Nutzungsbedingungen für den Service spot9

Max Heinr. Sutor oHG | Hermannstraße 46 | 20095 Hamburg

Ein Service der Sutor Bank

1. Serviceangebot

1.1
Die Max Heinr. Sutor oHG (im Folgenden auch „Bank") bietet unter der Marke spot9 Kunden die Möglichkeit, an von der Bank betriebenen Automaten Aufträge zum Kauf von Kryptowerten zu erteilen.

Kunden des Service spot9 erreichen die Bank wie folgt:

spot9
ein Service der Max Heinr. Sutor oHG
Hermannstraße 46, 20095 Hamburg
Deutschland
info@spot9.com

Die Bank bietet den Service spot9 in Kooperation mit der Spot9 GmbH, Fredersdorfer Straße 11, 10243 Berlin („spot9 GmbH") an.

1.2
Das Angebot, die Automaten zu nutzen, richtet sich ausschließlich an natürliche Personen mit Wohnsitz in Deutschland, die die deutsche oder die Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union („EU"), des Abkommens über den Europäischen Wirtschaftsraum („EWR") oder der Europäischen Freihandelsassoziation („EFTA") haben, die das 18. Lebensjahr vollendet haben (im Folgenden auch „Kunde") und die den Service ausschließlich für private Zwecke im eigenen Namen und für eigene Rechnung nutzen.

1.3
Das Angebot richtet sich zudem ausschließlich an gut informierte und erfahrene Kunden mit einer hohen Risikobereitschaft, die in der Lage sind, Verluste bis hin zum Totalverlust der Investition zu tragen. Die Bank und spot9 prüfen nicht, ob der Kauf von Kryptowerten für den Kunden angemessen ist. Eine Prüfung der finanziellen Verhältnisse, der Kenntnisse und Erfahrungen des Kunden erfolgt nicht.

Kunden, die US-Staatsbürger im Sinne der Steuergesetze der USA sind, in den USA wohnhaft und/oder hinsichtlich ihrer weltweiten Einkünfte gegenüber den US-Steuerbehörden steuerpflichtig sind, sind von der Nutzung des Service ausgeschlossen.

1.4
Um das Angebot der Bank nutzen zu können, ist die Registrierung unter www.spot9.com erforderlich. Hierbei ist vom Kunden eine E-Mail-Adresse und Mobilfunknummer eines Telekommunikationsanbieters mit Sitz in einem EU-Mitgliedstaat oder in einem Mitgliedstaat der Europäischen Freihandelsassoziation anzugeben, auf die ausschließlich er Zugriff hat. Nach der Registrierung steht dem Kunden das von spot9 betriebene sogenannte Dashboard (im Folgenden auch „Portal" genannt) zur Verfügung.

Die Registrierung setzt voraus, dass sich der Kunde im Einklang mit dem Geldwäschegesetz mittels PostIdent-Verfahren oder ggf. anderen anerkannten Verfahren identifiziert und die Bank den entsprechenden Antrag des Kunden auf Registrierung für den Service spot9 angenommen hat. Der Kunde verzichtet insoweit auf den Zugang der Annahmeerklärung der Bank. Der Kunde erhält zudem beim erstmaligen Login in das Dashboard eine vierstellige PIN (persönliche Identifikationsnummer), die der Authentifizierung von Transaktionen dient.

1.5
Die Bank ist berechtigt, die vom Kunden angegebene E-Mail-Adresse und Mobilfunknummer für die gesamte Kundenkommunikation zu verwenden.

1.6
Neben diesen Nutzungsbedingungen gelten ergänzend die Allgemeinen Geschäftsbedingungen der Bank, die unter anderem auf der Internetseite www.spot9.com abrufbar sind und außerdem in den Geschäftsräumen der Bank eingesehen werden können. Bei Widerspruch zwischen einzelnen Regelungen haben diese Nutzungsbedingungen Vorrang vor den Allgemeinen Geschäftsbedingungen der Bank. Daneben gelten die Allgemeinen Geschäftsbedingungen von spot9 zur Nutzung des spot9 Dashboards.

2. Voraussetzung für die Nutzung der Automaten und des Portals

2.1
Kunden benötigen für die Registrierung und Nutzung der Automaten ein Mobiltelefon bzw. eine Mobilfunknummer eines Telekommunikationsanbieters mit Sitz in einem Mitgliedstaat der EU, des EWR oder der EFTA. Darüber hinaus benötigt der Kunde einen amtlichen Lichtbildausweis und, sofern es sich um einen Staatsangehörigen eines Mitgliedstaates der EU, des EWR oder der EFTA handelt, zusätzlich eine deutsche Meldebescheinigung. Für die Registrierung sowie die Nutzung des Kundenkontos und den Service spot9 benötigt der Kunde einen Internetzugang und eine E-Mail-Adresse.

2.2
Der Kunde ist verpflichtet, nur solche Wallet-Adressen anzugeben, die ausschließlich ihm gehören und die ausschließlich von ihm kontrolliert werden. Er wird dies der Bank auf Verlangen in einer für die Bank akzeptablen Form nachweisen.

2.3
Um die Automaten und das Portal zu nutzen, muss sich der Kunde gegenüber der Bank authentifizieren.

2.4
Die Authentifizierung gegenüber der Bank erfolgt über ein mit der Bank vereinbartes Verfahren, mit dessen Hilfe die Bank die Identität des Kunden oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Kunden überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Kunden sich gegenüber der Bank als berechtigter Kunde ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 5 dieser Bedingungen).

2.5
Authentifizierungselemente sind
- Wissenselemente, also etwas, das nur der Kunde weiß (z. B. persönliche Identifikationsnummer (PIN) bzw. ein Passwort),
- Besitzelemente, also etwas, das nur der Kunde besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern (hier: „TAN"), die den Besitz des Kunden nachweisen, wie das mobile Endgerät), oder
- Seinselemente, also etwas, das der Kunden ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Kunden).

2.6
Die Authentifizierung des Kunden erfolgt, indem der Kunden gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.

2.7
Diese Authentifizierung gilt grundsätzlich für die jeweilige Sitzung insgesamt.

3. Zugangsberechtigung

Der Kunde kann den Service der Bank nutzen, wenn
- er seine individuelle Kundenerkennung (z. B. E-Mail-Adresse) 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 erfolgreicher Authentifizierung kann auf Informationen zugegriffen oder Kryptowerte an den von der Bank betriebenen Automaten gekauft werden.

4. Kauf auf eigene Verantwortung

4.1
Dem Kunden ist bekannt, dass der Kauf von Kryptowerten ausschließlich auf sein Risiko erfolgt und die Bank weder die Geeignetheit noch die Angemessenheit des Geschäfts prüfen wird. Die Bank erbringt insbesondere keine Beratungsleistungen und übernimmt keine Gewähr für die Werthaltigkeit der erworbenen Kryptowerte oder deren Eignung für die vom Kunden verfolgten Zwecke.

4.2
Soweit die Bank dem Kunden allgemeine Informationen über Kryptowerte zur Verfügung stellt (z. B. über www.spot9.com oder den Kundenservice), geschieht dies ausschließlich zu dem Zweck, dem Kunden eine selbständige Anlageentscheidung zu ermöglichen. Die bereitgestellten Informationen wurden von der Bank sorgfältig zusammengestellt und stammen aus Quellen, die die Bank für zuverlässig hält. Gleichwohl übernimmt die Bank für die Vollständigkeit und Richtigkeit der bereitgestellten Informationen keine Haftung.

4.3
Die Bank bestimmt die Kryptowerte, die über ihre Automaten angeboten werden, ausschließlich auf Grundlage ihrer Verbreitung und Handelbarkeit. Die Aufnahme in das Angebot bedeutet nicht, dass die Bank die Kryptowerte auf ihre Werthaltigkeit geprüft hat oder ihren Erwerb empfiehlt.

5. Kauf von Kryptowerten über Automaten

5.1 Authentifizierung
Die Nutzung der Automaten erfordert eine Registrierung des Kunden im Portal sowie dessen Authentifizierung am Automaten. Auf Anforderung hat er hierzu Authentifizierungselemente entweder bei dem Start der Sitzung für die Sitzung insgesamt oder für die einzelne Transaktion zu verwenden.

5.2 Prüfung der Transaktionsdaten
Bevor der Kunde seinen Kaufauftrag erteilt, werden ihm von dem Automaten die wesentlichen Transaktionsdaten (z. B. Preis, Wallet-Adresse des Kunden) anzeigt. Sofern diese Transaktionsdaten nicht der vom Kunden gewünschten Transaktion entsprechen, hat der Kunde die Möglichkeit, die Daten entsprechend seinen Wünschen zu korrigieren.

5.3 Widerruf von Kaufaufträgen
Der Kunde ist berechtigt, seinen Kaufauftrag bis zur Bestätigung der Transaktion zu widerrufen. Nach Bestätigung der Transaktion ist ein Widerruf durch den Kunden grundsätzlich nicht mehr möglich.

5.4 Ablauf des Kaufvorgangs am Automaten
(1) Kunden haben vorbehaltlich der Verfügbarkeit des Services spot9 die Möglichkeit, der Bank über Automaten Aufträge zum Kauf von Kryptowerten zu erteilen und den hierfür erforderlichen Kaufpreis in Form von Bargeld direkt am Automaten einzuzahlen. Es werden hierbei ausschließlich Euro-Banknoten akzeptiert.

(2) Der Kunde wählt am Automaten, der indikative Preise und indikative Transaktionskosten anzeigt, zunächst den Kryptowert aus, den er kaufen möchte, und gibt das Volumen der von ihm beabsichtigten Transaktion an. Anschließend meldet sich der Kunde mit seiner Mobilfunknummer, einer per SMS erhaltenen temporären Transaktionsnummer (TAN) und der PIN am Automaten an.

(3) Mit Einlesen eines QR-Codes am QR-Code-Leser des Automaten bestimmt der Kunde das Zielwallet, das für die Abwicklung der Transaktion genutzt werden soll. Abhängig von der Ausstattung des jeweiligen Automaten kann darüber hinaus die Möglichkeit bestehen, für die Abwicklung der Transaktion am Automaten ein Paper-Wallet zu erstellen. Macht der Kunde in diesem Fall von der Möglichkeit zur Erstellung eines Paper-Wallet Gebrauch, werden der öffentliche und private Schlüssel direkt am Automaten ausgedruckt. Ein Anspruch auf die Möglichkeit zur Erstellung eines Paper-Wallet besteht nicht. Auf Ziffer 2.2 wird hingewiesen.

(4) Über den Automaten erteilt der Kunde der Bank den Auftrag, im eigenen Namen für seine Rechnung an dem von der Bitstamp Ltd, 5 New Street Square, London EC4A 3TW United Kingdom, betriebenen Handelsplatz den von ihm ausgewählten Kryptowert im Gegenwert des von ihm in den Automaten eingeführten Betrages abzüglich der anfallenden Gebühren zu erwerben. Der Erwerb erfolgt zu dem aktuellen vom Handelsplatz bestimmten Preis. Der vom Handelsplatz für die Transaktion in Rechnung gestellte Preis kann aufgrund von Marktschwankungen höher oder niedriger als der zu Beginn der Transaktion vom Automaten angezeigte indikative Preis sein kann.

(5) Der Auftrag wird vom Kunden erteilt, indem er Banknoten bis zu dem von ihm zuvor bestimmten Wert in den Automaten einführt und im Anschluss den Button „Kaufen" drückt.

(6) Während des Einführens der Banknoten kann der Kunde die Transaktion jederzeit durch Drücken des Buttons „Abbrechen" abbrechen. Bricht der Kunde den Vorgang ab, erstattet die Bank bereits eingezahlte Beträge durch Überweisung auf ein Konto des Kunden, dass ihr zu diesem Zweck vom Kunden zu benennen ist. Barrückzahlungen am Automaten sind aus technischen Gründen nicht möglich.

(7) Betätigt der Kunde nach dem Einführen der gewünschten Menge an Banknoten den Button „Kaufen", wird die Bank am Handelsplatz im eigenen Namen für Rechnung des Kunden ein verbindliches und unwiderrufliches Angebot zum Kauf von Kryptowerten zum jeweils aktuellen Marktpreis platzieren. Die Annahme bzw. Ablehnung dieses Angebots wird dem Kunden umgehend auf dem Display des Automaten angezeigt.

(8) Wird das Angebot der Bank angenommen, ist die Kauftransaktion zu dem jeweils aktuellen, vom Handelsplatz ermittelten Preis abgeschlossen und kann unter normalen Umständen nicht mehr geändert oder rückgängig gemacht werden.

(9) Nach jeder Kauftransaktion übersendet die Bank dem Kunden an seine E-Mail-Adresse eine Abrechnung, aus der der endgültige Kaufpreis sowie die erhobenen Gebühren ersichtlich sind. Zusammen mit der Abrechnung erhält der Kunde eine Bestätigung, dass die Übertragung der erworbenen Kryptowerte auf das angegebene Kunden-Wallet veranlasst wurde. Die Abrechnung der Transaktionen kann der Kunde auch im spot9 Portal einsehen. Beanstandungen muss der Kunde unverzüglich und spätestens bis zum Ende des auf die Ausführung des Kaufs folgenden Tages geltend machen.

(10) Dem Kunden ist bekannt, dass aufgrund der technischen Gegebenheiten einer Blockchain weder die Bank noch der Handelspartner beeinflussen können, wie lange es dauert, bis die Übertragung der Kryptowerte in das Kunden-Wallet abgeschlossen ist.

(11) Die Bank ist jederzeit berechtigt, den Service auszusetzen oder endgültig einzustellen.

6. Verfügbarkeit der Automaten

6.1
Die Bank kann auf Grund verschiedener Einflussfaktoren einen unterbrechungsfreien Betrieb der Automaten innerhalb der Betriebszeiten nicht sicherstellen. Es ist grundsätzlich möglich, dass die technischen Systeme der Bank, von Handelsplattformen und weiteren Dienstleistern vorübergehend nicht ordnungsgemäß funktionieren. Darüber hinaus kann es notwendig sein, Wartungsarbeiten ausnahmsweise während der Betriebszeiten durchzuführen. Der Betrieb kann auch durch höhere Gewalt gestört sein. In diesen Fällen ist die Bank berechtigt, die Betriebszeiten einzuschränken.

6.2
Soweit die Automaten in Geschäftsräumen eingerichtet sind, steht der Service den Kunden ausschließlich im Rahmen der üblichen Öffnungszeitendieses Geschäfts zur Verfügung.

7. Sorgfaltspflichten der Kunden

7.1 Schutz der Authentifizierungselemente
(1) Der Kunde hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente vor unbefugtem Zugriff zu schützen.

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

a) Wissenselemente, 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 Portals 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 Portal 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 Kunden (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 Portal (z. B. Portal-App, Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für das Portal (z. B. Portal-App, Authentifizierungs-App) auf dem Endgerät des Kunden zu deaktivieren (bei einem PC die Cookies zu löschen), bevor der Kunde 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 Portals mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und
- muss der Kunde, der von der Bank einen Code zur Aktivierung des Besitz-elements (z. B. Mobiltelefon mit Anwendung für das Portal) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitz-element für das Portal des Kunden aktivieren.

c) Seinselemente, wie z. B. Fingerabdruck oder Gesichtszüge des Kunden, sind zurzeit zur Authentifizierung nicht vorgesehen.

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

(4) Der Kunde hat dafür Sorge zu tragen, dass der von ihm für den Zugang zum Portal verwendete Computer gesichert und mit den üblichen Schutzmechanismen und -programmen (z. B. Firewall, Antivirenscanner, usw.) ausgestattet ist. Der Kunde hat darauf zu achten, dass die Sitzung immer durch Klick auf Abmelden geschlossen wird. Dies gilt auch, wenn der Kunde das jeweilige Zugangsmedium physisch verlässt, um zu verhindern, dass andere Personen Portal-Aufträge über das Zugangsmedium erteilen können.

(5) Bei der Nutzung von Automaten hat der Kunde darauf zu achten, dass sämtliche Eingaben verdeckt erfolgen, damit diese nicht ausgespäht werden können.

7.2 Sicherungshinweise der Bank
Der Kunde muss etwaige Sicherheitshinweise im Portal sowie an den Automaten, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige
(1) Stellt der Kunde
- den Verlust oder den Diebstahl eines Besitzelementes zur Authentifizierung (z. B. mobiles Endgerät, autorisierter PC, Signaturkarte) oder
- die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstrumentsfest,

muss der Kunde die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Kunde kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.

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

(3) Hat der Kunde 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 Kunden
Die Bank sperrt auf Veranlassung des Kunden, insbesondere im Fall der Sperranzeige nach Nummer 8.1 dieser Bedingungen,
- den Zugang zum Portal für ihn und die Automatennutzung für ihn oder
- seine Authentifizierungselemente zur Nutzung des Portals bzw. der Automaten.

9.2 Sperre auf Veranlassung der Bank
(1) Die Bank darf den Zugang zum Portal bzw. Automaten für einen Kunden sperren, wenn
- sie berechtigt ist, diesen Vertrag über den Kauf von Kryptowerten über von der Bank betriebenen Automaten aus wichtigem Grund zu kündigen,
- soweit das Vertragsverhältnis über die Nutzung des Portals gekündigt oder sonst wie beendet worden ist oder beendet werden kann,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Kunden 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 Sperrung
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 Portal 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
Eine Haftung der Bank aus und in Verbindung mit der Ausführung von Kaufaufträgen ist in folgenden Fällen ausgeschlossen:
- bei Störungen des Handelssystems,
- bei Störungen in den Datenleitungen, die außerhalb der Verantwortung der Bank liegen,
- bei Entscheidungen von Gerichten oder Aufsichtsbehörden, die es der Bank untersagen, ihrer Verpflichtung gegenüber dem Kunden nachzukommen.

10.2
Die Bank haftet in keinem Falle für Verluste an Kryptowerten, die durch das Wallet, den Wallet-Betreiber oder durch die Verwendung falscher oder manipulierter Wallet-Adressen entstehen können.

10.3
Die Bank haftet nicht für Wertschwankungen, die infolge einer Teilung der Blockchain (sogenannte „Hard Fork") oder allgemeinen Marktentwicklungen auftreten können.

10.4
Die im Portal der Bank enthaltenen Informationen wurden mit großer Sorgfalt erstellt und stammen aus Quellen, die die Bank für vertrauenswürdig hält. Gleichwohl übernimmt die Bank keine Haftung für die Richtigkeit und Vollständigkeit dieser Informationen.

10.5
Die Bank haftet nicht für Bedienungsfehler des Kunden.

10.6
In allen übrigen Fällen haftet die Bank nur im Falle vorsätzlichen oder grob fahrlässigen Verhaltens oder im Falle der Verletzung wesentlicher Vertragspflichten für den bei Geschäften dieser Art typischen und vorhersehbaren Schaden.

10.7
Die Haftung für Personenschäden oder die Haftung nach dem Produkthaftungsgesetz bleibt von den vorstehenden Regelungen unberührt.

10.8
Sobald die Bank eine Sperranzeige eines Kunden gemäß Nummer 8.1 dieser Bedingungen erhalten hat, übernimmt sie alle danach durch nicht autorisierte Transaktionen entstehenden Schäden. Dies gilt nicht, wenn der Kunde in betrügerischer Absicht gehandelt hat.

10.9
Beruhen nicht autorisierte Transaktionen (z. B. Aufträge zum Kauf von Kryptowerten) 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, haftet der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

11. Aufrechung/Verbot der Abtretung und/oder Verpfändung

11.1
Die Bank ist berechtigt, jederzeit Forderungen des Kunden mit eigenen Forderungen gegen den Kunden aufzurechnen. Der Kunde ist nur dann zu einer Aufrechnung berechtigt, wenn seine Forderung an die Bank unbestritten oder rechtskräftig festgestellt ist.

11.2
Dem Kunden ist es nicht gestattet, Ansprüche gegen die Bank abzutreten oder zu verpfänden. Dieses Verbot umfasst sämtliche Ansprüche.

12. E-Mail-Kommunikation und spot9 Portal

12.1
Mit der Erteilung seines Einverständnisses zur E-Mail-Kommunikation trifft der Kunde die ausdrückliche Wahl, dass die Bank mit ihm per E-Mail kommunizieren kann. Die Bank verwendet die ihr vom Kunden auf einem ihrer Formulare oder auf sonstigem Wege mitgeteilte E-Mail-Adresse. Änderungen seiner E-Mail-Adresse teilt der Kunde der Bank unverzüglich mit.

12.2
Die Kommunikation zwischen der Bank und dem Kunden erfolgt insbesondere per E-Mail und beinhaltet auch die Erfüllung von Bericht- und Informationspflichten der Bank und Fälle, in denen aufsichtsrechtliche Regelungen ein solches Einverständnis ausdrücklich verlangen. Rechnungen werden im spot9 Portal zur Verfügung gestellt.

12.3
Sämtliche relevante Informationen zum Kundenkonto und andere ebenfalls in Teilen personenbezogene Dokumente werden dem Kunden per E-Mail sowie im spot9 Portal zur Verfügung gestellt.

12.4
Der Kunde ist verpflichtet, die per E-Mail übersandten Dokumente regelmäßig einzusehen, zu prüfen und auszudrucken bzw. auf seinem Datenträger abzulegen. Für die per E-Mail übersandten Dokumente gelten die Regelungen der Nummer 6.2 sowie der Nummer 11.4 der Allgemeinen Geschäftsbedingungen der Bank, als wären sie über den Postweg zugestellt worden.

12.5
Die im spot9 Portal gespeicherten Dokumente werden während der Dauer der Geschäftsbeziehung für mindestens 10 Jahre vorgehalten. Die Bank haftet nicht für den Verlust von Dokumenten, die nach 10 Jahren aus dem spot9 Portal gelöscht werden.

12.6
Im Ausnahmefall ist es der Bank möglich, dem Kunden die Dokumente auch auf anderen Wegen (z. B. per Post) zuzustellen, wenn dies unter Berücksichtigung des Kundeninteresses sinnvoll erscheint.

13. Bestellung von spot9 als Empfangsbevollmächtigten

13.1 Bestellung von spot9 als Empfangsbevollmächtigten des Kunden
Hiermit bestellt der Kunde im Rahmen der Nutzung des spot9 Service die spot9 GmbH zu seiner Empfangsbevollmächtigten, an welche die Bank alle an den Kunden gerichteten gesetzlich vorgeschriebenen und alle weiteren Informationen und Unterlagen zustellen darf.

13.2 spot9 als Erklärungsbote des Kunden
Gegenüber der spot9 GmbH abgegebene Weisungen und Mitteilungen des Kunden gehen der Bank erst in dem Zeitpunkt zu, in dem die spot9 GmbH die Weisung oder Mitteilung an die Bank weitergeleitet hat. Die spot9 GmbH ist dabei Erklärungsbote des Kunden. Die Bank ist nicht für die ordnungsgemäße und rechtzeitige Weiterleitung der Weisungen und Mitteilungen des Kunden durch die spot9 GmbH verantwortlich.

14. Kündigung/Vertragsende/Vertragsübernahme

14.1 Kündigungsrecht des Kunden
Der Kunde kann den Vertrag zur Nutzung des Services spot9 jederzeit kündigen. Kündigungserklärungen bedürfen zu ihrer Wirksamkeit der Textform. Laufende und/oder bereits abgeschlossene Transaktionen werden durch eine Kündigung nicht berührt. Im Übrigen gelten die Regelungen der Allgemeinen Geschäftsbedingungen der Bank.

14.2 Kopplung der Laufzeit an das Vertragsverhältnis zwischen Kunden und spot9
Dieser Vertrag über die Nutzung des spot9 Service endet automatisch mit Wirksamwerden einer Kündigung des Vertrages zwischen Kunden und der

spot9 GmbH über die Nutzung des spot9 Portals, da dieses Vertragsverhältnis in einem inhaltlichen Zusammenhang mit diesem Vertrag steht.

14.3 Vertragsübernahme
Die Bank behält sich das Recht vor, diesen Vertrag über den Service spot9 auf die spot9 GmbH, Fredersdorfer Straße 11, 10243 Berlin, zu übertragen. Im Verhältnis zur spot9 GmbH gelten dieselben Rechte und Pflichten des Kunden fort.

15. Änderungen dieser Nutzungsbedingungen

Änderungen dieser Vertragsbedingungen richten sich nach den Allgemeinen Geschäftsbedingungen der Bank in der jeweils aktuellen Fassung.

16. Schlussbestimmungen

16.1 Anwendbares Recht
Für den Vertrag gilt deutsches Recht.

16.2 Salvatorische Klausel
Sollte eine der vorstehenden Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt. Statt der unwirksamen Bestimmung gelten in diesem Fall die gesetzlichen Regelungen.