur falsch eingegeben wird.

(2) Wird die Geheimzahl zur WebSign-Chipkarte bzw. zur personalisierten Electronic-Banking-Karte dreimal hintereinander (Karten ab Bestelldatum 09/2012) bzw. achtmal hintereinander (Karten vor Bestelldatum 09/2012) falsch eingegeben, wird die Karte automatisch gesperrt.

(3) Ein TAN-Generator als Bestandteil einer Chipkarte, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn der Code dreimal in Folge falsch eingegeben wird.

(4) Die in den Absätzen 1, 2 und 3 genannten Authentifizierungsinstrumente können dann nicht mehr für das Online-Banking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

10. Haftung

10.1 Haftung der Bank bei einer nicht autorisierten Online- oder Telefon-Banking-Verfügung[1] und einer nicht, fehlerhaft oder verspätet ausgeführten Online- oder Telefon-Banking-Verfügung

Die Haftung der Bank bei einer nicht autorisierten Online- und Telefon-Banking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Online-/Telefon-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung eines biometrischen Merkmals bzw. Personalisierten Sicherheitsmerkmals oder eines Authentifizierungsinstruments

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge[1] 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 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, Diebstahl oder die missbräuchliche Verwendung des Authentifizierungsinstruments, des zugehörigen Geräts (z. B. Smartphone mit installierter Banksoftwareanwendung zur Authentifizierung) oder des Personalisierten Sicherheitsmerkmals nicht unverzüglich der Bank anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1 Absatz 1),
– das Personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe Nummer 7.2 Absatz 2, 1. Punkt),
– das Personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1, 2. Punkt),
– das Personalisierte Sicherheitsmerkmal per E-Mail weitergegeben hat (siehe Nummer 7.2 Absatz 2, 6. Punkt),
– das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2, 7. Punkt),
– mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2, 8. Punkt),
– beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Online-Banking nutzt (siehe Nummer 7.2 Absatz 2, 9. Punkt),
– die Softwareanwendungen der Bank nicht direkt von der Bank oder von einem von der Bank benannten Anbieter bezieht (siehe Nummer 7.2 Absatz 2, 13. Punkt),
– die auf seinem Authentifizierungsinstrument angezeigten Auftragsdaten nicht prüft (siehe Nummer 7.4),
– bei Abweichen der Daten auf dem Authentifizierungsinstrument von den für die Transaktion vorgesehenen Daten den Vorgang nicht abbricht und die Bank nicht unverzüglich informiert (siehe Nummer 7.4).

(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 hat, 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, das 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 der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

(6) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, 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 nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
– Die Haftungsbeschränkung in Absatz 2, 1. Punkt findet keine Anwendung.

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

10.2.3 Haftung der Bank ab der Sperranzeige
Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-/Telefon-Banking-Verfügungen[1] entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.2.4 Haftungsausschluss
Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

1 Zum Beispiel Überweisung, Dauerauftrag und Lastschrift.