Bedingungen für Zahlungsdienste (Zahlungsdiensterahmenvertrag)

Stand: 01.09.2019

Die Bedingungen für Zahlungsdienste (Zahlungsdiensterahmenvertrag) gelten für die Ausführung von Zahlungsdiensten der Consors Finanz (nachfolgend auch „Bank“ genannt) als Zahlungsdienstleister gegenüber dem Kreditnehmer der Consors Finanz (nachfolgend auch „Kunde“ oder „Karteninhaber“ genannt) als Zahler.

A. Allgemeine Regeln für Zahlungsdienste

I. Geschäftstage der Bank

Geschäftstag ist jeder Tag, an dem die an der Ausführung eines Zahlungsvorgangs beteiligten Zahlungsdienstleister den für die Ausführung von Zahlungsvorgängen erforderlichen Geschäftsbetrieb unterhalten. Die Bank unterhält den für die Ausführung von Zahlungsaufträgen erforderlichen Geschäftsbetrieb an allen Werktagen mit Ausnahme von Samstagen und des 24. und 31. Dezember. Für **Bargeldauszahlungen** ist jeder Tag Geschäftstag.

II. Finanzielle Nutzungsgrenze

Der Kunde darf Zahlungsaufträge nur innerhalb des ihm eingeräumten Kreditrahmens erteilen.

III. Autorisierung von Zahlungsaufträgen / Einsatz der Karte

Der Kunde erteilt seine Zustimmung (Autorisierung) zur Belastung des ihm von der Bank eingeräumten Kreditrahmens (Zahlungsauftrag) mittels der ihm zur Verfügung gestellten Zahlungsinstruments (im Folgenden auch "Karte" oder „MasterCard“ genannt) wie folgt:

1. Bei Nutzung der Mastercard ist entweder ein Beleg zu unterschreiben, auf den das Vertragsunternehmen die Kartendaten übertragen hat, oder an Geldautomaten und automatisierten Kassen die PIN einzugeben. Nach vorheriger Abstimmung zwischen Kunde und Vertragsunternehmen kann der Kunde – insbesondere zur Beschleunigung eines Geschäftsvorfalls im Rahmen eines fernmündlichen Kontakts – ausnahmsweise darauf verzichten, den Beleg zu unterzeichnen und stattdessen lediglich seine Mastercard-Nummer angeben.
2. Beim Karteneinsatz an automatisierten Kassen kann von der Eingabe der PIN abgesehen werden:
   - Zur Bezahlung von Verkehrsnutzungsentgelten oder Parkgebühren an unbeaufsichtigten automatisierten Kassen.
   - Zur kontaktlosen Bezahlung von Kleinbeträgen. Hierbei ist die Karte mit Kontaktlosfunktion an ein Kartenlesegerät zu halten. Es gelten die von der Bank festgelegten Betrags- und Nutzungsgrenzen.
3. Bei Online-Bezahlvorgängen erfolgt die Authentifizierung des Karteninhabers, indem er auf Anforderung die gesondert vereinbarten Authentifizierungselemente einsetzt. **Authentifizierungselemente** sind
   - **Wissenselemente** (etwas, das der Karteninhaber weiß, z.B. Online-Passwort)
   - **Besitzelemente** (etwas, das der Karteninhaber besitzt, z.B. mobiles Endgerät zur Erzeugung und zum Empfang von einmal verwendbaren Transaktionsnummern (TAN) als Besitznachweis) oder
   - **Seinselemente** (etwas, das der Karteninhaber ist, z.B. Fingerabdruck).
4. Mit dem Einsatz der Karte erteilt der Karteninhaber die Zustimmung (Autorisierung) zur Ausführung der Kartenzahlung. Soweit dafür zusätzlich die Unterschrift, eine PIN oder ein sonstiges Authentifizierungselement erforderlich ist, wird die Zustimmung erst mit deren Einsatz erteilt. Nach Erteilung der Zustimmung kann der Karteninhaber die Kartenzahlung nicht mehr widerrufen. In der Autorisierung ist zugleich die ausdrückliche Zustimmung enthalten, dass die Bank die für die Ausführung der Kartenzahlung notwendigen personenbezogenen Daten des Karteninhabers verarbeitet, übermittelt und speichert.

IV. Ablehnung von Zahlungsaufträgen

Die Bank ist berechtigt, die Ausführung von Zahlungsaufträgen insgesamt abzulehnen, wenn

- sich der Karteninhaber nicht mit seiner PIN oder seinem sonstigen Authentifizierungselement legitimiert hat,
- der für die Kartenzahlung geltende Verfügungsrahmen der Karte oder die finanzielle Nutzungsgrenze nicht eingehalten ist,
- die Karte des Kunden gesperrt ist bzw. die Voraussetzungen für eine Sperrung der Karte vorliegen,
- der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der Karte besteht
- der Kunde entgegen seiner vertraglichen Pflicht Änderungen seiner Anschrift nicht unaufgefordert mitgeteilt hat.

Der Kunde wird unverzüglich über die Nichtausführung eines Zahlungsauftrags unterrichtet. Soweit möglich, wird die Bank die Gründe für die Nichtausführung und eventuelle Abhilfemöglichkeiten benennen. Hierüber wird der Karteninhaber über das Terminal, an dem die Karte eingesetzt wird, oder beim Online-Einsatz auf dem vereinbarten Weg unterrichtet.

V. Information über die Ausführung von Zahlungsvorgängen

1. Die Information über die Ausführung von Zahlungsvorgängen erteilt die Bank mit dem monatlichen Rechnungsabschluss (Kontoauszug), den der Kunde nach Maßgabe der „Vertragsbedingungen Kreditrahmen“ erhält.
2. Der Kunde hat seine Kontoauszüge und sonstigen Abrechnungen unverzüglich auf ihre Richtigkeit und Vollständigkeit hin zu überprüfen und etwaige Einwendungen gegen die Richtigkeit oder Vollständigkeit des Rechnungsabschlusses nach Maßgabe der mit dem Kunden vereinbarten Vertragsbedingungen Kreditrahmen geltend zu machen.

VI. Erstattungs-, Berichtigungs- und Schadensersatzansprüche des Kunden und der Bank

1. **Erstattung bei einem nicht autorisierten Zahlungsauftrag:** Im Falle eines nicht autorisierten Zahlungsauftrags in Form der Abhebung von Bargeld oder der Verwendung der Karte zur Bezahlung bei einem Vertragsunternehmen hat die Bank gegen den Karteninhaber keinen Anspruch auf Erstattung ihrer Aufwendungen. Wurde der Betrag einem Konto belastet, bringt die Bank dieses wieder auf den Stand, auf dem es sich ohne den nicht autorisierten Zahlungsauftrag befunden hätte. Vorgenannte Verpflichtung ist spätestens bis zum Ende des Geschäftstags zu erfüllen, der auf den Tag folgt, an welchem der Bank angezeigt wurde, dass der Zahlungsauftrag nicht autorisiert ist oder die Bank auf andere Weise davon Kenntnis erhalten hat. Hat die Bank einer zuständigen Behörde berechtigte Gründe für den Verdacht, dass ein betrügerisches Verhalten des Kunden vorliegt, schriftlich mitgeteilt, hat die Bank ihre Verpflichtung aus den Sätzen 2 und 3 unverzüglich zu prüfen und zu erfüllen, wenn sich der Betrugsverdacht nicht bestätigt.
2. **Erstattung bei nicht erfolgter, fehlerhafter oder verspäteter Ausführung eines autorisierten Zahlungsauftrags:** Im Falle einer nicht erfolgten oder fehlerhaften Ausführung eines autorisierten Zahlungsauftrags in Form der Abhebung von Bargeld oder der Verwendung der Karte zur Bezahlung bei einem Vertragsunternehmen kann der Karteninhaber von der Bank die unverzügliche und ungekürzte Erstattung des Verfügungsbetrages insoweit verlangen, als die Kartenverfügung nicht erfolgte oder fehlerhaft war. Wurde der Betrag einem Konto belastet, bringt die Bank dieses wieder auf den Stand, auf dem es sich ohne die nicht erfolgte oder fehlerhafte Kartenverfügung befunden hätte.

   Der Kunde kann darüber hinaus die Erstattung derjenigen Entgelte und Zinsen von der Bank insoweit verlangen, die die Bank ihm im Zusammenhang mit der nicht erfolgten oder fehlerhaften Ausführung der Zahlung in Rechnung gestellt oder mit denen sie das Konto des Kunden belastet hat.

   Geht der Zahlungsbetrag beim Zahlungsdienstleister des Zahlungsempfängers erst nach Ablauf der Ausführungsfrist in Abschnitt E. Ziffer V. ein (Verspätung), kann der Kunde von der Bank fordern, dass die Bank vom Zahlungsdienstleister des Zahlungsempfängers verlangt, dass dieser die Gutschrift des Zahlungsbetrags auf dem Konto des Zahlungsempfängers so vornimmt, als sei die Kartenzahlung ordnungsgemäß ausgeführt worden.

Wurde eine autorisierte Kartenverfügung nicht oder fehlerhaft ausgeführt, wird die Bank die Kartenverfügung auf Verlangen des Karteninhabers nachvollziehen und ihn über das Ergebnis unterrichten.

3. **Schadensersatzansprüche des Kunden aufgrund einer nicht autorisierten oder einer nicht erfolgten oder fehlerhaften Ausführung eines autorisierten Zahlungsauftrags:** Im Falle eines nicht autorisierten Zahlungsauftrags oder im Falle einer nicht erfolgten, fehlerhaften oder verspäteten Ausführung einer autorisierten Zahlung, kann der Kunde von der Bank einen etwaigen Schaden, der nicht bereits von Nr. 1 und 2 erfasst ist, ersetzt verlangen. Dies gilt nicht, wenn die Bank die Pflichtverletzung nicht zu vertreten hat. Die Bank hat hierbei ein Verschulden, das einer zwischengeschalteten Stelle zur Last fällt, wie eigenes Verschulden zu vertreten, es sei denn, dass die wesentliche Ursache bei einer zwischengeschalteten Stelle liegt, die der Zahlungsdienstnutzer vorgegeben hat. Erfolgt der Einsatz der Karte in einem Land außerhalb Deutschlands und des Europäischen Wirtschaftsraumes, beschränkt sich die Haftung der Bank für das Verschulden einer an der Abwicklung des Zahlungsvorgangs beteiligten Stelle auf die sorgfältige Auswahl und Unterweisung einer solchen Stelle. Hat der Kunde durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Bank und Kunde den Schaden zu tragen haben. Die Haftung nach diesem Absatz ist auf 12.500 EUR je Kartenverfügung begrenzt. Diese betragsmäßige Haftungsbeschränkung gilt nicht

   - für nicht autorisierte Zahlungen,
   - bei Vorsatz oder grober Fahrlässigkeit der Bank,
   - für Gefahren, die die Bank besonders übernommen hat, und
   - für den dem Kunden entstandenen Zinsschaden, wenn der Kunde Verbraucher ist.

4. **Ausschluss von Ansprüchen und Frist für deren Geltendmachung:** Ansprüche und Einwendungen des Kunden gegen die Bank nach den Regeln dieser Ziffer VI. sind in folgenden Fällen ausgeschlossen:

4.1. Die Bank weist gegenüber dem Kunden nach, dass der Zahlungsbetrag rechtzeitig und ungekürzt beim Zahlungsdienstleister des Zahlungsempfängers eingegangen ist.

4.2. Die Zahlung wurde in Übereinstimmung mit der vom Zahlungsempfänger angegebenen fehlerhaften Kundenkennung des Zahlungsempfängers ausgeführt. In diesem Fall kann der Kunde jedoch von der Bank verlangen, dass sie sich im Rahmen ihrer Möglichkeiten darum bemüht, den Zahlungsbetrag wiederzuerlangen. Ist die Wiedererlangung des Zahlungsbetrags nicht möglich, so ist die Bank verpflichtet, dem Kunden auf schriftlichen Antrag alle verfügbaren Informationen mitzuteilen, damit der Kunde gegen den tatsächlichen Empfänger des Zahlungsbetrags einen Anspruch auf Erstattung des Zahlungsbetrags geltend machen kann. Für die Tätigkeiten nach den Sätzen 2 und 3 berechnet die Bank das im „Preis- und Leistungsverzeichnis“ der Bank ausgewiesene Entgelt für Nachforschungen.

4.3. Ansprüche des Kunden sind ausgeschlossen, wenn der Kunde die Bank nicht spätestens 13 Monate nach dem Tag der Belastung mit der Kartenverfügung darüber unterrichtet, dass es sich um eine nicht autorisierte oder fehlerhaft ausgeführte Zahlung handelt. Der Lauf der 13-monatigen Frist beginnt nur, wenn die Bank den Kunden über die Belastungsbuchung im Rechnungsabschluss unterrichtet hat; andernfalls ist für den Fristbeginn der Tag der Unterrichtung maßgeblich.

4.4. Ansprüche des Kunden sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das die Bank keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können, oder von der Bank aufgrund einer gesetzlichen Verpflichtung herbeigeführt wurden.

VII. Sorgfalts- und Mitwirkungspflichten des Kunden

1. **Anzeige des Ausbleibens von Mitteilungen (insbesondere von Kontoauszügen):** Falls dem Kunden Kontoauszüge/Rechnungsabschlüsse nicht zugehen, muss er die Bank unverzüglich benachrichtigen.
2. **Anzeige nicht autorisierter Verfügungen:** Der Kunde hat die Bank unverzüglich nach Feststellung eines nicht autorisierten, fehlerhaft oder verspätet ausgeführten Zahlungsvorgangs zu unterrichten. Dies gilt auch im Fall der Beteiligung eines Zahlungsauslösedienstleisters. Die Unterrichtung kann unter der in Abschnitt B. Ziffer II. Nr. 6.1 genannten Telefonnummer erfolgen. In Fällen missbräuchlicher Verfügungen durch Dritte hat der Kunde unverzüglich Anzeige bei der Polizei zu erstatten.

VIII. Sperrung eines verfügbaren Geldbetrags

Die Bank ist berechtigt, auf dem Kreditkonto des Kunden einen im Rahmen der finanziellen Nutzungsgrenze verfügbaren Geldbetrag zu sperren, wenn der Zahlungsvorgang vom oder über den Zahlungsempfänger ausgelöst worden ist und der Kunde auch der genauen Höhe des zu sperrenden Geldbetrags zugestimmt hat. Den gesperrten Geldbetrag gibt die Bank unbeschadet sonstiger gesetzlicher oder vertraglicher Rechte unverzüglich frei, nachdem ihr der genaue Zahlungsbetrag mitgeteilt oder der Zahlungsauftrag zugegangen ist.

B. Nutzung der Karte

I. Allgemeine Regelungen

1. **Beschreibung der Karte, Eigentum und Gültigkeit:** Das dem Kunden zur Verfügung gestellte Zahlungsmittel (nachfolgend auch „Karte“ genannt) kann als physische Karte oder als digitale Karte zur Speicherung auf einem Telekommunikations-, Digital- oder IT-Gerät (mobiles Endgerät) ausgegeben werden. Diese Bedingungen gelten für beide Kartenformen gleichermaßen, es sei denn, es ist ausdrücklich etwas anderes geregelt. Für die digitale Karte gelten ergänzend die gesondert mit der Bank vereinbarten Nutzungsbedingungen für die digitale Karte. Die Karte gilt für das auf ihr angegebene Konto und wird auf den Namen des Kunden (Kreditnehmer 1) ausgestellt. Im Übrigen bleibt die Karte im Eigentum der Bank und ist nicht übertragbar. Sie ist ein Zahlungsinstrument und enthält neben der Kartennummer und dem Gültigkeitsdatum eine dreistellige Prüfziffer als Sicherheitsmerkmal, die gegebenenfalls zur Veranlassung von Zahlungsaufträgen benötigt wird. Der Nutzungsumfang der Karte ergibt sich aus den Vertragsbedingungen Kreditrahmen.
2. **Persönliche Geheimzahl (PIN):** Für die Nutzung von automatisierten Kassen bei Vertragsunternehmen und von Geldautomaten kann dem Karteninhaber für seine Karte eine persönliche Geheimzahl (PIN) zur Verfügung gestellt werden. Die Karte kann an automatisierten Kassen sowie an Geldautomaten, an denen im Zusammenhang mit der Verwendung der Karte die PIN eingegeben werden muss, nicht mehr eingesetzt werden, wenn die PIN dreimal hintereinander falsch eingegeben wurde. Der Karteninhaber sollte sich in diesem Fall mit seiner Bank, möglichst mit der kontoführenden Stelle, in Verbindung setzen.
3. **Rückgabe der Karte:** Mit Aushändigung einer neuen, spätestens aber nach Ablauf der Gültigkeit der Karte, ist die Bank berechtigt, die alte Karte zurückzuverlangen. Endet die Berechtigung, die Karte zu nutzen, vorher (z.B. durch Kündigung der Kontoverbindung oder des Kartenvertrages), so hat der Karteninhaber die Karte unverzüglich an die Bank zurückzugeben. Die Bank behält sich das Recht vor, auch während der Laufzeit einer Karte diese gegen eine neue auszutauschen. Kosten entstehen dem Karteninhaber dadurch nicht.

II. Sorgfalts- und Mitwirkungspflichten des Kunden

1. **Unterschrift:** Der Karteninhaber hat die Karte nach Erhalt unverzüglich auf dem Unterschriftsfeld zu unterschreiben.
2. **Sorgfältige Aufbewahrung der Karte:** Die Karte ist mit besonderer Sorgfalt aufzubewahren, um Abhandenkommen und Missbrauch zu verhindern. Sie darf insbesondere nicht unbeaufsichtigt im Kraftfahrzeug aufbewahrt werden, da sie missbräuchlich eingesetzt werden kann.
3. **Geheimhaltung der PIN:** Der Karteninhaber hat dafür Sorge zu tragen, dass kein Dritter Kenntnis von seiner PIN erlangt. Die PIN darf insbesondere nicht auf der Karte vermerkt oder in anderer Weise zusammen mit dieser aufbewahrt werden. Denn jede Person, die die PIN kennt und in den Besitz der Karte kommt beziehungsweise die Mastercard-Nummer kennt, hat die Möglichkeit, missbräuchliche Verfügungen zu tätigen (zum Beispiel Geld an Geldautomaten abzuheben).
4. **Schutz der Authentifizierungselemente für Online-Bezahlvorgänge:** Der Karteninhaber hat alle zumutbaren Vorkehrungen zu treffen, um seine mit der Bank vereinbarten Authentifizierungselemente für Online-Bezahlvorgänge vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass die Authentifizierungselemente für Online-Bezahlvorgänge missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt werden. Zum Schutz der einzelnen Authentifizierungselemente für Online-Bezahlvorgänge hat der Karteninhaber vor allem Folgendes zu beachten:

4.1. **Wissenselemente**, wie z.B. das Online-Passwort, sind geheim zu halten; sie dürfen insbesondere

   - nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden,

- nicht außerhalb von Online-Bezahlvorgängen in Textform (z.B. per E-Mail oder Messenger-Dienst) weitergegeben werden,
- nicht ungesichert elektronisch gespeichert (z.B. Speicherung des Online-Passworts im Klartext 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) oder zur Prüfung des Seinselements (z.B. mobiles Endgerät mit Anwendung für Kreditkartenzahlung und Fingerabdrucksensor) dient.

4.2. **Besitzelemente**, wie z.B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Karteninhabers (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 Kreditkartenzahlungen (z.B. Karten-App, Authentifizierungs- App) nicht nutzen können,
- ist die Anwendung für das Online-Banking (z.B. Karten-App, Authentifizierungs-App) auf dem mobilen Endgerät des Kunden zu deaktivieren, bevor der Kunde den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf oder Entsorgung des Mobiltelefons) und
- dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb der Online-Bezahlvorgänge mündlich (z.B. per Telefon) oder in Textform (z.B. per Email, Messenger-Dienst) weitergegeben werden.

4.3. **Seinselemente**, wie z.B. Fingerabdruck des Karteninhabers, dürfen auf einem mobilen Endgerät des Karteninhabers für Online-Bezahlvorgänge nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für Online-Bezahlvorgänge genutzt wird, Seinselemente anderer Personen gespeichert, ist für Online-Bezahlvorgänge das von der Bank ausgegebene Wissenselement (z.B. Online-Passwort) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

5. **Kontrollpflichten bei Online-Bezahlvorgängen:** Sollten bei Online-Bezahlvorgängen an den Karteninhaber Angaben zum Zahlungsvorgang (z.B. der Name des Vertragsunternehmens und der Verfügungsbetrag) mitgeteilt werden, sind diese Daten vom Karteninhaber auf Richtigkeit zu prüfen.

6. **Unterrichtungs- und Anzeigepflichten des Karteninhabers:**

6.1. Stellt der Karteninhaber den Verlust oder Diebstahl seiner Karte, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von Karte, PIN oder für Online-Bezahlvorgänge vereinbarter Authentifizierungselemente fest, so ist die Bank, und zwar möglichst die kontoführende Stelle, oder eine Repräsentanz des MasterCard-Verbundes unverzüglich zu unterrichten, um die Kreditkarte sperren zu lassen (Sperranzeige). **Die Sperranzeige kann der Karteninhaber auch jederzeit gegenüber dem Zentralen Sperrannahmedienst (Telefon 02 03/34 69 54 02 (kostenpflichtig) oder 116 116 (kostenfreier Notdienst) und aus dem Inland und +49 116 116 oder +4930-4050 4050 aus dem Ausland) abgeben.** Der Karteninhaber hat die Bank unverzüglich nach Feststellung einer nicht autorisierten oder fehlerhaft ausgeführten Kartenverfügung zu unterrichten und jeden Diebstahl oder Missbrauch auch unverzüglich bei der Polizei anzuzeigen.

6.2. Hat der Karteninhaber den Verdacht, dass eine andere Person unberechtigt in den Besitz seiner Karte gelangt ist, eine missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von Karte, PIN oder für Online-Bezahlvorgänge vereinbarter Authentifizierungselemente vorliegt, muss er ebenfalls unverzüglich eine Sperranzeige abgeben.

6.3. Für den Ersatz einer verlorenen, gestohlenen, missbräuchlich verwendeten oder sonst nicht autorisiert genutzten Karte berechnet die Bank dem Karteninhaber das im „Preis- und Leistungsverzeichnis“ der Bank genannte Entgelt, welches allenfalls die ausschließlich und unmittelbar mit dem Ersatz verbundenen Kosten abdeckt. Dies gilt nicht, wenn die Bank die Umstände, die zur Ausgabe der Ersatzkarte geführt haben, zu vertreten hat oder diese ihr zuzurechnen sind.

III. Sperre und Einziehung der Karte

Die Bank darf die Karte sperren und ihren Einzug (z.B. an Geldautomaten) veranlassen, wenn

- sachliche Gründe im Zusammenhang mit der Sicherheit der Karte dies rechtfertigen,
- der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der Karte besteht,
- ein wesentlich erhöhtes Risiko besteht, dass der Kunde seiner Zahlungsverpflichtung nicht nachkommen kann,
- sie berechtigt ist, den Kreditrahmen außerordentlich zu kündigen.

Die Bank wird den Karteninhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre, über die Sperre unterrichten. Die Bank wird die Karte entsperren und diese durch eine neue Karte ersetzen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Auch hierüber unterrichtet sie den Karteninhaber unverzüglich.

IV. Umrechnung von Fremdwährungsbeträgen

Nutzt der Karteninhaber die Karte für Verfügungen, die nicht auf EUR lauten oder außerhalb der Staaten der Euro-Zone getätigt werden, wird das Konto gleichwohl in EUR belastet. Zur Umrechnung der auf eine Fremdwährung lautenden Umsätze zieht die Bank den von MasterCard auf Basis verschiedener Großhandelskurse (herangezogen aus unabhängigen internationalen Quellen wie beispielsweise Bloomberg, Reuters oder staatlich festgelegter Kurse) für die jeweilige Währung gebildeten Wechselkurs als Referenzwechselkurs heran (Umrechnungskurs) Dieser Umrechnungskurs ist auf www.mastercard.com/global/currencyconversion abrufbar; Verkaufsabschläge werden keine berechnet. Für Verfügungen, die nicht in Euro erfolgen, wird die Bank – soweit vereinbart – ein Entgelt in Rechnung stellen. Der Tag für die Umrechnung ist der Geschäftstag (inklusive Samstag), an welchem die Bank mit der Forderung der jeweiligen Akzeptanzstelle belastet wird (Eingangstag). Zur Umrechnung wird jeweils der Referenzwechselkurs des Vortags herangezogen. Fällt der Eingangstag auf einen Montag, wird der Referenzwechselkurs des vorhergehenden Samstags verwendet. Die Bank gibt dem Kunden mit dem Kontoauszug den Eingangstag und den Umrechnungskurs bekannt.

V. Haftung

1. **Haftung des Kunden bis zur Sperranzeige**

1.1. Verliert der Karteninhaber seine Karte oder PIN, werden sie ihm gestohlenen, kommen sie ihm sonst abhanden oder werden die Karte oder die für Online-Bezahlvorgänge vereinbarten Authentifizierungselemente sonst missbräuchlich verwendet und kommt es dadurch zu nicht autorisierten Kartenverfügungen in Form der Abhebung von Bargeld oder der Verwendung der Karte zur Bezahlung bei einem Vertragsunternehmen, so haftet der Karteninhaber für Schäden, die bis zum Zeitpunkt der Sperranzeige verursacht werden, bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Karteninhaber an dem Verlust, Diebstahl oder sonstigen Abhandenkommen oder sonstigen Missbrauch ein Verschulden trifft.

1.2. Der Karteninhaber haftet nicht nach Ziffer 1.1, wenn

- es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung der Karte oder der für Online-Bezahlvorgänge vereinbarten Authentifizierungselemente vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust der Karte durch einen Angestellten, einen Agenten, eine Zweigniederlassung der Bank oder eine sonstige Stelle, an die Tätigkeiten der Bank ausgelagert wurden, verursacht worden ist.

1.3. Erfolgt der Einsatz der Karte in einem Land außerhalb Deutschlands und des Europäischen Wirtschaftsraumes, trägt der Karteninhaber den aufgrund nicht autorisierter Kartenverfügungen entstehenden Schaden nach Ziffer 1.1 auch über einen Betrag von 50 Euro hinaus, wenn der Karteninhaber die ihm nach diesen Bedingungen obliegenden Pflichten fahrlässig verletzt hat. Hat die Bank durch eine Verletzung ihrer Pflichten zur Entstehung des Schadens beigetragen, haftet die Bank für den entstandenen Schaden im Umfang des von ihr zu vertretenden Mitverschuldens.

1.4. Kommt es vor der Sperranzeige zu nicht autorisierten Verfügungen und hat der Kunde in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit kann insbesondere dann vorliegen, wenn

- der Kunde den Verlust oder Diebstahl der Karte oder die missbräuchliche Verfügung der Bank oder einer MasterCard-Repräsentanz schuldhaft nicht unverzüglich mitgeteilt hat, nachdem er hiervon Kenntnis erlangt hat,
- die persönliche Geheimzahl oder das vereinbarte Wissenselement für Online-Bezahlvorgänge (z.B. Online-Passwort) auf der Karte vermerkt oder zusammen mit der Karte verwahrt war (z.B. im Originalbrief, in dem sie dem Karteninhaber mitgeteilt wurde) oder

- die persönliche Gemeinzahl oder das vereinbarte Wissenselement für Online-Bezahlvorgänge (z.B. Online-Passwort) einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde.

1.5. Eine Haftung des Kunden für Schäden, die innerhalb des Zeitraums, für den der Kreditrahmen (Abschnitt A. Ziffer II.) gilt, verursacht werden, beschränkt sich in jedem Fall auf den für die Karte geltenden Kreditrahmen.

1.6. Der Karteninhaber ist nicht zum Ersatz des Schadens nach den Nr. 1.1, 1.3 und 1.4 verpflichtet, wenn der Karteninhaber die Sperranzeige nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

1.7. Abweichend von den Nr. 1.1, 1.3 und 1.4 ist der Karteninhaber nicht zum Schadensersatz verpflichtet, wenn die Bank vom Karteninhaber eine starke Kundenauthentifizierung im Sinne des § 1 Abs. 24 Zahlungsdiensteaufsichtsgesetz (ZAG) nicht verlangt hat oder der Zahlungsempfänger oder sein Zahlungsdienstleister diese nicht akzeptiert hat, obwohl die Bank zur starken Kundenauthentifizierung nach § 55 ZAG verpflichtet war. Eine starke Kundenauthentifizierung erfordert die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen (etwas, das der Karteninhaber weiß, zum Beispiel PIN oder Online-Passwort), Besitz (etwas, das der Karteninhaber besitzt, zum Beispiel Kreditkarte oder mobiles Endgerät) oder Sein (etwas, das der Karteninhaber ist, zum Beispiel Fingerabdruck).

Die Nr. 1.2, 1.5 bis 1.7 finden keine Anwendung, wenn der Karteninhaber in betrügerischer Absicht gehandelt hat.

2. **Haftung des Kunden ab Sperranzeige**

Sobald der Verlust oder Diebstahl der Karte, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung der Karte, PIN oder für Online-Bezahlvorgänge vereinbarter Authentifizierungselemente gegenüber der Bank oder einer MasterCard-Repräsentanz angezeigt wurde, übernimmt die Bank alle danach durch Verfügungen in Form

- der Abhebung von Bargeld oder
- der Verwendung der Karte zur Bezahlung bei einem Vertragsunternehmen

entstehenden Schäden. Handelt der Karteninhaber in betrügerischer Absicht, trägt der Karteninhaber auch die nach der Sperranzeige entstehenden Schäden.

VI. Gesamtschuldnerische Haftung mehrerer Kunden

Für die Verbindlichkeiten aus einer gemeinsam beantragten Mastercard haften die Kunden als Gesamtschuldner, d.h. die Bank kann von jedem Kunden die Erfüllung sämtlicher Ansprüche fordern. Jeder Kunde hat dafür Sorge zu tragen, dass die an ihn ausgegebene Karte mit Wirksamwerden der Kündigung unverzüglich an die Bank zurückgegeben wird. Die Aufwendungen, die aus der weiteren Nutzung einer Karte bis zu ihrer Rückgabe an die Bank entstehen, haben die Kunden ebenfalls gesamtschuldnerisch zu tragen. Unabhängig davon wird die Bank zumutbare Maßnahmen ergreifen, um Mastercard-Verfügungen nach der Kündigung des Mastercard-Vertragsverhältnisses zu unterbinden.

VII. Zahlungsverpflichtungen der Bank; Einwendungen

Die Bank ist gegenüber Vertragsunternehmen sowie den Kreditinstituten, die die MasterCard an ihren Geldautomaten akzeptieren, verpflichtet, die vom Karteninhaber mit der Karte getätigten Umsätze zu begleichen. Die Bank unterrichtet den Karteninhaber mindestens einmal monatlich auf dem vereinbarten Weg über alle im Zusammenhang mit der Begleichung der Kartenumsätze entstehenden Aufwendungen. Der Betrag ist fällig, nachdem die Bank dem Karteninhaber Abrechnung erteilt hat. Nach Erteilung der Abrechnung werden die Umsätze dem vereinbarten Abrechnungskonto belastet. Einwendungen und sonstige Beanstandungen des Karteninhabers aus dem Vertragsverhältnis zu dem Vertragsunternehmen, bei dem die Karte eingesetzt wurde, sind unmittelbar gegenüber dem Vertragsunternehmen geltend zu machen.

C. Online-Banking

I. Leistungsangebot

Der Kunde kann während der Vertragslaufzeit über den Kreditrahmen Bankgeschäfte mittels Online-Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Online-Banking abrufen und gemäß § 675f Absatz 3 BGB Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absätze 33 und 34 Zahlungsdiensteaufsichtsgesetz (ZAG) nutzen. Darüber hinaus kann er von ihm ausgewählte Drittdienste nutzen.

II. Voraussetzungen zur Nutzung des Online-Banking

1. Der Kunde 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 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 Kunde sich gegenüber der Bank als berechtigte Person auszuweisen, auf Informationen zugreifen (siehe Ziffer III.) sowie Aufträge erteilen (siehe Abschnitt E.).
3. Authentifizierungselemente sind
   - **Wissenselemente**, also etwas, das nur der Kunde weiß (z.B. persönliche Identifikationsnummer für das Online-Banking (OLB-PIN)
   - **Besitzelemente**, also etwas, das nur der Kunde besitzt (z.B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern (TAN), die den Besitz des Kunden nachweisen, wie das mobile Endgerät), oder
   - **Seinselemente**, also etwas, das der Kunde ist (Inhärenz, z.B. Fingerabdruck als biometrisches Merkmal des Kunden).
4. Die Authentifizierung des Kunden erfolgt, indem der Kunde gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.

III. Zugang zum Online-Banking

1. Der Kunde erhält Zugang zum Online-Banking der Bank, wenn
   - er seine individuelle Teilnehmerkennung (z.B. Kontonummer, Anmeldename) angibt und
   - er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
   - keine Sperre des Zugangs vorliegt (siehe Ziffer IV Nr. 4 und Ziffer V.).

   Nach Gewährung des Zugangs zum Online-Banking kann auf Informationen zugegriffen oder können 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 Kunden auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Online Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kunden und die Kontonummer sind für den vom Kunden genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Zahlungsdaten (§ 1 Absatz 26 Satz 2 ZAG).

IV. Sorgfaltspflichten des Kunden

1. **Schutz der Authentifizierungselemente**

1.1. Der Kunde hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird.

1.2. Zum Schutz der einzelnen Authentifizierungselemente hat der Kunde vor allem Folgendes zu beachten:

(1) **Wissenselemente**, wie z.B. die PIN, 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 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) oder zur Prüfung des Seinselements (z.B. mobiles Endgerät mit Anwendung für das Online Banking und Fingerabdrucksensor) dient.

(2) **Besitzelemente**, wie z.B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
   - ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Kunden (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 Kunden zu deaktivieren, bevor der Kunde 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 Banking mündlich (z.B. per Telefon) oder in Textform (z.B. per Email, Messenger-Dienst) weitergegeben werden und
- muss der Kunde, 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 Kunden aktivieren.

(3) **Seinselemente**, wie z.B. Fingerabdruck des Kunden, dürfen auf einem mobilen Endgerät des Kunden für das Online Banking 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.

1.3. Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (z.B. Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.

1.4. Die für das mobile-TAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Kunde diese Telefonnummer für das Online Banking nicht mehr nutzt.

1.5. Ungeachtet der Schutzpflichten nach den Ziffern 1.1 bis 1.4 darf der Kunde seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden. Sonstige Drittdienste hat der Kunde mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

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

3. **Prüfung der Auftragsdaten mit von der Bank angezeigten Daten:** Die Bank zeigt dem Kunden die von ihr empfangenen Auftragsdaten (z.B. Betrag, Kontonummer des Zahlungsempfängers) über das gesondert vereinbarte Gerät des Kunden an (zum Beispiel mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Kunde ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

4. **Anzeige- und Unterrichtungspflichten/Sperranzeige:** Stellt der Kunde 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 Kunde die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Kunde kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle (z.B. telefonisch) abgeben. Der Kunde hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen. Hat der Kunde den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls unverzüglich eine Sperranzeige abgeben.

V. Nutzungssperre

1. **Sperre auf Veranlassung des Kunden:** Die Bank sperrt auf Veranlassung des Kunden, insbesondere im Fall der Sperranzeige nach vorstehender Ziffer IV. Nr. 4,
   - den Online-Banking-Zugang für ihn oder
   - seine Authentifizierungselemente zur Nutzung des Online-Banking

2. **Sperre auf Veranlassung der Bank**

2.1. Die Bank darf den Online-Banking-Zugang für einen Kunden sperren, wenn
- sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
- 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.

2.2. Wurde die OLB-PIN dreimal in Folge falsch eingegeben, sperrt die Bank ebenfalls den Zugang zum Online-Banking. Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Kommunikationsweg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

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. Der Kunde kann sein Aufhebungsverlangen während der Geschäftszeiten der Bank auch unter der Rufnummer **02 03/34 69 54 02** an die Bank richten.

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 unterblieben, 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.

VI. Haftung

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 Bedingungen (z.B. Bedingungen für den Überweisungsverkehr).

2. **Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente**

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 Kunden ein Verschulden trifft.

(2) Der Kunde ist nicht zum Ersatz des Schadens vorgenannten Schadens 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 Kunde in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den in den Absätzen (1) und (2) genannten Regelungen den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Kunden kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach den Ziffern IV. Nr. 1.2, IV. Nr. 1.4, IV. Nr. 3 und IV. Nr. 4 dieser Bedingungen verletzt hat.

(4) Abweichend von den in den Absätzen (1) und (3) genannten Regelungen ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Kunden 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.

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

(6) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen (1) und (3) verpflichtet, wenn er die Sperranzeige nach Ziffer IV. Nr. 4 dieser Bedingungen nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

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

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.

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.

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.

VII. Änderungen

Die Bank ist berechtigt, das Angebot des Online-Banking teilweise oder ganz jederzeit einzustellen; eine Verpflichtung zur Aufrechterhaltung des Angebots des Online-Banking besteht nicht. Über eine Einstellung wird die Bank rechtzeitig vorab auf dem elektronischen Kommunikationsweg (z.B. per E-Mail oder SMS) informieren.

D. MasterCard® 3D Secure

Der Kunde hat das ihm bereitgestellte MasterCard® 3D Secure-Verfahren (nachfolgend „Mastercard Identity Check“) für die an ihn ausgegebene Karte zu nutzen. Mastercard Identity Check ist ein Verfahren zur Authentifizierung des Kunden und dient dazu, missbräuchliche Zahlungen mit der Karte bei Kartenakzeptanzstellen im Internet (nachfolgend „Internet-Zahlungsvorgang“) zu vermeiden. Die Bank ist berechtigt, Ausnahmen für eine Authentifizierung mit Mastercard Identity Check für Kleinbetragszahlungen zuzulassen.

I. Registrierung

Jeder Kunde mit einer gültigen und nicht gesperrten Karte hat sich nach Aufforderung der Bank für Mastercard Identity Check über sein Online-Banking gemäß Vorgabe der Bank zu registrieren.

II. Authentifizierung

1. Der Kunde kann sich derzeit entweder über die Banking-App oder über das mobileTAN-Verfahren über ein mobiles Endgerät gemäß Nr. 2 authentifizieren. Die Bank behält sich vor, weitere Verfahren anzubieten oder angebotene Verfahren wieder abzuschalten. Der Kunde muss das von ihm gewünschte Verfahren bei Registrierung bzw. später im Online-Bank aktivieren; für das mobileTAN-Verfahren muss der Kunde zusätzlich eine Antwort auf eine Sicherheitsfrage hinterlegen.
2. Die für einen Internet-Zahlungsvorgang erforderliche Authentifizierung findet je nach Wahl des Authentifizierungs-Verfahrens wie folgt statt:
   - **Banking-App**: Der Kunde erhält über die Banking-App eine Push-Benachrichtigung auf sein mobiles Endgerät. Die Authentifizierung erfolgt über eine Bestätigungsseite der Banking-App, in dem die Transaktionsdetails angezeigt werden, und über die der Kunde den Internet-Zahlungsvorgang bestätigen kann.
   - **mobileTAN**: Der Kunde erhält eine transaktionsbezogene, zeitlich begrenzt gültige mobileTAN mit Transaktionsdetails an seine bei der Bank hinterlegte Mobilfunknummer. Die mobileTAN wird ungültig, wenn sie nicht innerhalb der vorgegebenen Zeit verwendet wird oder der Kunde eine neue mobileTAN für einen Internet-Zahlungsvorgang anfordert. Die Authentifizierung erfolgt über die Eingabe der mobileTAN auf einer Bestätigungsseite der Kartenakzeptanzstelle im Internet und die korrekte Beantwortung der ihm gegebenenfalls gestellten Sicherheitsfrage.

III. Sorgfaltspflichten

Der Kunde hat die folgenden Sorgfaltspflichten für die Nutzung von Mastercard Identity Check zu beachten:

1. Der Kunde hat das Risiko eines unberechtigten Zugriffs auf sein mobiles Endgerät durch geeignete Schutzmaßnahmen zu minimieren, z.B. durch eine passwortgeschützte Zugangssperre. Er hat insbesondere dafür zu sorgen, dass kein Dritter unberechtigt Kenntnis von den Zugangsdaten für das Endgerät erlangt, er diese Zugangsdaten Dritten nicht mitteilt oder zugänglich macht sowie die Zugangsdaten vor dem Zugriff Dritter sicher verwahrt.
2. Der Kunde hat das Betriebssystem des von ihm verwendeten mobilen Endgerätes stets aktuell zu halten; er darf an seinem mobilen Endgerät keine Veränderung der Administratorrechte vornehmen bzw. vom Hersteller gesetzte Nutzungsbeschränkungen entfernen (Jailbreaking, Rooting).
3. Der Kunde hat die Übereinstimmung der während des Internet-Zahlungsvorgangs zur Authentifizierung übermittelten Transaktionsdetails zu prüfen. Entsprechen diese nicht der vorgesehenen Transaktion, hat er die Transaktion abzubrechen und die Bank unverzüglich darüber zu informieren. Gleiches gilt, wenn der Kunde die Aufforderung zur Bestätigung eines Internet-Zahlungsvorgangs erhält, den er nicht beauftragt hat.

E. Überweisungen innerhalb Deutschlands

I. Merkmale des Zahlungsdienstes

Der Kunde kann die Bank nach Maßgabe der Ziffern II. bis V. beauftragen, durch Einzelüberweisungen Geldbeträge bargeldlos zu seinen Gunsten auf sein bei der Bank hinterlegtes Referenzkonto zu übermitteln. Die Bank kann dem Kunden weitere Überweisungsarten anbieten; für diese gelten die Ziffern II. bis V. entsprechend.

II. Auftragserteilung sowie Autorisierung und Widerruf

1. Die Bank führt Überweisungsaufträge anhand der vom Kunden in Textform angegebenen Kundenkennung IBAN (Internationale Bankkontonummer) durch, sofern der Zahlungsauftrag nicht mit dem Abschluss des Vertrages über den Kreditrahmen im Kreditvertrag selbst erteilt wurde. Der Kunde muss z.B. im Überweisungsauftrag folgende Angaben machen: Name des Zahlungsempfängers, IBAN des Zahlungsempfängers, Betrag, Name des Kunden, IBAN des Kunden.
2. Sofern Zahlungsempfänger der Kunde selbst ist und die Bankverbindung des Zahlungsempfängers mit dem bei der Bank hinterlegten Referenzkonto des Kunden übereinstimmt, nimmt die Bank Überweisungsaufträge auch fernmündlich (CashCall) oder elektronisch (CashClick) entgegen. Beim CashCall ist lediglich der Betrag für den Zahlungsauftrag anzugeben, beim CashClick wird der Überweisungsauftrag über das Online Banking-Portal der Bank erteilt.
3. Der Kunde muss einem Auftrag (z.B. Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z.B. Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden. In dieser Autorisierung ist zugleich die ausdrückliche Zustimmung enthalten, dass die Bank die für die Ausführung der Überweisung notwendigen personenbezogenen Daten des Kunden abruft (aus ihrem Datenbestand), verarbeitet, übermittelt und speichert. Die Bank bestätigt mittels Online Banking den Eingang des Auftrags.
4. Der Kunde ist berechtigt, für die Erteilung des Überweisungsauftrages an die Bank auch einen Zahlungsauslösedienst gemäß § 1 Abs. 33 ZAG zu nutzen, es sei denn, das Zahlungskonto des Kunden ist für ihn nicht online zugänglich.
5. Hat der Kunde einen Auftrag (z.B. Überweisung) autorisiert, kann der Kunde den Zahlungseingang mit Zugang des Auftrags bei der Bank bzw. mit Errei-

chen eines etwaig abweichenden Ausführungstermins nicht mehr widerrufen. Nutzt der Kunde für die Erteilung seines Überweisungsauftrags einen Zahlungsauslösedienstleister, so kann er den Überweisungsauftrag nicht mehr gegenüber der Bank widerrufen, nachdem er dem Zahlungsauslösedienstleister die Zustimmung zur Auslösung der Überweisung erteilt hat. Der Widerruf von Aufträgen kann nur außerhalb des Online Banking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Online Banking ausdrücklich vor.

III. Bearbeitung von Aufträgen durch die Bank

1. Für die Bearbeitung von Aufträgen gelten die in Ziffern IV. und V. getroffenen Regelungen. Geht der Auftrag nach dem angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Abschnitt A. Ziffer I. dieser Bedingungen, 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 Kunde hat den Auftrag autorisiert.
   - Die Berechtigung des Kunden für die jeweilige Auftragsart liegt vor.
   - Das Online-Banking-Datenformat ist eingehalten.
   - Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.
   - Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

   Liegen die Ausführungsbedingungen vor, führt die Bank die Aufträge aus. Liegen die Ausführungsbedingungen 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.

IV. Annahmefristen für Überweisungsaufträge

Überweisungsaufträge gelten als am Tag ihres Eingangs bei der Bank zugegangen, sofern sie innerhalb der Annahmefrist bei der Bank eingehen. Das gilt auch, wenn der Überweisungsauftrag über einen Zahlungsauslösedienstleister erteilt wird. Die Annahmefrist endet bei:

- beleghaften und fernmündlichen Aufträgen: um 15 Uhr an Geschäftstagen der Bank;
- beleglosen Aufträgen (per Online-Banking): um 16 Uhr an Geschäftstagen der Bank.

V. Ausführungsfristen (Überweisungsaufträge in Euro)

Die Bank hat sicherzustellen, dass der Überweisungsbetrag beim Zahlungsdienstleister des Zahlungsempfängers spätestens wie folgt eingeht:

- beleghafte und fernmündliche Überweisungsaufträge: max. 2 Geschäftstage ab Zugang des Auftrags
- beleglose Überweisungsaufträge (per Online-Banking): max. 1 Geschäftstag ab Zugang des Auftrags.

VI. Informationen des Kunden über Überweisungen

Die Bank unterrichtet den Kunden über die getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

F. Lastschriften

I. Allgemeine Merkmale

1. Der Kunde kann durch das SEPA-Basislastschriftverfahren („SEPA-LV“) über die Bank an einen Zahlungsempfänger Zahlungen in Euro bewirken. Im Falle des SEPA-LV können sich Zahlungsempfänger auch innerhalb des Gebiets des einheitlichen Euro-Zahlungsverkehrsraums (Single Euro Payments Area/ SEPA) befinden. Eine Lastschrift ist ein vom Zahlungsempfänger ausgelöster Zahlungsvorgang zu Lasten des Kontos des Kunden, bei dem die Höhe des jeweiligen Zahlungsbetrags vom Zahlungsempfänger angegeben wird.
2. Für die Ausführung von Zahlungen im SEPA-LV müssen der Zahlungsempfänger und dessen Zahlungsdienstleister das SEPA-LV nutzen.
3. Für das SEPA-LV hat der Kunde als Kundenkennung gegenüber dem Zahlungsempfänger die ihm mitgeteilte IBAN und bei grenzüberschreitenden Zahlungen außerhalb des EWR zusätzlich den BIC der Bank zu verwenden. Die Bank und die weiteren beteiligten Stellen führen die Zahlung an den Zahlungsempfänger ausschließlich anhand der im Lastschriftdatensatz angegebenen Kundenkennung aus.

II. Erteilung des SEPA-Lastschriftmandats

1. Der Kunde erteilt dem Zahlungsempfänger vor dem Zahlungsvorgang ein SEPA-Lastschriftmandat. Damit autorisiert er gegenüber der Bank die Einlösung von SEPA-Basislastschriften des Zahlungsempfängers. Das Mandat ist schriftlich oder in der mit der Bank vereinbarten Art und Weise zu erteilen. In dieser Autorisierung ist zugleich die ausdrückliche Zustimmung enthalten, dass die am Lastschrifteinzug beteiligten Zahlungsdienstleister und etwaige zwischengeschaltete Stellen die für die Ausführung der Lastschrift notwendigen personenbezogenen Daten des Kunden abrufen, verarbeiten, übermitteln und speichern. In dem SEPA-Lastschriftmandat müssen die folgenden Erklärungen des Kunden enthalten sein:
   - Erklärung des Zahlungsempfängers, Zahlungen vom Konto des Kunden mittels SEPA-Basislastschrift einzuziehen, und
   - Weisung an die Bank, die vom Zahlungsempfänger auf sein Konto gezogenen SEPA-Basislastschriften einzulösen.
2. Das SEPA-Lastschriftmandat muss folgende Autorisierungsdaten enthalten:
   - Bezeichnung des Zahlungsempfängers,
   - eine Gläubigeridentifikationsnummer,
   - Kennzeichnung als einmalige oder wiederkehrende Zahlung,
   - Name des Kunden (sofern verfügbar),
   - Bezeichnung der Bank des Kunden und
   - seine Kundenkennung.

   Die Einzugsermächtigung kann zusätzliche Angaben enthalten.
3. Der Zahlungsempfänger übermittelt elektronisch den Datensatz zur Einziehung der SEPA-Basislastschrift unter Einschaltung seines Zahlungsdienstleisters an die Bank als Zahlstelle.

III. Begrenzung und Nichtzulassung von SEPA-Basislastschriften

Der Kunde kann der Bank gesondert die Weisung erteilen, Zahlungen aus SEPA-Basislastschriften zu begrenzen oder nicht zuzulassen. Diese Weisung ist möglichst schriftlich zu erteilen und muss der Bank bis spätestens zum Ende des Geschäftstages vor dem im Datensatz der Lastschrift angegebenen Fälligkeitstag zugehen. Zusätzlich sollte diese auch gegenüber dem Zahlungsempfänger erklärt werden.

IV. Einzug der SEPA-Basislastschrift auf Grundlage des SEPA-Basislastschriftmandats durch den Zahlungsempfänger

Der Lastschriftdatensatz verkörpert auch die Weisung des Kunden an die Bank zur Einlösung der jeweiligen SEPA-Basislastschrift. Für den Zugang dieser Weisung verzichtet die Bank auf die für die nach Ziffer I. Nr. 2 vereinbarte Form für die Erteilung des SEPA-Lastschriftmandats.

V. Widerruf des SEPA-Lastschriftmandats

Das SEPA-Lastschriftmandat kann vom Kunden durch Erklärung gegenüber dem Zahlungsempfänger oder gegenüber der Bank möglichst schriftlich mit der Folge widerrufen werden, dass nachfolgende Zahlungsvorgänge nicht mehr autorisiert sind. Erfolgt der Widerruf gegenüber der Bank, wird dieser ab dem auf den Eingang des Widerrufs folgenden Geschäftstag wirksam. Zusätzlich sollte der Widerruf auch gegenüber dem Zahlungsempfänger erklärt werden, damit dieser keine weiteren Lastschriften einzieht.

VI. Verbleib des SEPA-Lastschriftmandats

Das vom Kunden erteilte SEPA-Lastschriftmandat verbleibt beim Zahlungsempfänger. Dieser übernimmt die Autorisierungsdaten und setzt etwaige zusätzliche Angaben in den Datensatz zur Einziehung von Lastschriften. Der jeweilige Lastschriftbetrag wird vom Zahlungsempfänger angegeben.

VII. Einlösung von Lastschriften

1. Die Bank stellt sicher, dass der Zahlungsbetrag spätestens zum jeweiligen Fälligkeitszeitpunkt beim Zahlungsdienstleister des Zahlungsempfängers eingeht. Lastschriften sind eingelöst, wenn die Belastungsbuchung nicht spätestens am zweiten Bankarbeitstag nach ihrer Vornahme rückgängig gemacht wird.

2. Lastschriften werden nicht dem Konto belastet oder werden bis spätestens am zweiten Bankarbeitstag nach ihrer Vornahme rückgängig gemacht, wenn
   - einer der in Abschnitt A. Ziffer IV. genannten Gründe vorliegt;
   - die im Lastschriftdatensatz angegebene IBAN des Zahlungspflichtigen keinem Konto des Kunden bei der Bank zuzuordnen ist,
   - der Bank ein Widerruf des SEPA-Lastschriftmandats zugegangen ist.

   Teileinlösungen nimmt die Bank nicht vor.
3. SEPA-Basislastschriften können darüber hinaus rückgängig gemacht werden, wenn die Lastschrift von der Bank nicht verarbeitet werden kann, weil
   - eine Gläubiger-Identifikationsnummer fehlt oder für die Bank erkennbar fehlerhaft ist,
   - eine Mandatsreferenz fehlt,
   - ein Ausstellungsdatum des Mandats fehlt oder
   - kein Fälligkeitstag angegeben ist.

VIII. Erstattungsanspruch des Kunden bei einer autorisierten Zahlung

1. Der Kunde kann bei einer aufgrund Lastschrift autorisierten Zahlung binnen einer **Frist von acht Wochen** ab dem Zeitpunkt der Belastungsbuchung auf seinem Konto von der Bank ohne Angaben von Gründen die Erstattung des belasteten Lastschriftbetrags verlangen. Die Bank bringt das Konto dann wieder auf den Stand, auf dem es sich ohne die Belastung durch die Zahlung befunden hätte. Etwaige Zahlungsansprüche des Zahlungsempfängers gegen den Kunden bleiben hiervon unberührt.
2. Der Erstattungsanspruch nach Nr. 1 ist ausgeschlossen, sobald der jeweilige Betrag der Lastschriftbelastungsbuchung durch eine ausdrückliche Genehmigung des Kunden unmittelbar gegenüber der Bank autorisiert worden ist.
3. Im Übrigen richten sich Erstattungsansprüche nach Abschnitt A. Ziffer VI.

G. Entgelte und Aufwendungen

I. Entgelte für Leistungen der Bank

Die Höhe der Entgelte für die üblichen Bankleistungen, die die Bank gegenüber Kunden erbringt, ergeben sich aus dem im Internet auf www.consorsfinanz.de veröffentlichten Preis- und Leistungsverzeichnis der Bank.

Wenn ein Kunde eine dort aufgeführte Sonderleistung in Anspruch nimmt und dabei keine abweichende Vereinbarung getroffen wurde, gelten die zu diesem Zeitpunkt im Preis- und Leistungsverzeichnis angegebenen Entgelte.

Für die Vergütung der nicht im Preis- und Leistungsverzeichnis aufgeführten Sonderleistungen, die im Auftrag des Kunden erbracht werden und die, nach den Umständen zu urteilen, nur gegen eine Vergütung zu erwarten sind, gelten, soweit keine andere Vereinbarung getroffen wurde, die gesetzlichen Vorschriften.

II. Aufwendungen

Ein möglicher Anspruch der Bank auf Ersatz von Aufwendungen richtet sich nach den gesetzlichen Vorschriften.

H. Vertragslaufzeit, Kündigung

I. Vertragslaufzeit

Der Zahlungsdiensterahmenvertrag wird auf unbestimmte Zeit geschlossen. Er endet aber mit Beendigung des Vertrages über die Einräumung eines Kreditrahmens, ohne dass es einer Kündigung bedarf.

II. Kündigung durch den Kunden

Der Kunde kann diesen Zahlungsdiensterahmenvertrag jederzeit ohne Einhaltung einer Frist zum Ende eines Monats kündigen. Sind mehrere Kunden Vertragspartner dieses Zahlungsdiensterahmenvertrages, kann jeder Kunde diesen Zahlungsdiensterahmenvertrag nur mit Wirkung für alle Kunden durch Kündigung beenden.

III. Kündigung durch die Bank

Die Bank kann diesen Zahlungsdiensterahmenvertrag mit einer Frist von zwei Monaten kündigen. Sofern die mit dem Kunden Vertragsbedingungen für den Kreditrahmen bzw. das Bürgerliche Gesetzbuch für die Kündigung eines Verbraucherdarlehensvertrages Sonderregelungen vorsehen, kann die Bank auch nach Maßgabe dieser Sonderregelungen kündigen. Im Übrigen bleibt das Recht der Bank zur außerordentlichen fristlosen Kündigung aus wichtigem Grund unberührt.

I. Änderungen des Zahlungsdiensterahmenvertrages

Änderungen dieses Zahlungsdiensterahmenvertrages werden dem Kunden spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens auf einem dauerhaften Datenträger angeboten.

Hat der Kunde mit der Bank im Rahmen der Geschäftsbeziehung einen elektronischen Kommunikationsweg vereinbart (z. B. das Online-Banking), können die Änderungen auch auf diesem Wege angeboten werden. Der Kunde kann den Änderungen vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens entweder zustimmen oder sie ablehnen. 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 besonders hinweisen.

Werden dem Kunden Änderungen von Bedingungen für Zahlungsdienste (zum Beispiel Überweisungsbedingungen) angeboten, kann er den von der Änderung betroffenen Zahlungsdiensterahmenvertrag vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen auch fristlos und kostenfrei kündigen. Auf dieses Kündigungsrecht wird ihn die Bank in ihrem Angebot besonders hinweisen.