Bedingungen für die Commerzbank Virtual Debit Card[1]

Stand: 19. April 2020

I. Geltungsbereich

1. Verwendungsmöglichkeiten

Die von der Bank ausgegebene Commerzbank Virtual Debit Card (im Folgenden „digitale Karte“ genannt) ist eine Debitkarte, die dem Kunden ausschließlich digital zur Verfügung gestellt wird. Der Karteninhaber erhält keine physische Karte (Plastikarte). Die digitale Karte wird dem Karteninhaber in Form der Nennung der Kartennummer im Online-Banking oder in der Banking App bekannt gemacht.

Die Karte kann digital auf einem oder mehreren digitalen Endgeräten (Telekommunikations-, Digital- oder IT-Geräte) zur Nutzung von digitalen Bezahlverfahren hinterlegt werden.

Der Karteninhaber kann die Karte im Inland und als weitere Dienstleistung auch im Ausland im Rahmen des Mastercard-Verbundes

- zum kontaktlosen Bezahlen an automatisierten Kassen, und
- darüber hinaus als weitere Dienstleistung zur Bargeldauszahlung an Geldautomaten, die eine kontaktlose Nutzung unterstützen (Bargeldservice),

einsetzen.

Die Vertragsunternehmen sowie die Geldautomaten im Rahmen des Bargeldservice sind an dem Mastercard-Akzeptanzsymbol sowie dem Symbol für eine Kontaktloszahlung zu erkennen.

Online-Bezahlvorgänge sind nur innerhalb der Bezahlsysteme von Drittanbietern möglich. Hierzu muss der Karteninhaber die Karte einer digitalen Geldbörse (Wallet) bzw. App eines Drittanbieters (nachfolgend „App-Anwendung“ genannt) hinzufügen. Voraussetzung ist eine gesonderte Vereinbarung zwischen Karteninhaber und Drittanbieter. Die Bezahlung ist dann bei Online-Händlern, die das Bezahlsystem des Drittanbieters zur Bezahlung anbieten, möglich.

Für die Nutzung der Karte auf digitalen Endgeräten gelten ergänzend die gesondert mit der Bank zu vereinbarenden „Bedingungen für die Nutzung von digitalen Karten“.

2. Persönliche Geheimzahl (PIN)

Für die Nutzung von Geldautomaten mit Kontaktlosfunktion kann der Karteninhaber sich eine individuelle persönliche Geheimzahl (PIN) erstellen.

Die Karte kann an kontaktlosen 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 dem Karteninhaberservice, in Verbindung setzen.

II. Allgemeine Regeln

1. Karteninhaber

Die Karte gilt für das bei der Beantragung der Karte vereinbarte Konto. Sie kann nur auf den Namen des Kontoinhabers oder einer Person ausgestellt werden, der der Kontoinhaber Kontovollmacht erteilt hat. Wenn der Kontoinhaber die Kontovollmacht widerruft, ist er dafür verantwortlich, dass die an den Bevollmächtigten ausgegebene Karte gegenüber der Bank gekündigt wird.

2. Finanzielle Nutzungsgrenze

Der Karteninhaber ist verpflichtet die Karte nur innerhalb der finanziellen Nutzungsgrenze gemäß den Allgemeinen Bedingungen für Zahlungsdienste zu nutzen.

3. Umrechnung von Fremdwährungsbeträgen

Nutzt der Karteninhaber die Karte für Verfügungen, die nicht auf Euro lauten, wird das Konto gleichwohl in Euro belastet. Die Umrechnung erfolgt gemäß dem Preis- und Leistungsverzeichnis.

4. Sperre der Karte durch die Bank

Die Bank darf die Karte sperren,

- wenn sie berechtigt ist, den Kartenvertrag aus wichtigem Grund zu kündigen,
- wenn sachliche Gründe im Zusammenhang mit der Sicherheit der Karte dies rechtfertigen oder
- wenn der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der Karte besteht.

Darüber wird die Bank den Karteninhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre über die Sperre unterrichten. Die Angabe von Gründen unterbleibt, soweit sie gegen sonstige Rechtsvorschriften verstößt. Die Bank wird die Karte entsperren oder diese durch eine neue Karte ersetzen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Auch hierüber unterrichtet sie den Karteninhaber unverzüglich.

[1] Entspricht der standardisierten Zahlungskontenterminologie „Ausgabe einer Debitkarte“. Nachfolgend wird die Bezeichnung „Commerzbank Virtual Debit Card“ oder „digitale Karte“ geführt.

120/37/28 – HD0322-01

5. Sorgfalts- und Mitwirkungspflichten des Karteninhabers

a) Geheimhaltung der PIN

Der Karteninhaber hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von seiner persönlichen Geheimzahl (PIN) erlangt. Sie darf insbesondere nicht auf dem digitalen Endgerät vermerkt oder in anderer Weise zusammen mit diesem aufbewahrt werden.

b) Schutz der Authentifizierungselemente für Online-Bezahlvorgänge

Der Karteninhaber hat alle zumutbaren Vorkehrungen zu treffen, um seine mit der Bank vereinbarten Authentifizierungselemente für Online-Bezahlvorgänge (siehe Ziffer 6 dieser Bedingungen) 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:

(1) Wissenselemente, wie z.B. das Passwort oder der Entsperrcode des Endgerätes, sind geheim zu halten; sie dürfen insbesondere
- nicht mündlich (zum Beispiel telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb von Online-Bezahlvorgängen in Textform (z.B. per E-Mail oder Messenger-Dienst) weiter gegeben werden,
- nicht ungesichert elektronisch gespeichert (zum Beispiel Speicherung des Online-Passworts im Klartext im digitalen Endgerät) werden,
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (zum Beispiel digitales Endgerät) oder zur Prüfung des Seinselements (z.B. digitales Endgerät mit Anwendung für Kreditkartenzahlung und Fingerabdrucksensor) dient.

(2) Besitzelemente, wie zum Beispiel ein digitales Endgerät, sind vor Missbrauch zu schützen, insbesondere
- ist sicherzustellen, dass unberechtigte Personen auf das digitale Endgerät des Karteninhabers (zum Beispiel Mobiltelefon) nicht zugreifen können,
- ist dafür Sorge zu tragen, dass andere Personen die auf dem digitalen Endgerät (z.B. Mobiltelefon) befindliche Anwendung für Kreditkartenzahlungen (zum Beispiel Karten-App, Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für Online-Bezahlvorgänge (zum Beispiel Karten-App, Authentifizierungs-App) auf dem digitalen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem digitalen 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 E-Mail, Messenger-Dienst) weiter gegeben werden.

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

c) Kontrollpflichten bei -Bezahlvorgängen

Sollten bei Bezahlvorgängen dem Karteninhaber Angaben zum Zahlungsvorgang (zum Beispiel der Name des Vertragsunternehmens und der Verfügungsbetrag) mitgeteilt werden, sind diese Daten vom Karteninhaber auf Richtigkeit zu prüfen.

d) Unterrichtungs- und Anzeigepflichten des Karteninhabers

(1) Stellt der Karteninhaber den Verlust oder Diebstahl seines digitalen Endgerätes, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von digitaler Karte, PIN oder für Bezahlvorgänge vereinbarter Authentifizierungselemente fest, so ist die Bank, und zwar möglichst unter der dem Karteninhaber mitgeteilten Sperrhotline, unverzüglich zu unterrichten, um eine Sperre zu veranlassen. Die Kontaktdaten, unter denen eine Sperranzeige abgegeben werden kann, werden dem Karteninhaber gesondert mitgeteilt. Der Karteninhaber hat jeden Diebstahl oder Missbrauch auch unverzüglich bei der Polizei anzuzeigen.

(2) Hat der Karteninhaber den Verdacht, dass eine andere Person unberechtigt in den Besitz seines digitalen Endgerätes gelangt, ist eine missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von digitalen Kartendaten, PIN oder für Bezahlvorgänge vereinbarter Authentifizierungselemente vorliegt, muss er ebenfalls unverzüglich eine Sperranzeige abgeben.

(3) Der Karteninhaber hat die Bank unverzüglich nach Feststellung einer nicht autorisierten oder fehlerhaft ausgeführten Kartenverfügung zu unterrichten.

(4) Der Kunde hat die Umsätze der Karte auf ihre Richtigkeit und Vollständigkeit unverzüglich zu überprüfen und etwaige Einwendungen zu erheben.

6. Autorisierung von Kartenzahlungen durch den Karteninhaber

Die Autorisierung einer Kartenzahlung erfolgt durch die Nutzung der folgenden Authentifizierungselemente:
- Wissenselemente (etwas, das der Karteninhaber weiß, zum Beispiel PIN oder Passcode),
- Besitzelemente (etwas, das der Karteninhaber besitzt, zum Beispiel digitales Endgerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN] als Besitznachweis) oder
- Seinselemente (etwas, das der Karteninhaber ist, zum Beispiel Fingerabdruck).

Bei der Bezahlung an kontaktlosen automatisierten Kassen ist das digitale Endgerät (Besitzelement) mit dem gerätespezifischen Entsperrmechanismus (z.B. Geräte-Entsperrcode = Wissenselement oder Fingerabdruckscan/Gesichtsscan = Seinselement) zu entsperren und an die kontaktlose automatisierte Kasse zu halten.

120/37/28 – HD0322-01

Beim Karteneinsatz an unbeaufsichtigten automatisierten Kassen und bei der kontaktlosen Bezahlung von Kleinbeträgen kann vom Einsatz eines Wissens- oder Seinselements abgesehen werden:

- Zur Bezahlung von Verkehrsnutzungsentgelten oder Parkgebühren an unbeaufsichtigten automatisierten Kassen.
- Zur kontaktlosen Bezahlung von Kleinbeträgen. Es gelten die von der Bank festgelegten Betrags- und Nutzungsgrenzen.

Bei der Bargeldauszahlung an Geldautomaten ist das digitale Endgerät (Besitzelement) an den Geldautomaten mit Kontaktlosfunktion zu halten und die PIN (Wissenselement) einzugeben.

Zur Nutzung im Online-Handel über das Bezahlsystem eines Drittanbieters ergeben sich die Regelungen für die Authentifizierung aus den gesondert mit der Bank zu vereinbarenden „Bedingungen für die Nutzung von digitalen Karten".

Nach der Autorisierung der Kartenzahlung kann der Karteninhaber die Kartenzahlung nicht mehr widerrufen. In dieser 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.

7. Sperrung eines verfügbaren Geldbetrags

Die Bank ist berechtigt, auf dem Konto des Kontoinhabers einen im Rahmen der finanziellen Nutzungsgrenze (vgl. II Nummer 2.) verfügbaren Geldbetrag zu sperren, wenn

- der Zahlungsvorgang vom Zahlungsempfänger ausgelöst worden ist und
- der Karteninhaber auch der genauen Höhe des zu sperrenden Geldbetrags zugestimmt hat.[2]

Den gesperrten Geldbetrag gibt die Bank unbeschadet sonstiger gesetzlicher oder vertraglicher Rechte unverzüglich frei, nachdem ihr der genaue Zahlungsbetrag mitgeteilt worden ist.

8. Ablehnung von Kartenzahlungen durch die Bank

Die Bank ist berechtigt, die Kartenzahlung abzulehnen, wenn

- sich der Karteninhaber nicht mit seiner PIN oder seinem sonstigen Authentifizierungselement legitimiert hat,
- der für die Kartenzahlung geltende Verfügungsrahmen oder die finanzielle Nutzungsgrenze nicht eingehalten ist oder
- die Karte gesperrt ist.

Hierüber wird der Karteninhaber über das Terminal, an dem die Karte eingesetzt wird, oder beim Online-Einsatz unterrichtet.

9. Ausführungsfrist

Der Zahlungsvorgang wird vom Zahlungsempfänger ausgelöst. Nach Zugang des Zahlungsauftrages bei der Bank ist diese verpflichtet sicherzustellen, dass der Kartenzahlungsbetrag innerhalb der Ausführungsfrist von einem Geschäftstag beim Zahlungsdienstleister des Zahlungsempfängers eingeht.

Bei Kartenzahlungen innerhalb Deutschlands und in anderen Staaten des Europäischen Wirtschaftsraums (EWR[3]) in Währungen eines Staates außerhalb des EWR (Drittstaatenwährung) sowie Kartenzahlungen, bei denen der Zahlungsdienstleister des Zahlungsempfängers außerhalb des EWR (Drittstaaten) belegen ist, werden Kartenzahlungen baldmöglichst bewirkt. Geht der Zahlungsbetrag beim Zahlungsdienstleister des Zahlungsempfängers erst nach Ablauf der Ausführungsfrist ein (Verspätung), kann der Zahlungsempfänger von seinem Zahlungsdienstleister verlangen, dass dieser die Gutschrift des Zahlungsbetrages auf dem Konto des Zahlungsempfängers so vornimmt, als sei die Kartenzahlung ordnungsgemäß ausgeführt worden.

10. Zahlungsverpflichtung des Kunden

a) Die Bank ist gegenüber Vertragsunternehmen sowie den Kreditinstituten, die die Karte an ihren Geldautomaten akzeptieren, verpflichtet, die vom Karteninhaber mit der Karte getätigten Umsätze zu begleichen.

b) 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.

11. Entgelte und deren Änderung

Für die Erhebung von Entgelten und deren Änderung gelten die Regelungen in den Allgemeinen Bedingungen für Zahlungsdienste. Die einzelnen Entgelte ergeben sich aus dem Preis- und Leistungsverzeichnis.

[2] Z.B. Vorautorisierungen von Mietwagenkautionsleistungen oder in Hotels.

[3] Zum Europäischen Wirtschaftsraum gehören derzeit: Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich (einschließlich Französisch-Guayana, Guadeloupe, Martinique, Mayotte, Réunion), Griechenland, Irland, Island, Italien, Kroatien, Lettland, Liechtenstein, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn sowie Zypern.

12. Haftung des Karteninhabers für nicht autorisierte Kartenverfügungen

a) Haftung des Karteninhabers bis zur Sperranzeige

(1) Wird eine digitale Karte oder die für Online-Bezahlvorgänge vereinbarten Authentifizierungselemente missbräuchlich verwendet und kommt es dadurch zu nicht autorisierten Kartenverfügungen in Form

- der Bargeldauszahlungen oder
- der Verwendung der digitalen Karte zur Bezahlung bei einem Vertragsunternehmen,

so haftet der Karteninhaber für Schäden, die bis zum Zeitpunkt der Sperranzeige verursacht werden, gemäß Absatz 2 nur, wenn er seine Pflichten vorsätzlich oder grob fahrlässig verletzt hat.

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

- er den Verlust oder den Diebstahl der Karte oder die missbräuchliche Verfügung der Bank oder der ihm von der Bank mitgeteilten Sperrhotline schuldhaft nicht unverzüglich mitgeteilt hat, nachdem er hiervon Kenntnis erlangt hat,
- er den Entsperrcode des digitalen Endgeräts auf dem Gerät vermerkt oder zusammen mit dem Gerät verwahrt war,
- die persönliche Geheimzahl oder das vereinbarte Wissenselement für Online-Bezahlvorgänge (z.B. Passwort, Entsperrcode des digitalen Endgerätes) einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde.

(3) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den für die digitale Karte geltenden Verfügungsrahmen.

(4) Der Karteninhaber ist nicht zum Ersatz des Schadens nach den Absätzen (1) und (2) verpflichtet, wenn der Karteninhaber die Sperranzeige nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(5) Abweichend von den Absätzen (1) und (2) ist der Karteninhaber nicht zum Schadensersatz verpflichtet, wenn die Bank vom Karteninhaber eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 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, z.B. PIN oder Passwort), Besitz (etwas, das der Karteninhaber besitzt, z.B. digitales Endgerät) oder Sein (etwas, das der Karteninhaber ist, z.B. Fingerabdruck oder Gesichts-Scan).

(6) Die Absätze (3) bis (5) finden keine Anwendung, wenn der Karteninhaber in betrügerischer Absicht gehandelt hat.

b) Haftung des Karteninhabers ab Sperranzeige

Sobald der Verlust oder Diebstahl des digitalen Endgerätes, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von digitaler Karte, PIN oder für Bezahlvorgänge vereinbarter Authentifizierungselemente gegenüber der Bank oder der ihm von der Bank mitgeteilten Sperrhotline angezeigt wurde, übernimmt die Bank alle danach durch Verfügungen in Form

- der Verwendung der digitalen Karte zur Bezahlung bei einem Vertragsunternehmen entstehenden Schäden
  oder
- der Bargeldauszahlung.

c) Ergänzende Haftungs- und Erstattungsregeln

Soweit die Haftung in den vorgenannten Bestimmungen nicht schon geregelt ist, gelten im Übrigen die in den Allgemeinen Bedingungen für Zahlungsdienste geregelten Haftungs- und Erstattungsregeln des Kunden und die Haftungs- und Einwendungsausschlüsse für die Bank.

Commerzbank AG

120/37/28 – HD0322-01