Geschäftsbedingungen für Oberbank eBanking/App und HBCI-Service

1. Leistungsangebot

(1) Der Kontoinhaber und dessen Bevollmächtigte können Bankgeschäfte mittels eBanking bzw. HBCI-Service - im Folgenden als "HBCI" bezeichnet - in dem von der Oberbank AG – im Folgenden als „Bank“ bezeichnet - angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels eBanking bzw. HBCI abrufen. Der eBanking-Zugang beinhaltet explizit auch das mobile Internet mit dem Angebot einer Oberbank App für den Zugriff über mobile Endgeräte (Smartphones) (nachfolgend "App" genannt). Sie sind zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrages einen Zahlungsauslösedienst gemäß § 1 Absatz 33 Zahlungsdiensteaufsichtsgesetz und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienst gemäß § 1 Absatz 34 Zahlungsdiensteaufsichtsgesetz zu nutzen.

(2) Im Rahmen des Oberbank eBanking/App bzw. HBCI können verschiedene Dienstleistungen in Anspruch genommen werden. Die einzelnen Nutzungsmöglichkeiten ergeben sich aus dem dem Kunden bei Vereinbarung zur Nutzung des Services übergebenen Beiblatt. Die Bank behält sich vor, den daraus ersichtlichen Leistungsumfang der angebotenen Informationsmöglichkeiten bzw. Bankgeschäfte zu erweitern oder einzuschränken.

(3) Kontoinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

(4) Zur Nutzung des eBanking/App bzw. HBCI gelten die mit der Bank vereinbarten Verfügungslimite.

2. Voraussetzung zur Nutzung des eBanking/App bzw. HBCI

Der Teilnehmer benötigt für die Nutzung des eBanking/App bzw. HBCI 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, die auch alphanumerisch sein können, sind beispielsweise:

- eine eigene Teilnehmer-Nummer,
- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN, xTAN).
- der persönliche elektronische Schlüssel für die elektronische Signatur

2.2. Authentifizierungsinstrumente

Authentifizierungsinstrumente sind Personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurden und die vom Teilnehmer zur Erteilung eines eBanking- bzw. HBCI-Auftrags verwendet werden. Insbesondere mittels folgender Authentifizierungsinstrumente kann das Personalisierte Sicherheitsmerkmal (zB xTAN) dem Teilnehmer zur Verfügung gestellt werden:

- Liste mit einmal verwendbaren TAN
- TAN-Generator, der Bestandteil einer Chipkarte oder eines anderen elektronischen Gerätes zur Erzeugung von TAN ist
- mobiles Endgerätes (zB Mobiltelefon) zum Empfang von xTAN per SMS (extended TAN)
- Wisch-Geste bei Nutzung der Oberbank App

Weitere Details für das xTAN-Verfahren (extended TAN) siehe die gesonderte Regelung unter Nr. 11.
Der Teilnehmer nimmt ausdrücklich zur Kenntnis und ist damit einverstanden, dass die Bank berechtigt aber nicht verpflichtet ist, die TAN-Kuverts an die bekannt gegebene Adresse zu senden oder diese schalterlagernd an den Teilnehmer auszuhändigen.
Im Falle des Vorhandenseins eines weiteren eBanking-Zuganges in einem anderen Land, in dem der Kunde ebenfalls Konten der Oberbank unterhält, werden die ausländischen Konten, die eindeutig dem Kunden zugeordnet werden können, im Zuge der App-Nutzung automatisch mit angezeigt und es können darüber im vereinbarten Maße Verfügungen vorgenommen werden (Datenpairing).

3. Zugang zum eBanking/App bzw. HBCI

Der Teilnehmer erhält Zugang zum eBanking/App bzw. HBCI, wenn

- dieser die individuelle Empfangsbestätigung zur Bank übermittelt hat
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummer 8.1 und 9) vorliegt.

Nach Gewährung (Freischaltung) des Zugangs zum eBanking/App bzw. HBCI kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.
Die Sätze 1 und 2 gelten auch, wenn der Teilnehmer Zahlungsaufträge über einen Zahlungsauslösedienst auslöst und Zahlungskontoinformationen über einen Kontoinformationsdienst anfordert (siehe Nummer 1 Absatz 1 Satz 4).

4. eBanking/App- bzw. HBCI-Aufträge

4.1. Auftragserteilung und Autorisierung

Der Teilnehmer muss eBanking/App- bzw. HBCI-Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit mit dem von der Bank bereit gestellten Personalisierten Sicherheitsmerkmal (zB xTAN) oder mit dem vereinbarten biometrischen Sicherheitsmerkmal autorisieren und der Bank mittels eBanking/App bzw. HBCI übermitteln. Pro Tag dürfen im Rahmen des jeweils bestehenden Kontoguthabens oder der darüber hinaus vereinbarten Dispositionsmöglichkeiten beliebig viele Verfügungen im Rahmen des Transaktionslimits vorgenommen werden. Verfügungen und Aufträge, die mit der Eingabe einer gültigen Autorisierung abzuschließen sind (zB Überweisungen), gelten vom Teilnehmer als zur Durchführung freigegeben, wenn die jeweils gültige Autorisierung (zB xTAN) abschließend eingegeben wurde. Bei Anwendung des in Punkt 2 beschriebenen Datenpairings gilt die übermittelte xTAN zur Autorisierung aller in der Oberbank App angezeigten Konten, unabhängig davon, in welchem Land diese Konten geführt werden. Dies gilt auch dann, wenn zur Nutzung der eBanking Anwendungen unterschiedliche Mobiltelefonnummern registriert wurden.
Bei der Autorisierung mittels xTAN sind vom Teilnehmer zusätzlich die in der SMS angeführten Transaktionsdaten (zB bei Überweisung Empfänger-IBAN und Betrag) zu kontrollieren. Verfügungen mittels TAN sind beim Oberbank eBanking bis zu einem Limit von EUR 1.000,- pro Transaktion (eBanking Private) bzw. EUR 5.000,- (eBanking Business) möglich; für die Oberbank App (Verfügungen nur mittels xTAN möglich) gilt ein Limit von EUR 1.500,-. Das Transaktionslimit gilt nicht für Eigenüberträge (Überweisungen zwischen den in das Oberbank eBanking/App einbezogenen Oberbank Konten).
Änderungen der Limits müssen zwischen Oberbank und Kunden vereinbart werden. Der Kunde ist ohne Angabe von Gründen berechtigt, die Senkung des Limits bei der kontoführenden Stelle zu veranlassen. Die Bank bestätigt mittels eBanking/App bzw. HBCI den Eingang des Auftrages.
Dieser Absatz gilt auch, wenn der Teilnehmer einen Zahlungsauftrag über einen Zahlungsauslösedienst (siehe Nummer 1 Absatz 1 Satz 4) auslöst und übermittelt.

4.2. Widerruf von Aufträgen

Der Widerruf von Aufträgen kann nur außerhalb des eBanking/App bzw. HBCI erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im eBanking bzw. HBCI ausdrücklich vor.Die Bank kann einen Rückruf nur beachten, wenn er ihr so rechtzeitig zugeht, dass seine Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufes möglich ist und der Auftrag noch nicht ausgeführt ist.

5. Bearbeitung von eBanking/App- bzw. HBCI-Aufträgen durch die Bank

(1) Die Bearbeitung der eBanking/App- bzw. HBCI-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung) wie im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem im „Preis- und Leistungsverzeichnis“ angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

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

- der Teilnehmer hat den Auftrag autorisiert;
- die Berechtigung des Teilnehmers für die jeweilige Auftragsart (zum Beispiel Überweisung) liegt vor;
- das eBanking- bzw. HBCI-Datenformat ist eingehalten;
- die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung) 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 (zB Bedingungen für den Überweisungsverkehr) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird dem Teilnehmer hierüber mittels eBanking bzw. HBCI eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6. Information des Kontoinhabers über eBanking/App- bzw. HBCI-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels eBanking/App bzw. HBCI getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg. Die Anzeige von eingehenden und ausgehenden Zahlungsverkehrs-Transaktionen erfolgt je nach Produktnutzung eBanking/App bzw. HBCI unterschiedlich. Im Oberbank eBanking bzw. HBCI werden Zahlungsein- und -ausgänge als AVISI ausgewiesen. Im Zuge des letzten Buchungslaufes pro Geschäftstag wird auch der Kontostand aktualisiert. In der Oberbank App hingegen werden alle Aufträge mit Ausnahme von Fremdwährungs-Transaktionen sofort als gebucht angezeigt und der Kontostand auch sofort aktualisiert.

7. Sorgfaltspflicht des Teilnehmers

7.1. Technische Verbindung zum eBanking/App bzw. HBCI

Der Teilnehmer ist verpflichtet, die technische Verbindung zum eBanking/App bzw. HBCI nur über die von der Bank gesondert mitgeteilten Zugangskanäle (zB Internetadresse) herzustellen. Um sicherzustellen, mit der Oberbank verbunden zu sein, muss der Teilnehmer die Zertifikationsinformation der Secure Socket Layer-Verschlüsselung (SSL) auf den Inhalt zu prüfen. Weitere Sicherheitshinweise siehe Oberbank Homepage https://banking.oberbank.de/smartoffice/de/logon.htm unter Sicherheit.
Zur Auslösung eines Zahlungsauftrags und zum Abruf von Informationen über ein Zahlungskonto kann der Teilnehmer die technische Verbindung zum eBanking bzw. HBCI auch über einen Zahlungsauslösedienst bzw. einen Kontoinformationesdienst (siehe Nr. 1 Absatz 1 Satz 4) 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 nur über die von der Bank gesondert mitgeteilten eBanking/App-Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument (siehe Nummer 2.2.) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit der Kenntnis des dazugehörigen Personalisierten Sicherheitsmerkmals das eBanking/App- bzw. HBCI-Verfahren missbräuchlich nutzen. Die Geheimhaltungspflicht bezüglich der Personalisierten Sicherheitsmerkmale nach Satz 1 gilt nicht, wenn der Teilnehmer diese zur Erteilung eines Zahlungsauftrags oder zum Abruf von Informationen über ein Zahlungskonto an den von ihm ausgewählten Zahlungsauslösedienst bzw. Kontoinformationsdienst übermittelt (siehe Nummer 1 Absatz 1 Satz 4).

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

- Das Personalisierte Sicherheitsmerkmal darf nicht ungesichert elektronisch gespeichert werden (zum Beispiel im Kundensystem)
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- Das Personalisierte Sicherheitsmerkmal darf nicht per E-Mail weitergegeben werden.
- Das Personalisierte Sicherheitsinstrument (zB PIN) darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung zum Beispiel eines Auftrags oder der Aufhebung der Sperre nicht mehr als eine TAN verwenden.
- Beim mobilen xTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (zum Beispiel Mobiltelefon), nicht gleichzeitig für das eBanking/App genutzt werden.

7.3. Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise auf der Internetseite der Bank zum eBanking/App, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.4. Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem eBanking/App- bzw. HBCI-Auftrag (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät des Teilnehmers (zB Mobiltelefon, TAN-Generator mit Display) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten

8.1. Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder eines seiner Personalisierten Sicherheitsmerkmale

fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

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

(3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt
- den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder 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 Kontoinhaber hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1. Sperre auf Veranlassung des Teilnehmers

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

- den eBanking/App- bzw. HBCI-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument.

Über die Electronic Banking Hotline kann die Sperre in der Zeit von 08 - 17 Uhr von Montag bis Freitag

Tel: +49 (0)89/55989-255
elba@oberbank.at

mit Angabe der Kontonummer beauftragt werden.

9.2. Sperre auf Veranlassung der Bank

(1) Die Bank darf den eBanking/App- bzw. HBCI-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, den eBanking/App- bzw. HBCI-Vertrag aus wichtigen Gründen zu kündigen,
- die Nutzungsgestattung für das Electronic Banking/App bzw. HBCI beendet ist,
- 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 Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten.

9.3. Sperre durch den Teilnehmer

Der Teilnehmer hat in der eBanking/App- bzw. HBCI-Anwendung durch dreimalige Fehleingabe der PIN oder TAN / xTAN und unter dem Menü Benutzer selbst die Möglichkeit, den eBanking/App- bzw. HBCI-Zugang zu sperren. Sperren via Oberbank eBanking/App bzw. HBCI werden sofort wirksam.

9.4. 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 Kontoinhaber unverzüglich.

10. Haftung

10.1. Haftung der Bank bei einer nicht autorisierten eBanking/App- bzw. HBCI-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten eBanking/App- bzw. HBCI-Verfügung

Die Haftung der Bank bei einer nicht autorisierten eBanking/App- bzw. HBCI-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten eBanking/App- bzw. HBCI-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr).

10.2. Haftung des Kontoinhabers bei missbräuchlicher Nutzung eines Personalisierten Sicherheitsmerkmals oder seines Authentifizierungsinstruments

10.2.1. Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50,- Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn

- es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungsinstraumentsvor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Authentifizierungsinstruments durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er

- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1. Absatz 1),
- das Personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe Nummer 7.2. Absatz 2 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2. Absatz 1 2. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal per E-Mail weitergeben 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 Auftrages verwendet hat (siehe Nummer 7.2. Absatz 2 6.Spiegelstrich),
- beim mobilen TAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z.B. Mobil-telefon), auch für das eBanking/App nutzt (siehe Nummer 7.2. Absatz 2 7.Spiegelstrich).

(4) Abweichend von den Absätzen 1 und 3 ist der Kontoinhaber nicht zum Schadenersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt hat, obwohl die Bank zur starken Kundenauthentifizierung nach § 68 Absatz 4 Zahlungsdiensteaufsichtsgesetz verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, das der Teilnehmer weiß, zB PIN), Besitz (etwas, das der Teilnehmer besitzt, zB TAN-Generator) oder Inhärenz (etwas, das der Teilnehmer ist, zB Fingerabdruck).

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

(6) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

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

(8) Ist der Kontoinhaber kein Verbraucher, gilt ergänzend Folgendes:

- Der Kontoinhaber haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50,- Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

10.2.2. Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte eBanking/App-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 begründeten 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 vermieden werden können.

11. Besondere Bedingungen für das xTAN-Verfahren (extended TAN)

- Begriffsbestimmung xTAN-Verfahren:
  Beim xTAN-Verfahren ist ein Mobiltelefon erforderlich. Das Mobiltelefon besteht aus einem entsprechenden Gerät (ME) sowie der Chipkarte (SIM) des Telekommunikations-Netzbetreibers. Für das xTAN-Verfahren wird der Telekommunikationsanschluss des Teilnehmers registriert. Auf das registrierte Mobiltelefon wird dem Teilnehmer von der Oberbank bei Bedarf eine xTAN durch eine Textmeldung (SMS) übermittelt. Die technische Voraussetzung für die xTAN-Zustellung ist abhängig von der Empfangsmöglichkeit des vom Berechtigten verwendeten Mobilnetzbetreibers.
- Entgelte beim xTAN-Verfahren:
  die Nutzung des xTAN-Verfahrens und die Zustellung der xTAN (SMS) sind bis auf weiteres kostenlos.
- Umstieg auf das xTAN-Verfahren:
  Das bisher gültige TAN-Kuvert wird für das Oberbank eBanking gesperrt.
- Weitere Maßnahmen bei Verlust des Mobiltelefons:
  Stellt der Teilnehmer den Verlust seines Mobiltelefons oder der SIM-Karte fest oder besteht der Verdacht seiner missbräuchlichen Nutzung, so ist der Teilnehmer zu Folgendem verpflichtet: Der Teilnehmer hat die Oberbank und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. Zusätzlich ist das Mobiltelefon (die SIM-Karte) auch beim jeweiligen Mobilfunkbetreiber zu sperren.
- Verwendung der TAN beim xTAN-Verfahren:
  Der Teilnehmer erhält von der Bank auf Anforderung durch eine entsprechende eBanking/App- bzw. HBCI-Anwendung eine Textmeldung (SMS) mit einer xTAN auf das registrierte Mobiltelefon. Die so übermittelte xTAN ist nur für den Auftrag zu nutzen, für den angeforderte wurde. Jede übermittelte xTAN ist nur 5 Minuten gültig. Wird die Zeit überschritten oder die xTAN falsch eingegeben, verfällt diese und muss erneut im eBanking bzw. HBCI angefordert werden. Bei der Autorisierung mittels xTAN ist der Teilnehmer verpflichtet zusätzlich die in der SMS angeführten Transaktionsdaten (z.B. bei Überweisung Betrag und Kontonummer des Empfängers) zu kontrollieren.

12. Entgelt

Für die Leistung der Bank im Rahmen des eBanking/App bzw. HBCI gilt das dem Kunden ausgehändigte Preisblatt. Die Entgelte können gemäß den Regelungen in den "Allgemeinen Geschäftsbedingungen" der Oberbank AG, Zweigniederlassung Deutschland geändert werden.

13. Änderungen

Änderungen dieser Geschäftsbedingungen oder die Einführung zusätzlicher Bedingungen wird die Bank dem Kunden spätestens 2 Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in der jeweils gesetzlich zugelassenen Form anbieten. Die Zustimmung des Kunden gilt als erteilt, wenn er seine Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen angezeigt hat. Auf diese Genehmigungswirkung wird ihn die Bank in ihrem Angebot gesondert hinweisen. Die Bank wird dann die geänderte Fassung der Bedingungen und die zusätzlich eingeführten Bedingungen der weiteren Geschäftsbeziehung zugrunde legen.

14. Sonstige / Allgemeine Geschäftsbedingungen

Soweit hier nicht anders angeführt, gelten außerdem ergänzend die „Allgemeinen Geschäftsbedingungen“ der Oberbank AG, Niederlassung Deutschland, in ihrer jeweils gültigen Fassung.

Oberbank AG
Niederlassung Deutschland

Beiblatt – Leistungsumfang für das Oberbank eBanking

Im Rahmen des Oberbank eBanking können verschiedene Dienstleistungen in Anspruch genommen werden.
Derzeit umfassen diese:

eBanking *private*

- Abfrage der aktuellen Kontoinformationen in Salden / Auszügen (inkl. nicht gebuchter Umsätze)
- Kontoauszug im digital signierten PDF-Format
- Abfrage der Depots inkl. Depotkurswert
- Abfrage der Einzelposten des Depots
- Beauftragung von SEPA-Aufträgen (Überweisungen und Lastschriften)
- Terminaufträge (bis zu 28 Tagen im Voraus)
- Durchführung von Sammelaufträgen
- Durchführung von Periodenaufträgen
- Durchführung von Eigenüberträgen
- Vorlage abspeichern, ändern oder löschen
- Statusabfrage der Aufträge
- Anlegen von Vorlagen
- Anlegen von Empfängerdaten

eBanking *business bietet neben den Funktionen von eBanking private zusätzlich:*

- Beauftragung von SEPA-Eilaufträgen
- Beauftragung von Einzel- und Sammel-Auslandsaufträgen
- Import und Versand von Zahlungsverkehrsdateien im SEPA-Format und DTAZV-Format
- Export von Kontoauszügen im MT940-Format und CAMT053-Format

Die Bank behält sich vor, den Leistungsumfang des Oberbank eBanking zu erweitern bzw. auch einzuschränken oder abzuändern.

Beiblatt Leistungsumfang für die Oberbank App

Im Rahmen der Oberbank App können verschiedene Dienstleistungen in Anspruch genommen werden.
Derzeit umfassen diese:

Banking

- Finanzübersicht
  Die Finanzübersicht gibt Ihnen einen Überblick über all Ihre Konten, Kreditkarten und Depots.

- Konto- und Kreditkartenumsätze
  Ihre Einnahmen und/oder Ausgaben werden unter Angabe der wesentlichen Umsatzinformationen detailliert dargestellt.

- Depotübersicht
  Neben der Auflistung und aktuellen Bewertung Ihrer WP-Positionen erhalten Sie auch Informationen über die Entwicklung Ihres Wertpapierdepots.

- SEPA-Überweisung
  Mit der SEPA-Überweisung können Sie Überweisungen innerhalb Österreichs bzw. Europa durchführen. Sie benötigen dazu lediglich die IBAN und BIC des Zahlungsempfängers. Die BIC wird nur benötigt, wenn der Zahlungsempfänger außerhalb Österreich liegt.

- IBAN-Reader
  Zusätzlich ist die Oberbank App für die Erfassung einer SEPA Überweisung mit einem IBAN Reader ausgestattet. Von vorbedruckten Zahlscheinen kann damit einfach und schnell (mittels Scanfunktion) die IBAN in die SEPA Überweisung übernommen werden.

- Übertrag
  Der Eigenübertrag ist der schnellste und kürzeste Weg zwischen Ihren Oberbank Konten Geld zu überweisen.

- Getätigte Überweisungen
  Damit haben Sie den Status Ihrer Überweisungen stets im Überblick.

- BeraterIn
  Im angemeldeten Banking Bereich sind die Kontaktdetails Ihres persönlichen Beraters sowie die Servicenummer der technischen Support-Hotline hinterlegt.

Service

- Newsboard
  Aktuelle Informationen und Aktionen erhalten Sie direkt auf Ihr Smartphone. Sie sind damit jederzeit up-to-date.

- Filial- und Bankomatfinder
  Mit dem Filialfinder finden Sie schnell den richtigen Weg in die nächstgelegene Filiale und erhalten dabei alle wichtigen Kontaktdetails, wie Öffnungszeiten und Telefonnummern. Mit dem Bankomatfinder finden Sie schnell den Weg zum nächsten Bankomaten.

- Währungsrechner
  Der Oberbank Währungsrechner hilft Ihnen im Ausland ein Gefühl für Ihre Ausgaben zu bekommen. Zu beachten ist, dass die Wechselkurse auf dem Stand der letzten Internetverbindung (Aktualisierung) sind, falls Sie im Ausland über kein Internet verfügen.

- Länderinfo
  Hier finden Sie zahlreiche Informationen rund ums Thema Geld (Währung, Wechselkurs, Akzeptanz von Bankomat- und Kreditkarten, ...) zu Ihrem ganz persönlichen Urlaubsland.

- Karte sperren
  Bei Verlust oder Diebstahl Ihrer Bankomat- oder Kreditkarten haben Sie schnell den richtigen Ansprechpartner verfügbar. Die Rufnummern sind 24 Stunden, 7 Tage die Woche erreichbar.

- Hilfe und Feedback
  Unter dem Bereich Hilfe und Feedback können Sie uns Anregungen zur Oberbank App zukommen lassen. Zusätzlich haben wir für Sie die wichtigsten Antworten zu den häufig gestellten Fragen übersichtlich zusammengestellt.

Die Oberbank behält sich vor, den Leistungsumfang der Oberbank App zu erweitern bzw. auch aufgrund systemtechnischer Wartungsarbeiten vorübergehend einzuschränken.
Die angeführten Dienstleistungen stehen je nach getroffener Vereinbarung zur Verfügung.

Beiblatt – Leistungsumfang für das HBCI-Service

HBCI-Software-Produkte unterstützen abhängig vom Produkt folgende Funktionen:

- SEPA-Einzel- und Sammelüberweisungen sowie terminisierte SEPA-Einzel- und Sammelüberweisungen
- SEPA-Eilaufträge
- SEPA-Sammellastschriften (Basis und Firmen)
- SEPA-Daueraufträge
- Auslandsüberweisungen
- Verwaltung der Kontoumsätze
- Depotbestand abrufen
- Multibankfähig
- Datenimport SEPA-Format und DTAZV
- Datenexport MT940
- Automatische Datensicherung
- Tagesauszüge und Valuten-Salden
- Schnellerfassungsmaske
- Gemeinschaftlich Zeichnungsberechtigte

Alternative Autorisierungsverfahren zu xTAN:

Sicherheitsdatei
Sie starten Ihre Banking-Software und erfassen Ihre Aufträge wie gewohnt, um sie an die Oberbank zu senden. Mit der von Ihnen - bei der Initialisierung Ihres HBCI Zuganges - erstellten Sicherheitsdatei (Elektronische Unterschrift) und dem von Ihnen definierten PIN-Code wird der Auftrag bestätigt. Daraufhin wird der vorbereitete Auftrag verschlüsselt an den Bank-Server übertragen und bankseitig verarbeitet.

Digitale Signatur
Sie starten Ihre Banking-Software und erfassen Ihre Aufträge wie gewohnt, um sie an die Oberbank zu senden. Mit der Oberbank-Signaturkarte und dem von Ihnen definierten PIN-Code wird der Auftrag am Chipkarten-Lesegerät bestätigt. Daraufhin wird der vorbereitete Auftrag verschlüsselt an den Bank-Server übertragen und bankseitig verarbeitet.

chipTAN comfort
Sie starten Ihre Banking-Software und erfassen Ihre Aufträge wie gewohnt und senden diese an die Oberbank. Es öffnet sich ein Fenster mit einem aufflackernden Signal („Flickergrafik“) auf Ihrem Monitor. Vor dieser Grafik justieren Sie den TAN-Generator. Wichtige Werte der Zahlung werden ausgelesen und im Display Ihres TAN-Generators angezeigt. Überprüfen Sie, ob die auf dem Display angezeigten Werte mit den Daten Ihres Auftrages übereinstimmen und bestätigen Sie jeweils mit OK. Nach erfolgreicher TAN Generierung geben Sie bitte die TAN in Ihrer Anwendung ein.