Sonderbedingungen Online-Banking

1. Leistungsangebot

(1) Der Kontoinhaber kann Bankgeschäfte mittels Online-Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Online-Banking abrufen. Die Bank ist berechtigt, dem Kunden die Änderung ihrer Geschäftsbedingungen auf elektronischem Weg anzuzeigen und zum Abruf bereitzustellen. Wegen des Wirksamwerdens der Änderungen verbleibt es bei der Regelung in Nummer 1 Abs. 2 der Allgemeinen Geschäftsbedingungen oder den mit dem Kunden vereinbarten abweichenden Regelungen.

2. Voraussetzungen zur Nutzung des Online-Banking

(1) Der Kontoinhaber 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 Kontoinhabers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Kontoinhabers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Kontoinhaber sich gegenüber der Bank als berechtigter Kontoinhaber ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).

(3) Authentifizierungselemente sind
- Wissenselemente, also etwas, das nur der Kontoinhaber weiß (z.B. persönliche Identifikationsnummer [PIN] oder der Nutzungscode für die elektronische Signatur) und
- Besitzelemente, also etwas, das nur der Kontoinhaber besitzt (z.B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN], die den Besitz des Kontoinhabers nachweisen, wie das mobile Endgerät, sowie
- Seinselemente, also etwas, das der Kontoinhaber ist (Inhärenz, z.B. Fingerabdruck als biometrisches Merkmal des Kontoinhabers).

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

3. Zugang zum Online-Banking

(1) Der Kontoinhaber erhält Zugang zum Online-Banking der Bank, wenn
- dieser die Online-Banking ID und sein Passwort übermittelt hat,
- dieser sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Kontoinhabers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9) 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 Abs. 26 Satz 1 ZAG (z.B. zum Zweck der Änderung der Anschrift des Kunden) fordert die Bank den Kontoinhaber auf, sich unter Verwendung eines weiteren Authentifizierungselements, wie die Eingabe einer mobile TAN, auszuweisen.

4. Aufträge

4.1 Auftragserteilung

Der Kontoinhaber muss einem Auftrag (zum Beispiel Überweisung) zu deren Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z.B. Eingabe einer TAN oder elektronische Signatur als Nachweis des Besitzelements oder Nutzung der elektronischen Signatur als Nachweis des Wissenselements) zu verwenden, sofern mit der Bank nicht 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 Widerrufmöglichkeit 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 (zum Beispiel Überweisung) auf der Online-Banking-Seite der Bank bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank oder im Arbeitsablaufes angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Online-Banking-Seite der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- Der Kontoinhaber hat den Auftrag autorisiert.
- Die Berechtigung des Kontoinhabers für die jeweilige Auftragsart liegt vor (vgl. Nummer 4.1 dieser Bedingungen).
- Das Online-Banking-Datenformat ist eingehalten.

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) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen und dem Kontoinhaber 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 eine Information zur Verfügung stellen.

6. Information des Kontoinhabers über Online-Banking-Verfügungen

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

7. Sorgfaltspflichten des Kontoinhabers

7.1 Schutz der Authentifizierungsinstrumente

(1) Der Kontoinhaber 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 wird (vgl. Nummern 3 und 4 dieser Bedingungen).

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

(a) Wissenselemente, wie z.B. die PIN oder der Nutzungscode für die elektronische Signatur, sind geheim zu halten; sie dürfen insbesondere
- nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des Online-Bankings in Textform (z.B. per E-Mail, Messanger-Dienst) weitergegeben werden,
- nicht ungesichert elektronisch gespeichert (z.B. Speicherung der PIN im Klartext im PC 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. mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselement (z.B. mobiles Endgerät mit Anwendung für das Online-Banking und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z.B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
- ist die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Kontoinhabers (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 Kontoinhabers zu deaktivieren, bevor der Kontoinhaber 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-Bankings mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messanger-Dienst) weitergegeben werden und
- muss der Kontoinhaber, 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 Kontoinhabers aktivieren.

(c) Seinselemente, wie z.B. Fingerabdruck des Kontoinhabers, dürfen auf einem mobilen Endgerät des Kontoinhabers für das Online-Ban-

king 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) 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 Kontoinhaber diese Telefonnummer für das Online-Banking nicht mehr nutzt.

7.2 Sicherheitshinweise der Bank

Der Kontoinhaber 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 Kontoinhaber die von ihr empfangenen Auftragsdaten (z.B. Betrag, Kontonummer) über das gesondert vereinbarte Gerät des Kontoinhabers an (z.B. mittels mobilen Endgeräts). Der Kontoinhaber 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 Kontoinhaber
- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z.B. mobiles Endgerät) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements fest, muss der Kontoinhaber die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Kontoinhaber kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.

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

(3) Hat der Kontoinhaber 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 Kontoinhabers

Die Bank sperrt auf Veranlassung des Kontoinhabers, insbesondere im Fall der Sperranzeige nach Nummer 8.1 dieser Bedingungen,
- den Online-Banking-Zugang für ihn oder
- seine Authentifizierungselemente zur Nutzung des Online-Banking.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Online-Banking-Zugang für den Kontoinhaber sperren, wenn
- sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Kontoinhabers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

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. 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.

Eine Aufhebung der Sperre kann vom Kunden nicht mittels Online-Banking veranlasst werden und ist nur telefonisch über die Servicenummer der SWK Bank möglich, wenn die Gründe für die Sperre nicht mehr gegeben sind.

9.4 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 verspätetet 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 Authentifizierungsinstruments 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 Kontoinhaber ein Verschulden trifft.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach Abs. 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 Zweiniederlassung 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 Kontoinhaber 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 Kontoinhabers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach
- Nummer 7.1 Abs. 2,
- Nummer 7.1 Abs. 4,
- Nummer 7.3 oder
- Nummer 8.1 Abs. 1,

dieser Bedingungen verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Kontoinhaber 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 Abs. 3 dieser Bedingungen).

(5) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 3 verpflichtet, wenn der Kontoinhaber die Sperranzeige nach Nummer 8.1 dieser Bedingungen nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hat.

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

10.2.2 Haftung des Kunden bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten vor der Sperranzeige

Beruhen nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten 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 der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Kontoinhabers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-Banking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Kontoinhaber 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 Kunde an die in den Allgemeinen Geschäftsbedingungen näher bezeichneten Streitschlichtungs- oder Beschwerdestellen wenden.