

Bedingungen für das Onlinebanking

1. Leistungsangebot

- (1) Der Kunde kann Bankgeschäfte über sein Konto mittels Onlinebanking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Onlinebanking abrufen.
- (2) Zur Nutzung des Onlinebanking gelten die mit der Bank ggf. gesondert vereinbarten Verfügungslimite.

2. Voraussetzungen zur Nutzung des Onlinebanking

Der Kunde benötigt für die Abwicklung von Bankgeschäften mittels Onlinebanking die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als zum Onlinebanking berechtigter Kunde auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4).

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN)

2.2 Authentifizierungsinstrumente

Die TAN können dem Kunden auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:

- auf einer Liste mit einmal verwendbaren TAN,
- mittels eines mobilen Endgerätes (zum Beispiel Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN)

2.3 Besondere Regelungen für das mobile TAN-Verfahren

Für die Teilnahme am mobilen TAN-Verfahren ist ein Mobiltelefon mit deutscher SIM-Karte erforderlich. Das Mobiltelefon besteht aus dem mobilen Telekommunikations-Endgerät sowie aus der SIM-Karte des Telekommunikationsnetzbetreibers. Für das mobile TAN-Verfahren wird der mobile Telekommunikationsanschluss (inklusive der dazugehörigen Rufnummer) des Kunden bei der Bank registriert. Zur Durchführung von Transaktionen im Onlinebanking erhält der Kunde von der Bank auf Anforderung durch eine Online-Anwendung für jede Transaktion eine Textmeldung (SMS) mit einer TAN auf das registrierte Mobiltelefon. Die in der SMS angegebene TAN ist nur für die Transaktion gültig, für die sie angefordert wurde. Stellt der Kunde den Verlust seines mobilen Telekommunikations-Endgerätes oder der SIM-Karte fest oder besteht der Verdacht einer mißbräuchlichen Nutzung, ist der Kunde verpflichtet, die Bank unverzüglich zu benachrichtigen. Zusätzlich ist er verpflichtet, die SIM-Karte beim jeweiligen Telekommunikationsnetzbetreiber sperren zu lassen.

3. Zugang zum Onlinebanking

Der Kunde erhält Zugang zum Onlinebanking, wenn

- dieser die Kontonummer oder seine individuelle Kundenkennung und seine PIN übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Kunden ergeben hat und

- keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt. Nach Gewährung des Zugangs zum Onlinebanking kann der Kunde Informationen abrufen oder Aufträge erteilen.

4. Onlinebanking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Kunde muss Onlinebanking-Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit mit dem vereinbarten personalisierten Sicherheitsmerkmal (TAN) autorisieren und der Bank mittels Onlinebanking übermitteln. Die Bank bestätigt mittels Onlinebanking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Onlinebanking-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 Onlinebanking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Onlinebanking ausdrücklich vor.

5. Bearbeitung von Onlinebanking-Aufträgen durch die Bank

- (1) Die Bearbeitung der Onlinebanking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung) auf der Onlinebanking-Seite der Bank oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nicht an einem Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Bank zu, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen.
- (2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
 - der Kunde hat sich mit seinem personalisierten Sicherheitsmerkmal legitimiert;
 - die Berechtigung des Kunden für die jeweilige Auftragsart liegt vor;
 - das Onlinebanking-Datenformat ist eingehalten;
 - das gesondert vereinbarte Onlinebanking-Verfügungslimit ist nicht überschritten;
 - die 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 Onlinebanking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr) aus.
- (3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Onlinebanking-Auftrag nicht ausführen und dem Kunden über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Onlinebanking eine Information zur Verfügung stellen.

6. Information des Kunden über Onlinebanking-Verfügungen

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

7. Sorgfaltspflichten des Kunden

7.1 Technische Verbindung zum Onlinebanking

Der Kunde ist verpflichtet, die technische Verbindung zum Onlinebanking nur über die von der Bank gesondert mitgeteilten Onlinebanking-Zugangskanäle (zum Beispiel Internetadresse) herzustellen.

7.2 Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Kunde hat

- seine personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der Bank gesondert mitgeteilten Onlinebanking-Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument (siehe Nummer 2.2 und 2.3) vor dem Zugriff anderer Personen sicher zu verwahren. Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen personalisierten Sicherheitsmerkmal das Onlinebanking-Verfahren missbräuchlich nutzen.

(2) Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

- Das personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (zum Beispiel im Kundensystem).
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (zum Beispiel nicht auf Online-Händlerseiten).
- Das personalisierte Sicherheitsmerkmal darf nicht außerhalb des Onlinebanking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die PIN und die TAN-Liste dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Kunde darf zur Autorisierung zum Beispiel eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung einer neuen TAN-Liste 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 Onlinebanking genutzt werden.

7.3 Sicherheit des Kundensystems

Der Kunde muss die Sicherheitshinweise auf der Internetseite der Bank zum Onlinebanking, 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 Kunden Daten aus seinem Onlinebanking-Auftrag (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät des Kunden (zum Beispiel Mobiltelefon) zur Bestätigung anzeigt, ist der Kunde 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 Kunde

- den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines persönlichen Sicherheitsmerkmals fest, muss der Kunde die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Kunde kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

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

(3) Hat der Kunde 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 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 Kunden

Die Bank sperrt auf Veranlassung des Kunden, insbesondere im Fall der Sperranzeige nach Nummer 8.1

- den Onlinebanking-Zugang für ihn oder alle Kunden oder
- sein Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Onlinebanking-Zugang für einen Kunden sperren, wenn

- sie berechtigt ist, den Onlinebanking-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 Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre 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 Kunden unverzüglich.

10. Haftung

10.1 Haftung der Bank bei einer nicht autorisierten Onlinebanking-Verfügung und einer nicht oder fehlerhaft ausgeführten Onlinebanking-Verfügung

Die Haftung der Bank bei einer nicht autorisierten Onlinebanking-Verfügung und einer nicht oder fehlerhaft ausgeführten Onlinebanking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr).

10.2 Haftung des Kunden bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

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 abhanden gekommenen Authentifizierungsinstruments, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 EUR, ohne dass es darauf ankommt, ob den Kunden an dem Verlust, Diebstahl oder sonstigen Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.
- (2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 EUR, wenn der Kunde seine Pflicht zur sicheren Aufbewahrung der personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.
- (3) Ist der Kunde kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 EUR nach Absatz 1 und 2 hinaus, wenn der Kunde fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- (4) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Kunde die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

- (5) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Kunde seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kunde den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Kunden 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 im Kundensystem gespeichert hat (siehe Nummer 7.2 Absatz 2 1. Spiegelstrich),
 - das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1 2. Spiegelstrich),
 - das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2 3. Spiegelstrich),
 - das personalisierte Sicherheitsmerkmal außerhalb des Onlinebanking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2 4. Spiegelstrich),
 - das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 5. Spiegelstrich),
 - mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2 6. Spiegelstrich),
 - beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Onlinebanking nutzt (siehe Nummer 7.2 Absatz 2 7. Spiegelstrich).
- (6) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

10.2.2 Haftung der Bank ab der Sperranzeige

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

10.2.3 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.