

Sehr geehrte Kundin, sehr geehrter Kunde,

bevor Sie im Fernabsatz (per Internet, Telefon, E-Mail, Telefax oder Briefverkehr) mit uns Verträge abschließen, möchten wir Ihnen gemäß den gesetzlichen Bestimmungen (§ 312 c BGB i.V.m. der BGB - InfoV) einige allgemeine Informationen zur Bank, zur angebotenen Bankdienstleistung und zum Vertragsabschluss im Fernabsatz geben. Der Kunde gibt gegenüber der Credit Europe Bank N. V., Niederlassung Deutschland ein bindendes Angebot auf Abschluss des Produktvertrages ab, indem er den ausgefüllten und unterschriebenen Produktantrag an die Credit Europe Bank N. V., Niederlassung Deutschland per Post übermittelt und dieser ihr zugeht. Das Antragsformular erhält der Kunde auf seine telefonische, schriftliche oder elektronische Anforderung hin oder er lädt sich das Formular als Datei von der Webseite der Credit Europe Bank N. V., Niederlassung Deutschland herunter und druckt es aus. Der Vertrag kommt zustande, wenn die Bank dem Kunden nach der erfolgten Identitätsprüfung durch Post-Ident Verfahren oder Vermittlerlegitimierung das Konto eröffnet.

Anbieter

Credit Europe Bank N.V.,
Niederlassung Deutschland
Untermainkai 27-28
60329 Frankfurt am Main
Tel.: 0180 / 600 800 1 (20 Cent/Anruf aus dem Festnetz, max. 60 Cent/Anruf aus dem Mobilfunknetz)
Fax: 069-750 877-44 / E-Mail: info@crediteurope.de

Ständiger Vertreter:

Eric G. C. Schröder

Hauptgeschäftstätigkeit der Bank

Gegenstand des Unternehmens ist der Betrieb von Bankgeschäften und von damit zusammenhängenden Geschäften.

Zuständige Aufsichtsbehörde

Die Credit Europe Bank N.V. wurde nach niederländischem Recht gegründet und operiert heute mit einer umfassenden Bankenlizenz unter der generellen Aufsicht der niederländischen Zentralbank, De Nederlandsche Bank, Head Office Postbus 98, 1000 AB Amsterdam, Internet: www.dnb.nl. Die zuständige Aufsichtsbehörde in Deutschland ist die Bundesanstalt für Finanzdienstleistungsaufsicht, Graurheindorfer Straße 108, 53117 Bonn (Bankenaufsicht), Internet: www.bafin.de.

Eintragung im Handelsregister

Amtsgericht Frankfurt am Main HRB 45588

Umsatzsteueridentifikationsnummer

DE 195 743 101

Vertragsprache

Maßgebliche Sprache für dieses Vertragsverhältnis und die Kommunikation mit dem Kunden während der Laufzeit des Vertrages ist Deutsch.

Rechtsordnung/Gerichtsstand

Gemäß Nr. 6 Abs. 1 der „Allgemeinen Geschäftsbedingungen“ gilt für den Vertragsschluss und die gesamte Geschäftsverbindung zwischen dem Kunden und der Bank deutsches Recht. Es gibt keine vertragliche Gerichtsstandsklausel.

Außergerichtliche Streitschlichtung

Für die Beilegung von Streitigkeiten mit der Bank besteht die Möglichkeit, den Ombudsmann der privaten Banken anzurufen. Näheres regelt die „Verfahrensordnung für die Schlichtung von Kundenbeschwerden im deutschen Bankgewerbe“, die auf Wunsch zur Verfügung gestellt wird. Die Beschwerde ist schriftlich an die Kundenbeschwerdestelle beim Bundesverband deutscher Banken e. V., Postfach 04 03 07, 10062 Berlin, zu richten.

Einlagensicherungsfonds

Die Credit Europe Bank N.V., Niederlassung Deutschland, steht unter der Aufsicht der niederländischen Zentralbank (DNB) und ist dem niederländischen Einlagensicherungsfonds (Depositogarantiestelsel) für Banken in den Niederlanden angeschlossen. Für mehr Details über das niederländische Einlagensicherungssystem wird auf die Webseite der niederländischen Zentralbank verwiesen (<http://www.dnb.nl>).

Preise

Die aktuellen Bankentgelte für die Dienstleistungen der Bank ergeben sich aus beiliegendem „Preiseshang“. Die Änderung von Zinsen und Entgelten während des Vertragsverhältnisses erfolgt nach Maßgabe von Nr. 12 der „Allgemeinen Geschäftsbedingungen“. Das jeweils gültige „Preis- und Leistungsverzeichnis“ kann der Kunde im Internet unter www.crediteurope.de einsehen. Auf Wunsch wird die Bank ihm diese zusenden.

Hinweis auf vom Kunden zu zahlende Steuern

Soweit im Rahmen der Kontoführung Guthabenzinsen anfallen, sind diese Einkünfte steuerpflichtig. Bei Fragen sollte sich der Kunde an die für ihn zuständige Steuerbehörde bzw. seinen steuerlichen Berater wenden. Dies gilt insbesondere, wenn er im Ausland steuerpflichtig ist.

Zusätzliche Telekommunikationskosten

Für die Nutzung des Telefonbankings unter der Telefonnummer 0180-600 800 1 entstehen dem Kunden pro angefangener Minute für Inlandsgespräche aus dem Festnetz der Deutschen Telekom zusätzliche Kosten in Höhe von 20 Cent/Anruf, max. 60 Cent/Anruf aus dem Mobilfunknetz. Eigene Kosten (z.B. für Ferngespräche, Porti) hat der Kunde selbst zu tragen.

Leistungsvorbehalt

Bei Fremdwährungskonten gilt der in Nr. 10 Abs. 3 der beigefügten „Allgemeinen Geschäftsbedingungen“ genannte Vorbehalt.

Zahlung und Erfüllung

Einzelheiten zur Zahlung und Erfüllung entnehmen Sie bitte den „Allgemeinen Geschäftsbedingungen“ und den jeweiligen „Produkt- bzw. Sonderbedingungen“.

Vertragliche Kündigungsregeln

Es gelten die in Nr. 18 und 19 der „Allgemeinen Geschäftsbedingungen“ für den Kunden und die Bank festgelegten Kündigungsregeln einschließlich etwaiger Vertragsstrafen.

Mindestlaufzeit des Vertrages

Die Mindestlaufzeiten für Verträge entnehmen Sie bitte den jeweiligen Produktbedingungen.

(Stand: Ende September 2013. Diese Informationen gelten bis auf Weiteres.)

Credit Europe Bank N.V. – Niederlassung Deutschland
Postfach 11 15 51 – 60050 Frankfurt am Main
Telefon: 0180 / 600 800 1 (20 Cent/Anruf aus dem Festnetz,
Fax: 069/750 877-44 max. 60 Cent/Anruf aus dem Mobilfunknetz)

1. Leistungsangebot

- (1) Das Direct Banking umfasst Online Banking, Telefonbanking und die Abwicklung von Geschäftsvorgängen per Fax und Brief.
- (2) Der Kontoinhaber kann Bankgeschäfte mittels Direct Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Direct Banking abrufen.
- (3) Kontoinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet.
- (4) Zur Nutzung des Direct Banking gelten die mit der Bank gesondert vereinbarten Verfügungs-limite.
- (5) Die nachfolgenden Ziffern 2 – 11 gelten sofern die darin aufgeführten Serviceleistungen von der Bank aktuell angeboten werden.

2. Voraussetzungen zur Nutzung des Online-Banking und Telefonbanking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels Online-Banking und Telefonbanking die Kundennummer und die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4).

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN),
- der Nutzungscode für die elektronische Signatur.

2.2 Authentifizierungsinstrumente

Die TAN beziehungsweise die elektronische Signatur können dem Teilnehmer auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:

- auf einer Liste mit einmal verwendbaren TAN oder
- mittels eines mobilen Endgerätes (zum Beispiel Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
- auf einem sonstigen Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden.

3. Zugang zum Online-Banking und Telefonbanking

Der Teilnehmer erhält Zugang zum Online-Banking und Telefonbanking, wenn

- dieser die Kundennummer oder seine individuelle Kundenkennung und seine PIN oder elektronische Signatur übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperrung des Zugangs (siehe Nummern 10.1 und 11) vorliegt.

Nach Gewährung des Zugangs zum Online-Banking und Telefonbanking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

4. Online-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Online-Banking-Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (siehe unter Punkt 2.1) autorisieren und der Bank mittels Online-Banking übermitteln. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Online-Banking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Online-Banking ausdrücklich vor.

5. Bearbeitung von Telefonbanking-Aufträgen

5.1 Aufzeichnung von Telefongesprächen und mittels Telefonbanking erteilten Aufträgen

5.1.1 Die Bank zeichnet alle im Telefonbanking erteilten Aufträge zu Beweis Zwecken und auch aus Sicherheitsgründen auf. Die im Direct Banking erteilten Aufträge werden unter Beachtung der datenschutzrechtlichen Vorschriften aufgezeichnet, aufbewahrt und genutzt.

5.1.2 Mit der Aufzeichnung soll sichergestellt werden, dass eventuelle Zweifel über den Inhalt eines Auftrages sowie die Person des Auftraggebers geklärt werden können.

5.1.3 Der Teilnehmer stimmt weiterhin dem Mithören und Aufzeichnen von Telefongesprächen durch befugte Personen zu internen Trainings- und Beurteilungszwecken mit anschließender Auswertung zu.

5.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Telefonbanking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen.

6. Bearbeitung von Direct-Banking-Aufträgen durch die Bank

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

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

- der Teilnehmer hat sich mit seinem personalisierten Sicherheitsmerkmal legitimiert;
- die Berechtigung des Teilnehmers liegt vor;
- das Online-Banking-Datenformat ist eingehalten;
- das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten;
- die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor. Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Direct-Banking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen aus.

- (3) Legitimationsprüfung

Die Bank haftet nicht, sofern Fälschungen oder Manipulationen des telefonisch oder per Fax erteilten Auftrages für sie nicht erkennbar waren. Ergibt die Legitimation Unstimmigkeiten, wird die Bank den betreffenden Auftrag nicht bearbeiten und dem Teilnehmer hierüber unverzüglich eine Information mittels Direct Banking zur Verfügung stellen.

- (4) Das Ausbleiben einer Ausführungsanzeige im System des Onlinebankings ist der Bank unverzüglich anzuzeigen.

– Sofern eine manuelle Nachbearbeitung der Aufträge notwendig ist, übernimmt die Bank keine Zusage für den Zeitpunkt der Ausführung.

– Jeder telefonisch erteilte Auftrag wird dem Teilnehmer gegenüber vollständig mit den wesentlichen Angaben wiederholt. Die Ausführung des erteilten Auftrags erfolgt erst nach nochmaliger Bestätigung durch den Teilnehmer.

– Soweit die Bank dem Teilnehmer weitergehende Informationen über Aufträge zur Verfügung stellt, die noch nicht endgültig bearbeitet sind, geschieht dies für die Bank unverbindlich.

- (5) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Direct-Banking-Auftrag nicht ausführen und dem Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Direct-Banking eine Information zur Verfügung stellen.

7. Information des Kontoinhabers über Direct-Banking-Verfügungen

Die Bank unterrichtet den Kontoinhaber bei Transaktionen auf dem Sparkonto regelmäßig monatlich über ein reproduzierbares und speicherbares Dokument oder einen Datenträger. Die Information über die getätigten Verfügungen kann innerhalb des Online-Banking und auf den vereinbarten Kommunikationswegen übermittelt werden. Zusätzlich versendet die Bank an Top-

Interess Kontoinhaber vierteljährlich Kontoauszüge per Briefpost, auf deren Konten Umsätze stattgefunden haben. Für Inhaber des Credit Europe Online Tagesgeldkontos auf deren Konten Umsätze stattgefunden haben, werden die Kontoauszüge nicht in Druckform, sondern vierteljährlich, digitalisiert in das elektronische Postfach zugestellt.

8. Sorgfaltspflichten des Teilnehmers

8.1 Technische Verbindung zum Online-Banking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online-Banking nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle (zum Beispiel Internetadresse) herzustellen.

8.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

- (1) Der Teilnehmer hat
- seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln sowie
 - sein Authentifizierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstrumentes ist, kann das Telefonbanking- und Online-Banking-Verfahren missbräuchlich nutzen.

- (2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstrumentes zu beachten:
- Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (zum Beispiel im Kundensystem).
 - Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
 - Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (zum Beispiel nicht auf Online-Händlerseiten).
 - Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail und auch nicht gegenüber dritten Personen.
 - Die PIN und der Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
 - Der Teilnehmer darf zur Autorisierung zum Beispiel eines Auftrags, der Aufhebung einer Sperrung oder zur Freischaltung einer neuen TAN-Liste nicht mehr als eine TAN verwenden.
 - Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (zum

Beispiel Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.

8.3 Sicherheit des Kundensystems

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

8.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem Online-Banking-Auftrag (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers) im Kundensystem oder über ein anderes Gerät des Teilnehmers zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

9. Anzeige- und Unterrichtungspflichten

9.1 Sperranzeige

- (1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl des Authentifizierungsinstrumentes oder Personalisierten Sicherheitsmerkmals, die missbräuchliche Verwendung oder
 - die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstrumentes oder seines Persönlichen Sicherheitsmerkmals fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.
- (2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen.
- (3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt
- den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder
 - das Authentifizierungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet, muss er ebenfalls eine Sperranzeige abgeben.

9.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

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

10. Nutzungssperre

10.1 Sperrung auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 9.1

- den Telefonbanking- und Online-Banking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument oder sein

Personalisiertes Sicherheitsmerkmal.

10.2 Sperrung auf Veranlassung der Bank

- (1) Die Bank darf den Telefonbanking- und Online-Banking-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, den Telefonbanking- und Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
 - sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstrumentes oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
 - der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstrumentes besteht.
- (2) Die Bank wird den Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperrung unterrichten.

10.3 Aufhebung der Sperrung

Die Aufhebung der Sperrung kann der Kontoinhaber nur durch eine schriftliche Mitteilung (und nicht per Fax) an die Bank veranlassen. Die Bank wird eine Sperrung aufheben oder das Personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperrung nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber unverzüglich.

11. Haftung

11.1 Haftung der Bank bei einer nicht autorisierten Direct-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Direct-Banking-Verfügung

Die Haftung der Bank bei einer nicht autorisierten Direct-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Direct-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr).

11.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstrumentes

11.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

- (1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines abhanden gekommenen, oder gestohlenen Personalisierten Sicherheitsmerkmals oder Authentifizierungsinstrumentes, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,- Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigen Abhandenkommen des Personalisierten Sicherheitsmerkmals oder Authentifizierungsinstrumentes ein Verschulden trifft.
- (2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstrumentes oder Personalisierten Sicherheitsmerkmals, ohne dass

dieses gestohlen oder abhanden gekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,- Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der Personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

- (3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150,- Euro nach Absatz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- (4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 9.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.
- (5) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er
 - den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 9.1 Absatz 1),
 - das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 8.2 Absatz 2.1. Spiegelstrich),
 - das Personalisierte Sicherheitsmerkmal

einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 8.2 Absatz 1 2. Spiegelstrich),

- das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 8.2 Absatz 2 3. Spiegelstrich),
 - das Personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 8.2 Absatz 2 4. Spiegelstrich),
 - das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 8.2 Absatz 2 5. Spiegelstrich),
 - mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 8.2 Absatz 2 6. Spiegelstrich),
 - beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Online-Banking nutzt (siehe Nummer 8.2 Absatz 2 7. Spiegelstrich).
- (6) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.
- 11.2.2 Haftung der Bank ab der Sperranzeige**
Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Direct-Banking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.
- 11.2.3 Haftung der Bank bei Störung des Betriebes**
(1) Können Credit Europe Bank Kommunikationswege vorübergehend nicht benutzt werden, so haftet die Bank nur für ihr grobes Verschulden. Kann das Direct Banking auf-

grund technischer oder sonstiger Störungen vorübergehend nicht durchgeführt werden, haftet die Bank nur im Fall eines von ihr zu vertretenden Verschuldens und nur in dem Maße, in dem sie im Verhältnis zu anderen Ursachen an der Entstehung des Schadens mitgewirkt hat. Der Teilnehmer ist verpflichtet, Störungen bei der Übertragung von Daten der Bank unverzüglich mitzuteilen.

- (2) Für systembedingte Ausfälle, Unterbrechungen und Störungen des Telefonnetzes, des Internet und anderer Kommunikationssysteme der Netzbetreiber oder Tele-Dienstanbieter oder Online-Dienstanbieter haftet die Bank nur im Falle grober Fahrlässigkeit und nur in dem Maße, in dem sie im Verhältnis zu anderen Ursachen an der Entstehung des Schadens mitgewirkt hat.
- (3) Eine Überprüfung eingehender Faxe auf Echtheit ist der Bank nicht möglich. Die Bank führt daher die Aufträge auf Risiko des Kontoinhabers aus, wenn die Unterschriften und die äußeren Gegebenheiten des Auftrages im Gesamterscheinungsbild den Eindruck erwecken, vom Teilnehmer zu stammen.

11.2.4 Haftungsausschluss

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

Stand 12.04.2016 Bis auf Weiteres gültig