Bedingungen für das Online-Banking
unter Nutzung der App oder der browserbasierten Nutzeroberfläche des Partners der solarisBank

Für die Nutzung des von der solarisBank AG (nachstehend: „Bank“) ermöglichten Online Banking über die app- oder browserbasierte Nutzeroberfläche des Partners der solarisBank (im Folgenden „Nutzeroberfläche“) gelten die folgenden Sonderbedingungen neben den Allgemeinen Geschäftsbedingungen der Bank.

1. Leistungsangebot

(1) Der ~~Konto-/Depotinhaber~~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 Zahlungsdiensteaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.~~Sie sind zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrags einen Zahlungsauslösedienst gemäß § Abs. 33 Zahlungsdiensteaufsichtsgesetz zu nutzen.~~

(2) ~~Konto-/Depotinhaber~~Kunden und Bevollmächtigte werden einheitlich als „Teilnehmer“, Konto und Depot einheitlich als „Konto“ bezeichnet, es sei denn, dieses ist ausdrücklich anders bestimmt.

(3) Zur Nutzung des Online-Bankings gelten die mit der Bank gesondert vereinbarten Verfügungslimite.

2. Voraussetzungen zur Nutzung des Online-Banking~~s~~

(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 zu- greifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).

(3) Authentifizierungselemente sind

- Wissenselemente, also etwas, das nur der Teilnehmer weiß (z.B. persönliche Identifikationsnummer (PIN)),
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z.B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern (TAN), die den Besitz des Teilnehmers nachweisen, wie die girocard mit TAN-Generator oder das mobile Endgerät), oder
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z.B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

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

~~Der Teilnehmer benötigt für die Nutzung des Online-Bankings 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 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).~~

~~**2.2 Authentifizierungsinstrumente**~~

~~Authentifizierungsinstrumenten sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurden und die vom Teilnehmer zur Erteilung eines Online-Banking-Auftrages verwendet werden. Insbesondere mittels folgender Authentifizierungsinstrumente kann das personalisierte Sicherheitsmerkmal (z.B. TAN) dem Teilnehmer zur Verfügung gestellt werden:~~
~~– Online-Banking-App auf einem mobilen Endgerät (z.B. Mobiltelefon) zum Empfang oder zur Erzeugung von TAN~~
~~– über eine iOS- oder Android-Anwendung mittels sog. Device Binding~~
~~– mobiles Endgerätes (zum Beispiel Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN)~~
~~– Chipkarte mit Signaturfunktion~~
~~– sonstiges Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden~~
~~Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.~~

~~Die Bank kann die Liste der zulässigen Authentifizierungsinstrumente erweitern oder einschränken und teilt dies dem Teilnehmer mindestens zwei Monate vor dem Ausschluss bestehender bzw. der Aufnahme neuer Authentifizierungsinstrumente in die Liste mit.~~

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). ~~Der Teilnehmer erhält Zugang zum Online-Banking, wenn~~

~~dieser die Kontonummer oder seine individuelle Kundenkennung und seine PIN oder elektronische Signatur übermittelt 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 Nr. 1 Abs. 1 Satz 3).~~

4. ~~Online-Banking-~~Aufträge

4.1 Auftragserteilung ~~und Autorisierung~~

Der Teilnehmer muss einem Auftrag (zum Beispiel Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (zum Beispiel Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden.

Die Bank bestätigt mittels Online Banking den Eingang des Auftrags. ~~Der Teilnehmer muss Online-Banking-Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit mit dem von der Bank bereitgestellten 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 Zahlungsaufträge über einen Zahlungsauslösedienst auslöst und Zahlungskontoinformationen über einen Kontoinformationsdienst anfordert (siehe Nr. 1 Abs. 1 Satz 3).~~

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Online-Banking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit 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 (zum Beispiel Überweisung) auf der Online-Banking-Seite der Bank oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. 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 Bankarbeitstag gemäß „Preis- und Leistungsverzeichnis" der Bank, so gilt der Auftrag als am darauf folgenden Bankarbeitstag 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 (vgl. Nummer 4.1 dieser Bedingungen).
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (zum Beispiel Wertpapierorder) liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.
- Die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel 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 (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach ~~Abs.~~Absatz 2 Satz 1~~, Punkt 1-5~~ nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen. Sie wird dem Teilnehmer hierüber mittels Online-Banking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können. Dieses gilt nicht, wenn die Angabe von Gründen gegen sonstige Rechtsvorschriften verstößt.

6. Information des ~~Kontoinhabers~~ Kunden über Online-Banking-Verfügungen

Die Bank unterrichtet den ~~Kontoinhaber~~ Kunden 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~~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 (vergleiche Nummer 3 und 4 dieser Bedingungen).

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

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

- nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des 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 Seinselements (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 Text- form (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden und
- muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z.B. Mobiltelefon mit Anwendung für das Online Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online Banking des Teilnehmers aktivieren.

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

(3) Die für das mobile-TAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Online Banking nicht mehr nutzt.

(4) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 4 darf der Teilnehmer seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden (siehe Nummer 1 Absatz 1 Sätze 3 und 4 dieser Bedingungen). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

~~Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online-Banking nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle (zum Beispiel Internetadresse) herzustellen. Zur Auslösung eines Zahlungsauftrages 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 Abs. 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 und vor unbefugtem Zugriff zu schützen und nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln sowie~~

~~sein Authentifizierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren (Verwahrungspflichten).~~

~~Für die Erfüllung der Verwahrungspflichten hat der Teilnehmer alle zumutbaren Vorkehrungen zu treffen. Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit der Kenntnis des dazugehörigen personalisierten Sicherheitsmerkmales das Online-Banking-Verfahren missbräuchlich nutzen. Dies könnte zu einer Haftung des Konto-/Depotinhabers nach Nummer 10.2. führen. Die Geheimhaltungspflicht bezüglich der personalisierten Sicherheitsmerkmale nach Satz 1 gilt nicht, wenn der Teilnehmer diese zur Erteilung eines Zahlungsauftrages oder zum Abruf von Informationen über ein Zahlungskonto an den von ihm ausgewählten Zahlungsauslösedienst beziehungsweise Kontoinformationsdienst übermittelt (siehe Nummer 1 Abs. 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 zum Beispiel eines Auftrags oder zur Aufhebung einer Sperre nicht mehr als eine TAN verwenden.~~

~~Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN~~

~~empfangen werden (zum Beispiel Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.~~

7.2~~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.

7.3~~4~~ ~~Kontrolle~~ Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (zum Beispiel mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

~~Soweit die Bank dem Teilnehmer Daten aus seinem Online-Banking-Auftrag (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapier-Kennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (zum Beispiel 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 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

~~- den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung 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.~~

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. ~~(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~~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 ~~o~~oder
- seine Authentifizierungselemente zur Nutzung des Online-Banking~~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 der~~s Authentifizierungsinstruments~~ Authentifizierungselemente ~~des Teilnehmers oder des personalisierten Sicherheitsmerkmals~~ dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung ~~des~~ eines ~~Authentifizierungsinstruments~~ Authentifizierungselements besteht.

(2) Die Bank wird den ~~Konto-/Depotinhaber~~Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre 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 ~~das personalisierte Sicherheitsmerkmal beziehungsweise das~~ die betroffenen ~~Authentifizierungsinstrument~~ Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den ~~Konto-/Depotinhaber~~Kunden unverzüglich.

9.4 Automatische Sperre eines chip-basierten ~~Authentifizierungsinstruments~~Besitzelements

(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.

(32) ~~Das in~~ Die in ~~Absatz 1~~ Absätzen 1 und 2 genannten ~~Authentifizierungsinstrument~~ Besitzelemente ~~kann~~ 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~~r~~ nicht autorisierten ~~Online-Banking-Verfügung~~Auftrags und eines~~r~~ nicht, fehlerhaft oder verspätet ausgeführten ~~Online-Banking-Verfügung~~Auftrags

Die Haftung der Bank bei einem~~r~~ nicht autorisierten ~~Online-Banking-Verfügung~~ Auftrag und einem~~r~~ nicht, fehlerhaft oder verspätet ausgeführten Auftrag ~~Online-Banking-Verfügung~~ richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des ~~Konto-/Depotinhabers~~Kunden bei missbräuchlicher Nutzung ~~eines personalisierten Sicherheitsmerkmales oder eines~~ seiner Authentifizierungselemente~~Authentifizierungsinstruments~~

10.2.1 Haftung des ~~Kontoinhabers~~ Kunden 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 Authentifizierungselements~~Authentifizierungsinstruments~~ oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements~~Authentifizierungsinstruments~~, haftet der ~~Kontoinhaber~~ Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der ~~Kontoinhaber~~ 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~~Authentifizierungsinstruments~~ vor dem~~n~~ nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Authentifizierungselements~~Authentifizierungsinstruments~~ durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine Stelle, an die die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerische Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der ~~Kontoinhaber~~ 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 1

dieser Bedingungen verletzt hat.~~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 Abs. 1),~~
~~das personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2 Abs. 2 1. Spiegelstrich),~~
~~das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Abs. 1 2. Spiegelstrich),~~
~~das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Abs. 2 3. Spiegelstrich),~~
~~das personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Abs. 2 4. Spiegelstrich),~~
~~das personalisierte Sicherheitsmerk-mal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Abs. 2 5. Spiegelstrich),~~
~~mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Abs. 2 6. Spiegelstrich),~~
~~beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Online-Banking genutzt (siehe Nummer 7.2 Abs. 2 7. Spiegelstrich).~~

(4) Abweichend von den Absätzen 1 und 3 ist der ~~Kontoinhaber~~ Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 ~~Abs.~~Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt hat.~~, obwohl die Bank zur starken Kundenauthentifizierung nach § 68 Abs. 4 Zahlungsdiensteaufsichtsgesetz verpflichtet war.~~ Eine starke Kundenauthentifizierung erfordert insbesondere die

Verwendung von zwei voneinander unabhängigen Authentifizierungse~~E~~lementen aus den Kategorien Wissen ~~(etwas, das der Teilnehmer weiß, z.B. PIN)~~, Besitz ~~(etwas, das der Teilnehmer besitzt, z.B. TAN-Generator)~~ oder ~~Inhärenz~~ Sein ~~(etwas, das der Teilnehmer ist, z.B. Fingerabdruck)~~(siehe Nummer 2 Absatz 3 dieser Bedingungen).

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

(6) Der ~~Kontoinhaber~~ Kunde 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 Abwendung, 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 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 findet keine Anwendung.

10.2.2 Haftung des ~~Depotinhabers~~ 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 ~~Authentifizierungsinstruments~~ Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements~~personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments~~ und ist der Bank hierdurch ein Schaden entstanden, haften der ~~Depotinhaber~~ Kunde 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.

11. Erklärungen der Bank und Kontoauszüge

(1) Im Rahmen der Geschäftsbeziehung zwischen der Bank und dem Kunden ist die Nutzeroberfläche die vereinbarte Empfangsvorrichtung des Kunden. Mitteilungen und Erklärungen der Bank werden dem Kunden – soweit nicht die Schriftform mit dem Kunden ausdrücklich vereinbart wurde oder gesetzlich erforderlich ist – in elektronischer Form mittels der Nutzeroberfläche zur Verfügung gestellt.

(2) Über die Nutzeroberfläche werden dem Kunden Mitteilungen und Erklärungen betreffend das Geschäftsverhältnis mit der Bank verschlüsselt von der Bank bereitgestellt. Mitteilungen und Erklärungen, die über die Nutzeroberfläche bereitgestellt werden, werden nur dann zusätzlich postalisch versandt, wenn es aus rechtlichen Gründen erforderlich ist.

Die Bank ist ungeachtet der Nutzung der Nutzeroberfläche durch den Kunden als elektronisches Kommunikationsmedium berechtigt, einzelne oder bei technischen Problemen alle Mitteilungen und Erklärungen auf dem Postweg oder in sonstiger Weise an den Kunden zu übermitteln, wenn sie dies unter Berücksichtigung des Kundeninteresses als zweckmäßig erachtet.

Die Bank wird den Kunden über die Einstellung bestimmter Dokumente über die Nutzeroberfläche selbst oder über den Partner der Bank per E-Mail, SMS oder über einen anderen mit dem Kunden vereinbarten Weg informieren.

(3) Der Kunde ist verpflichtet, regelmäßig und zeitnah Mitteilungen und Erklärungen über die Nutzeroberfläche abzurufen und die Inhalte zu prüfen, sobald die Bank ihn über die Einstellung der Mitteilungen und Erklärungen informiert hat. Eventuelle Unstimmigkeiten sind der Bank unverzüglich, spätestens jedoch sechs Wochen nach Bereitstellung, anzuzeigen.

(4) Sämtliche Mitteilungen und Erklärungen, die dem Kunden über die Nutzeroberfläche übermittelt werden, gelten mit Information der Bank an den Kunden über die Einstellung und Möglichkeit des Abrufs über die Nutzeroberfläche als zugegangen. Bank und Kunde vereinbaren demgemäß, dass die Nutzeroberfläche die Vorrichtung des Kunden zum Empfang jeglicher Mitteilungen und Erklärungen der Bank, insbesondere von Kontoauszügen und Rechnungsabschlüssen, ist.

(5) Die Bank stellt die Unveränderbarkeit der Daten in der Nutzeroberfläche sicher. Diese Pflicht gilt nicht, soweit die Daten außerhalb der Nutzeroberfläche gespeichert oder aufbewahrt werden. Aufgrund der individuellen Hard- oder Softwareeinstellung stimmt ein Ausdruck optisch nicht immer mit der Darstellung am Bildschirm überein.

(6) Die Bank speichert alle von ihr über die Nutzeroberfläche bereitgestellten Dokumente dauerhaft während der laufenden Geschäftsbeziehung. Nach Beendigung der Geschäftsbeziehung kann der Kunde gegen Zahlung eines Entgeltes, das die Bank nach billigem Ermessen (§ 315 BGB) festsetzen kann, Zweitschriften der erteilten Kontoauszüge und Rechnungsabschlüsse von der Bank verlangen.

(7) Die sich aus §§ 675d ~~Abs.~~Absatz 1 Satz 1 BGB i.V.m. Art. 248 §§ 3-9 EGBGB und § 312i ~~Abs.~~Absatz 1 Satz 1 Nr. 1 bis 3 und Satz 2 BGB ergebenden Informationspflichten werden abbedungen, sofern der Kunde nicht Verbraucher im Sinne von § 13 BGB ist.