Santander

Santander Consumer Bank AG
Postfach 10 12 14
41012 Mönchengladbach

Auftrag mobileTAN-Verfahren

Ergänzend zu den auf Seite 2 genannten, für das Online Banking geltenden Sonderbedingungen der Santander Consumer Bank erteile ich,

Nachname:

Zugangsnummer/Benutzername:

Vorname:

IBAN D E

folgenden Auftrag:

☐ **Ich möchte das mobileTan-Verfahren nutzen.Bitte schalten Sie meine nachfolgend genannte Mobilfunknummer für das mobileTan-Verfahren frei:**

☐ **Ich benutze bereits das mobileTan-Verfahren. Meine Mobilfunknummer hat sich geändert. Bitte schalten Sie die nachfolgend genannte Mobilfunknummer für das mobileTan-Verfahren frei:**

Bedingungen für das mobileTAN-Verfahren

1. Ergänzend zu den Regelungen der Sonderbedingungen für das Online Banking der Santander Consumer Bank (im Folgenden Bank genannt),bietet die Bank das mobileTAN-Verfahren an.
2. Voraussetzung für die Teilnahme an dem mobile-TAN-Verfahren ist ein Mobilfunkzugang eines deutschen Netzbetreibers.
3. Bei dem mobileTAN-Verfahren wird auf Anforderung des Kunden eine individuelle TAN generiert und dem Kunden per SMS auf sein hierfür registriertes Mobiltelefon übermittelt (sog. mobile TAN).
4. Die mobileTAN kann nur für den Auftrag genutzt werden, für den sie angefordert wurde.
5. Das für das mobileTAN-Verfahren registrierte Mobiltelefon darf nicht dazu verwendet werden, den Online Banking-Zugang herzustellen.
6. Stellt der Kunde den Verlust des für das mobile-TAN-Verfahren registrierten Mobiltelefons oderder SIM-Karte fest oder besteht der Verdachteiner missbräuchlichen Nutzung, so ist er verpflichtet,das Telefon bei seinem Mobilfunkbetreiber zu sperren und die Bank unverzüglichzu benachrichtigen.

Datenschutz:
Bitte beachten Sie, dass wir bei der Benutzung unserer Webseiten und Applikationen im Rahmen des Online Banking Ihre personenbezogenen Daten verarbeiten. Informationen hierzu entnehmen Sie bitte den spezifischen Datenschutzhinweisen der jeweiligen Webseite bzw. Applikation. Im Übrigen gelten für Kontoinhaber die bei Abschluss des jeweiligen Kontovertrags bereitgestellten Datenschutzhinweise; für Kontobevollmächtigte die zusammen mit den Vollmachtsformularen bereitgestellten Datenschutzhinweise.

Stand 05/2018

Datum ✗ Unterschrift

Hinweis
Bitte senden Sie diesen Auftrag unterschrieben per Post an die oben genannte Adresse. Per Fax an uns gerichtete Aufträge zur Freischaltung des mobile TAN-Verfahrens können nicht bearbeitet werden.

Bedingungen für die Nutzung des Online Banking

I. Allgemeine Bedingungen zum Fernabsatz

Die Santander Consumer Bank AG, Santander-Platz 1, 41061 Mönchengladbach (Amtsgericht Mönchengladbach, HRB 1747) **wird vertreten durch den Vorstand: Vito Volpe (Vorsitzender), Oliver Burda (stv. Vorsitzender), Walter Donat, José María Echanove, Thomas Hanswillemenke, Jochen Klöpper.** Das zuständige Aufsichtsamt ist die Bundesanstalt für Finanzdienstleistungsaufsicht, Graurheindorfer Straße 108, 53117 Bonn und Marie-Curie-Straße 24-28, 60439 Frankfurt am Main und die Europäische Zentralbank, Sonnemannstraße 20, 60314 Frankfurt.

Der Gegenstand des Unternehmens ist die Ausführung von Bankgeschäften aller Art, mit Ausnahme der Bankgeschäfte im Sinne des § 1 Abs. 1 Nr. 1 a und Nr. 12 des Kreditwesengesetzes.
Die USt.-IdNr. der Santander Consumer Bank AG lautet DE120492390. Soweit nicht anders angegeben, sind Entgelte aus Finanzdienstleistungen umsatzsteuerfrei. Der Vertrag kommt durch Angebot des Kontoinhabers und durch Annahme der Bank zu Stande. Die Vertragsanbahnung sowie der Vertragsabschluss unterliegen deutschem Recht. Vertragssprache ist Deutsch.
Für die Beilegung von Streitigkeiten mit der Bank besteht für Privatkunden die Möglichkeit, den Ombudsmann der privaten Banken anzurufen. Die Beschwerde ist in Textform (z.B. mittels Brief, Telefax oder E-Mail) an die Kundenbeschwerdestelle beim Bundesverband deutscher Banken e.V., Postfach 04 03 07, 10062 Berlin, Telefax: (030) 1663-3169, E-Mail: ombudsmann@bdb.de, zu richten.

Bei Vertragsabschluss im Wege des Fernabsatzes (z.B. Brief, Fax, E-Mail) gilt folgende Widerrufsbelehrung:

Widerrufsbelehrung

Widerrufsrecht
Sie können Ihre Vertragserklärung innerhalb von 14 Tagen ohne Angabe von Gründen mittels einer eindeutigen Erklärung widerrufen. Die Frist beginnt nach Erhalt dieser Belehrung auf einem dauerhaften Datenträger, jedoch nicht vor Vertragsschluss und auch nicht vor Erfüllung unserer Informationspflichten gemäß Artikel 246b § 2 Absatz 1 in Verbindung mit Artikel 246b § 1 Absatz 1 EGBGB. Zur Wahrung der Widerrufsfrist genügt die rechtzeitige Absendung des Widerrufs, wenn die Erklärung auf einem dauerhaften Datenträger (z.B. Brief, Telefax, E-Mail) erfolgt. Der Widerruf ist zu richten an:

Santander Consumer Bank AG, Santander-Platz 1, 41061 Mönchengladbach

Widerrufsfolgen
Im Falle eines wirksamen Widerrufs sind die beiderseits empfangenen Leistungen zurückzugewähren. Sie sind zur Zahlung von Wertersatz für die bis zum Widerruf erbrachte Dienstleistung verpflichtet, wenn Sie vor Abgabe Ihrer Vertragserklärung auf die Rechtsfolge hingewiesen wurden und ausdrücklich zugestimmt haben, dass wir vor dem Ende der Widerrufsfrist mit der Ausführung der Gegenleistung beginnen. Besteht eine Verpflichtung zur Zahlung von Wertersatz, kann dies dazu führen, dass Sie die vertraglichen Zahlungsverpflichtungen für den Zeitraum bis zum Widerruf dennoch erfüllen müssen. Ihr Widerrufsrecht erlischt vorzeitig, wenn der Vertrag von beiden Seiten auf Ihren ausdrücklichen Wunsch vollständig erfüllt ist, bevor Sie Ihr Widerrufsrecht ausgeübt haben. Verpflichtungen zur Erstattung von Zahlungen müssen innerhalb von 30 Tagen erfüllt werden. Die Frist beginnt für Sie mit der Absendung Ihrer Widerrufserklärung, für uns mit deren Empfang.

Ende der Widerrufsbelehrung

II. Bedingungen für das Online Banking

Die nachfolgenden Bedingungen für die Nutzung des Online Banking liegen den Online Banking-Angeboten (nachfolgend Online Banking) bei der Santander Consumer Bank AG (nachfolgend Bank) zugrunde.

1 Leistungsangebot

(1) Der Konto-/Depotinhaber und dessen Bevollmächtigte können Bankgeschäfte mittels Online Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online Banking abrufen. Sie sind zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrages 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.

(2) Konto-/Depotinhaber 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 Online Banking gelten die mit der Bank gesondert vereinbarten Verfügungslimite.

2 Voraussetzungen zur Nutzung des Online Banking

Der Teilnehmer benötigt für die Nutzung des Online Banking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) 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),
- einmal verwendbare Transaktionsnummern (TAN),
- der Nutzungscode 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 Online Banking-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 TAN
- TAN-Generator, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist,
- Online Banking-App auf einem mobilen Endgerät (z.B. Mobiltelefon) zum Empfang oder Erzeugung von TAN,
- mobiles Endgerät (z B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
- Chipkarte mit Signaturfunktion oder
- sonstiges Authentifzierungsinstrument, auf dem sich Signaturschlüssel befinden.

3 Zugang zum Online Banking

Der Teilnehmer erhält Zugang zum Online Banking, wenn

- dieser die Kontonummer oder seine individuelle Teilnehmerkennung und seine PIN oder elektronische Signatur übermittelt 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 8.1 und 9) 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 3).

4 Online Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Online Banking-Aufträge (z.B. Überweisungen) zu deren Wirksamkeit mit dem von der Bank bereit gestellten 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 3) auslöst und übermittelt.

4.2 Widerruf von Aufträgen

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

5 Bearbeitung von Online Banking-Aufträgen durch die Bank

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

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

- Der Teilnehmer hat 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.
- 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 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 Banking-Auftrag nicht ausführen. Sie wird den 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.

6 Information des Kontoinhabers über Online Banking-Verfügungen

Die Bank unterrichtet den Kontoinhaber, sofern nicht abweichend vereinbart, mindestens einmal monatlich über die mittels Online Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7 Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum Online Banking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online Banking über die von der Bank gesondert mitgeteilten Online Banking-Zugangskanäle (z.B. Internetadresse) herzustellen. Zur Auslösung 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 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 der Kenntnis des dazugehörigen Personalisierten Sicherheitsmerkmals das Online Banking-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 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 elektronisch gespeichert werden.
- 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 z.B. eines Auftrags oder der Aufhebung einer Sperre nicht mehr als eine TAN verwenden.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z.B. Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.

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.

7.4 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.

8 Anzeige- und Unterrichtungspflichten

8.1 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 Personalisierten 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.

8.2 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.

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 Online Banking-Zugang für ihn oder alle Teilnehmer [oder
- sein Authentifizierungsinstrument].

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Online Banking-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, den Online Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder 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 auf dem vereinbarten Weg 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.

9.4 Automatische Sperre eines chip-basierten Authentifizierungsinstruments

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

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

(3) Die in Absätzen 1 und 2 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 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 nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z.B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft.)

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

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen 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 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 8.1 Absatz 1),
- das Personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe Nummer 7.2 Absatz 2 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1),
- das Personalisierte Sicherheitsmerkmal per E-Mail weitergegeben hat (siehe Nummer 7.2 Absatz 2 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 4. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2 5. Spiegelstrich),
- 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 6. Spiegelstrich).

(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. eine TAN) oder Inhärenz (etwas, das der Teilnehmer ist, z.B. Fingerabdruck).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

(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 erster Spiegelstrich und findet keine Anwendung.

10.2.2 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.

10.2.3 Haftung der Bank ab der Sperranzeige

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

10.2.4 Haftungsausschluss

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