

# Bedingungen für das Online Banking für den justTRADE Service

Sutor Bank GmbH | Hermannstraße 46 | 20095 Hamburg

## 1 Leistungsangebot

(1) Der Kunde kann Bankgeschäfte mittels Online Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Sutor Bank GmbH (im Folgenden auch „Bank“) mittels Online Banking abrufen.

(2) Der Kunde wird einheitlich als „Teilnehmer“, Konto und Depot einheitlich als „Konto“ bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

(3) Zur Nutzung des Online Banking gelten die mit der Bank gesondert vereinbarten Verfügungsmitel. Das Verfügungsmitel ist initial auf 10.000,- EUR pro Bankarbeitstag eingestellt. Eine Änderung dieses Limits kann der Kunde mit der Bank vereinbaren.

(4) Der Teilnehmer kann die von der Bank angebotenen Online-Dienste (d. h. die von der Bank per Internet oder in sonstiger Weise jeweils zur Verfügung gestellten Handelsapplikationen) für den Zugang für Bankgeschäfte mittels Online Banking nutzen. Sofern die Bank über eines der genannten Kommunikationsmittel nicht erreichbar ist, ist der Teilnehmer verpflichtet, auf ein anderes dieser Kommunikationsmittel oder auch das Telefon auszuweichen.

## 2 Voraussetzungen zur Nutzung des Online Banking

(1) Der Teilnehmer kann das Online Banking nutzen, wenn die Bank ihn authentifiziert hat.

(2) Die Authentifizierung gegenüber der Bank erfolgt über ein mit der Bank vereinbartes Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).

(3) Authentifizierungselemente sind

- Wissensselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer (PIN) bzw. ein Passwort),
- 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 das mobile Endgerät oder der mit Hilfe eines Browser-Cookies von der Bank autorisierte PC des Teilnehmers), oder
- Seinsselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

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

(5) Diese Authentifizierung gilt grundsätzlich für die jeweilige Online Sitzung insgesamt.

(6) Die Bank behält sich das Recht vor, den Teilnehmer am Telefon in anderer Weise als durch die vorstehend genannten Authentifizierungsmerkmale zu legitimieren.

## 3 Zugang zum Online Banking

(1) Der Teilnehmer erhält Zugang zum Online Banking der Bank, wenn

- er seine individuelle Teilnehmerkennung (z. B. Kontonummer, Anmeldeame) 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.

(3) Für den Fall, dass die Bank im Rahmen des Zugangsversuchs eines Teilnehmers feststellt, dass dieser von einem der Bank nicht bekanntem

Endgerät Zugang zu einer Handelsapplikation nehmen möchte, kann dieses nicht bekannte Endgerät durch den Teilnehmer durch die Eingabe eines Authentifizierungselementes autorisiert und damit zu einem Authentifizierungselement der Kategorie Besitz werden.

## 4 Aufträge

### 4.1 Auftragserteilung

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) entweder bei dem Start der Online Sitzung für die Sitzung insgesamt oder für die einzelne Transaktion zu verwenden. 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. Der Widerruf von Aufträgen kann nur außerhalb des Online Banking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Online Banking ausdrücklich vor.

## 5 Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der Aufträge erfolgt an Bankarbeitstagen entsprechend der jeweiligen Auftragsart (zum Beispiel Überweisung) im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem auf der Online Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis für den justTRADE Service“ angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Bankarbeitstag, so gilt der Auftrag am darauf folgenden Bankarbeitstag als zugegangen. Die Bearbeitung beginnt erst an diesem Bankarbeitstag.

(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-Verfügungsmitel ist nicht überschritten (vgl. Nummer 1 Absatz 3 dieser Bedingungen). Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen 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 (zum Beispiel Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird den 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.

## 6 Information des Kunden über Online Banking-Verfügungen

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

## 7 Sorgfaltspflichten des Teilnehmers

### 7.1 Schutz der Authentifizierungselemente

(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummer 3 und 4 dieser Bedingungen).

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

- (a) Wissensselemente, wie z. B. die PIN bzw. ein Passwort, 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 bzw. des Passwortes 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. mobiles Endgerät, Signaturkarte, autorisierter PC) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Online Banking und Fingerabdrucksensor) dient.
- (b) Besitzelemente, wie z. B. ein mobiles Endgerät oder der autorisierte PC, sind vor Missbrauch zu schützen, insbesondere
- ist sicherzustellen, dass unberechtigte Personen auf das Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können,
  - ist dafür Sorge zu tragen, dass andere Personen die auf dem 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 Endgerät des Teilnehmers zu deaktivieren (bei einem PC die Cookies zu löschen), bevor der Teilnehmer den Besitz an diesem Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons oder PCs),
  - dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und
  - muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das Online Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online Banking des Teilnehmers aktivieren.
- (c) Seinselemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem Endgerät des Teilnehmers für das Online Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem Endgerät, das für das Online Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Online Banking das von der Bank ausgegebene Wissenalelement (z. B. PIN bzw. ein Passwort) zu nutzen und nicht das auf dem Endgerät gespeicherte Seinselement.
- (3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (zum Beispiel Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.
- (4) 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.
- (5) Der Teilnehmer hat dafür Sorge zu tragen, dass der von ihm für den Zugang verwendete Computer gesichert und mit den üblichen Schutzmechanismen und -programmen (z. B. Firewall, Anti-Viren Scanner, usw.) ausgestattet ist. Der Teilnehmer hat darauf zu achten, dass die Sitzung immer durch Klick auf Logout geschlossen wird. Dies gilt auch, wenn der Teilnehmer das jeweilige Zugangsmedium physisch verlässt, um zu verhindern, dass andere Personen Online Banking-Aufträge über das Zugangsmedium erteilen können.

## 7.2 Sicherheitshinweise der Bank

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

## 7.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer die von ihr empfangenen Auftragsdaten (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers (zum Beispiel mittels mobilem Endgerät, Chipkartenlesegerät mit Display) anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehene 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. mobiles Endgerät, autorisierter PC, Signaturkarte) oder
  - die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstrumente fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der

Teilnehmer kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgebenen.

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

(3) Hat der Teilnehmer den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

### 8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Teilnehmer hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

## 9 Nutzungssperre

### 9.1 Sperre auf Veranlassung des Teilnehmers

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

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

### 9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Online Banking-Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den Online Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Teilnehmers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

(2) Die Bank wird den Kunden möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten.

### 9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

### 9.4 Automatische Sperre

Der Zugang zum Online Banking der Bank wird aus Sicherheitsgründen automatisch für einen gewissen Zeitraum gesperrt, sobald ein falsches Passwort eingegeben wurde. Bei wiederholter Eingabe eines falschen Passwortes verlängert sich jeweils der Zeitraum der Sperre.

## 10 Haftung

### 10.1 Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Bank bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für Wertpapiergeschäfte).

### 10.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungsinstrumente

#### 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 Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

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

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

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang.

Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltpflichten nach

- Nummer 7.1 Absatz 2,
- Nummer 7.1 Absatz 4,
- Nummer 7.3 oder
- Nummer 8.1 Absatz 1 dieser Bedingungen

verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Sein (siehe Nummer 2 Absatz 3 dieser Bedingungen).

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

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

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

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

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

#### 10.2.2 Haftung des Kunden bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige

Beruhend nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

#### 10.2.3 Haftung ab der Sperranzeige

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

#### 10.2.4 Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.