



Kundeninformation
mit Erläuterungen zu den Änderungen der Sonderbedingungen für das Online-Banking
zum 14. September 2019

Sehr geehrte Kundin,
sehr geehrter Kunde,

am 14. September 2019 treten neue gesetzliche Bestimmungen für die Erbringung von Zahlungsdiensten in Kraft. Diese haben ihren Ursprung in europäischen Vorgaben der Zweiten EU-Zahlungsdiensterichtlinie. Sie dienen vor allem der Gewährleistung der Sicherheit im Online-Banking. Deshalb ändern wir mit Wirkung zum 14. September 2019 die Sonderbedingungen für das Online-Banking, die wir Ihnen als Anlage beifügen. Erläuterungen zu den wesentlichen Änderungen können Sie dieser Kundeninformation entnehmen.

I. Sicherheit durch Kundenauthentifizierung

Wenn Sie als Kunde eine Zahlung per Online-Banking auslösen, nutzen Sie die mit uns als Bank vereinbarten Authentifizierungselemente, wie z. B. Online-PIN und -TAN. So können wir feststellen, dass tatsächlich Sie als unser Kunde diese Vorgänge berechtigterweise veranlasst haben. Die Zweite EU-Zahlungsdiensterichtlinie erkennt diese Authentifizierungsverfahren an und regelt diese nunmehr gesetzlich:

- Grundsätzlich soll bei jeder Transaktion eine starke Kundenauthentifizierung erfolgen. Das erfordert, dass Authentifizierungselemente aus den Kategorien Wissen, Besitz und Sein (z. B. eine PIN als Wissensselement oder ein Mobiltelefon, an welches eine TAN übermittelt wird, als Besitzelement) einzusetzen sind. Das bedeutet für Sie konkret, dass Sie beispielsweise beim Zugriff auf Kontoinformationen in der Regel zwei Authentifizierungselemente – Online-PIN und -TAN – einsetzen müssen, wie Sie es bereits bisher gewohnt sind.
- Allerdings geben die gesetzlichen Vorschriften uns als Bank die Möglichkeit, in bestimmten Fällen den Einsatz nur eines Authentifizierungselements anzufordern. So können wir z. B. beim wiederholten Abruf von Kontoinformationen innerhalb einer bestimmten Zeitspanne auch nur die Online-PIN verlangen. Weitere Ausnahmemöglichkeiten bestehen beispielsweise bei Überweisungen an vertrauenswürdige Empfänger, auf Eigenkonten und bei Kleinbetragszahlungen.

II. Einzelne Änderungen der Sonderbedingungen für das Online-Banking

1. Beschreibung des Einsatzes der Authentifizierungselemente

Die Regelungen über Authentifizierungselemente sind neu gefasst worden, um einerseits den neuen gesetzlichen Vorgaben Rechnung zu tragen und andererseits die Vielfalt an möglichen Authentifizierungsverfahren technikneutral zu erfassen. Das bedeutet im Einzelnen:

- In Nummer 2 der Bedingungen wird der neue Begriff „Authentifizierung“ eingeführt. Dabei handelt es sich um das Verfahren, mit dessen Hilfe die Bank Ihre Identität oder die berechtigte Verwendung eines vereinbarten Zahlungsinstrumentes überprüfen kann (Nummer 2 Absatz 2). Ihre Authentifizierung ist die Voraussetzung für die Nutzung des Online-Banking (Nummer 2 Absatz 1). Sie erfolgt anhand der zwischen Ihnen und der Bank vereinbarten Authentifizierungselemente (Nummer 2 Absatz 2 und Absatz 4).
- In Nummer 2 Absatz 3 wird der neue Begriff „Authentifizierungselemente“ eingeführt. Dies sind:
 - Wissensselemente, also etwas, das nur Sie wissen (z. B. eine PIN),
 - Besitzelemente, also etwas, das nur Sie besitzen (z. B. Ihre girocard mit TAN-Generator oder ein Mobiltelefon, an welches eine TAN übermittelt wird), oder
 - Seinselemente, also etwas, das nur Sie sind (z. B. Ihr Fingerabdruck als biometrisches Merkmal).
- Mit Authentifizierungselementen können Sie sich im Online-Banking als berechtigter Teilnehmer ausweisen, auf Informationen (z. B. Kontostand und Umsätze) zugreifen sowie Aufträge (z. B. Überweisungen) erteilen (Nummer 2 Absatz 4). Welche Authentifizierungselemente Sie im Online-Banking einsetzen müssen, richtet sich nach der Vereinbarung zwischen Ihnen und Ihrer Bank und der jeweiligen Anforderung durch die Bank.
- In Nummern 3 und 4 wird der Einsatz der Authentifizierungselemente beschrieben, um Zugang zum Online-Banking und Zugriff auf Informationen (z. B. Kontodaten) zu erhalten und Aufträge zu erteilen. Wichtig ist, dass wir als Bank von Ihnen die jeweils erforderlichen Authentifizierungselemente anfordern (z. B. bei Erteilung eines Zahlungsauftrags Online-PIN und -TAN), damit wir prüfen können, wer handelt.
- Aufgrund der Einführung des Begriffs „Authentifizierungselemente“ haben sich auch weitere Regelungen geändert. So sind die Authentifizierungselemente nunmehr der Bezugspunkt für die Sorgfaltspflichten (Nummer 7.1), der Pflicht zur Sperranzeige (Nummer 8.1), der Nutzungssperre (Nummer 9) und der Regelungen zu Haftung (Nummer 10).



2. Sorgfaltspflichten zum Schutz der Sicherheit des Online-Banking

Aufgrund der neuen gesetzlichen Bestimmungen und der damit einhergehenden technischen Anpassungen an die neuen Sicherheitsanforderungen haben sich auch Ihre Sorgfaltspflichten als Teilnehmer im Online-Banking geändert (Nummer 7.1). Zum Schutz Ihrer

Authentifizierungselemente vor unbefugtem Zugriff müssen Sie alle zumutbaren Vorkehrungen treffen. Anderenfalls besteht die Gefahr, dass das Online-Banking nicht autorisiert oder missbräuchlich genutzt wird. So müssen Sie nach Nummer 7.1 Absatz 2 insbesondere

- Ihre Wissens Elemente (z. B. Ihre PIN) geheim halten,
- Ihre Besitzelemente (z. B. Ihre girocard mit TAN-Generator oder Ihr Mobiltelefon, an welches eine TAN übermittelt wird) vor Missbrauch schützen und
- bei der Verwendung von Seinelementen (z. B. Ihr Fingerabdruck als biometrisches Merkmal) beachten, dass auf Ihrem mobilen Endgerät (z. B. Mobiltelefon mit Finger-abdrucksensor) keine anderen Seinelemente anderer Personen gespeichert sind.

Wir bitten Sie, die Sorgfaltspflichten sorgfältig zu lesen. Indem Sie die Sorgfaltspflichten be-achten, schützen Sie Ihr Online-Banking und reduzieren die Betrugsrisiken. Bei vorsätzlicher oder grob fahrlässiger Verletzung der Sorgfaltspflichten könnten Sie für den hieraus entstandenen Schaden haften.

3. Nutzung des Online-Banking mittels Kontoinformationsdiensten, Zahlungsauslösediensten und sonstigen Drittdiensten

Sie können das Online-Banking auch mittels Kontoinformationsdiensten, Zahlungsauslöse-diensten und von Ihnen ausgewählten, sonstigen Drittdiensten nutzen (Nummer 1 Absatz 1). Ihre Authentifizierungselemente dürfen Sie gegenüber einem von ihnen ausgewählten Zah-lungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst ver-wenden. Sofern Sie sonstige Drittdienste nutzen, müssen Sie diese sorgfältig auswählen (Nummer 7.1 Absatz 5).

Den gesetzlichen Regelungen entsprechend kann die Bank nach Nummer 9.5 Kontoinforma-tions- und Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformations- oder des Zahlungsauslö-sedienstleisters zum Zahlungskonto es rechtfertigen. Über die Sperre sowie ggf. über die Aufhebung der Sperre wird der Kontoinhaber informiert.



Sonderbedingungen für das Online-Banking

Fassung: September 2019

Gültig ab 14.09.2019

1 Leistungsangebot

- (1) Der Kunde 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. Des Weiteren sind sie gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absätze 33 und 34 Zahlungsdienstestaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.
- (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 Online-Banking gelten die mit der Bank gesondert vereinbarten Verfügungsmitel. Eine Änderung dieser Mitel kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

2 Voraussetzungen zur Nutzung des Online-Banking

- (1) Der Teilnehmer kann das Online-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 überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).
- (3) Authentifizierungselemente sind
 - Wissensselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer PIN oder der Nutzungscode für die elektronische Signatur) und
 - Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern TAN, die den Besitz des Teilnehmers nachweisen, wie die girocard mit TAN-Generator oder das mobile Endgerät), sowie
 - 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 Wissensselement, 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 Teilnehmerkennung (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 8.1 und 9 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 Absatz 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 Absatz 26 Satz 2 ZAG).

4 Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss einem Auftrag (z. B. Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z. B. Eingabe einer TAN oder elektronische Signatur als Nachweis des Besitzelements) zu verwenden, sofern mit der Bank nichts anderes vereinbart wurde.

Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines 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 Aufträgen durch die Bank

- (1) Die Bearbeitung der 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 Arbeitslaufs. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis“ angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Online-Banking-Seite der Bank oder „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.
- (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 (z. B. Wertpapierorder) liegt vor.
 - Das Online-Banking-Datenformat ist eingehalten.
 - Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten (vgl. Nummer 1 Absatz 3 dieser Bedingungen).
 - Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Sonderbedingungen für den Überweisungsverkehr) liegen vor.Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die 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 Auftrag nicht ausführen und dem Teilnehmer eine Information 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-Banking zur Verfügung stellen.

6 Information des Kunden über Online-Banking-Verfügungen

Die Bank unterrichtet den Kunden mindestens einmal monatlich über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.



7 Sorgfaltspflichten des Teilnehmers

7.1 Schutz der Authentifizierungselemente

- (1) Der Teilnehmer 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 Online-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vgl. Nummern 3 und 4 dieser Bedingungen).
- (2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:
- (a) Wissensselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere
- nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden,
 - nicht außerhalb des Online-Banking in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben 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. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinelements (z. B. mobiles Endgerät mit Anwendung für das Online-Banking und Fingerabdrucksensor) dient.
- (b) Besitzelemente, wie z. B. die girocard mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
- sind die girocard mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
 - ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (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) Seinelemente, 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 Seinelemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online-Banking genutzt wird, Seinelemente anderer Personen gespeichert, ist für das Online-Banking das von der Bank ausgegebene Wissensselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinelement.
- (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.
- (4) 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.
- (5) 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 3 und 4 dieser Bedingungen). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

7.2 Sicherheitshinweise der Bank

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

7.3 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 (z. B. 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. Bei Feststellung von Abweichungen ist die Transaktion abzubrechen.

8 Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

- (1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. girocard mit TAN-Generator, mobiles Endgerät; Signaturkarte) oder
 - die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines 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.

8.2 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.

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 dieser Bedingungen,
- den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
 - seine Authentifizierungselemente zur Nutzung des Online-Banking.

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 der Authentifizierungselemente des Teilnehmers dies rechtfertigen oder
 - der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.
- (2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.



9.3 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.

9.4 Automatische Sperre eines Chip-basierten Besitzelements

- (1) Eine Chipkarte mit Signaturfunktion sperrt sich selbst, wenn der Nutzungscode für die elektronische Signatur dreimal in Folge falsch eingegeben wird.
- (2) Ein TAN-Generator als Bestandteil einer Chipkarte, der die Eingabe eines eigenen Nutzungscode erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.
- (3) Die in den Absätzen 1 und 2 genannten Besitzelemente 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.

9.5 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.

10. Haftung

10.1 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 (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

10.2.1 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 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 7.1 Absatz 2,
 - Nummer 7.1 Absatz 4,
 - Nummer 7.3 oder
 - Nummer 8.1 Absatz 1dieser 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 des § 1 Abs. 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 Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.
- (6) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 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 finden keine Anwendung, 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 nach Absätzen 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 findet keine Anwendung.

10.2.2 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.

10.2.3 Haftung 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.

11 Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit

Für die Beilegung von Streitigkeiten mit der Bank kann sich der Teilnehmer an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- oder Beschwerdestellen wenden