Miles & More

Bedingungen für den Zugang zur Deutsche Bank AG (nachstehend Bank) über elektronische Medien zur Nutzung der Lufthansa Miles & More Credit Card (Kreditkarte)

Stand 03/25

Die nachfolgenden Bedingungen gelten für die Lufthansa Miles & More Credit Card (Kreditkarte), her-ausgegeben von der Deutsche Bank AG (nachfolgend „Bank" genannt), soweit der Kunde das Miles & More Kreditkarten-Banking oder Telefon-Banking der Bank nutzt. Sie sind in Verbindung mit den Bedingungen für die Lufthansa Miles & More Credit Card (Kreditkarte), herausgegeben von der Deutsche Bank AG zu lesen. Für die Nutzung des Deutsche Bank Online-Banking oder Telefon-Banking durch den Kunden gelten die dazu mit dem Kunden vereinbarten Bedingungen.

1. Leistungsangebot

(1) Der Kunde und dessen Bevollmächtigte können ausgewählte Bankgeschäfte mittels elektronischer Zugangsmedien für die Miles & More Kreditkarte, im Einzelnen Kreditkarten-Banking und Telefon-Banking (jeweils einzeln „Kreditkarten-Banking" bzw. „Telefon-Banking" sowie gemeinsam „Zugangsmedien" bzw. „elektronische Medien"), in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank zur Nutzung der Miles & More Kreditkarte mittels Kreditkarten- und Telefon-Banking abrufen.

(2) Das 3D Secure-Verfahren (bei Mastercard als „Identity Check" bezeichnet) ist ein Verfahren zur Authentifizierung des Kreditkarteninhabers bei Online-Transaktionen.

(3) Die Bank ist berechtigt, einen Kreditkartenumsatz im Internet abzulehnen, den der Kreditkarteninhaber bei einem Unternehmen, das den Einsatz des 3D Secure-Verfahrens für diese Transaktion vorsieht, ohne dessen Nutzung tätigen will.

(4) Kunde und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer" bezeichnet.

(5) Für die Nutzung der Zugangsmedien gelten die mit der Bank gesondert vereinbarten Verfügungslimite.

2. Voraussetzungen zur Nutzung der elektronischen Medien

(1) Der Teilnehmer kann ausgewählte Bankgeschäfte über elektronische Medien abwickeln, wenn die Bank ihn authentifiziert hat.

(2) Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers und die berechtigte Verwendung der Miles & More Kreditkarte, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).

(3) Authentifizierungselemente sind:

- Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. die persönliche Identifikationsnummer (PIN) oder das persönliche Passwort),
- Besitzelemente, also etwas, was nur der Teilnehmer besitzt (z. B. das mobile Endgerät), oder
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

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

(5) Je nach Authentifizierungsverfahren und -instrument benötigt der Teilnehmer hierfür gegebenenfalls geeignete Hard- und Software. Über das Angebot der bankeigenen Anwendungen hinaus bleibt der Teilnehmer selbst für die Beschaffung, Installation und Pflege dieser Hard- und Software verantwortlich.

(6) Bei der Nutzung einer Hard- bzw. Software von Drittanbietern durch den Teilnehmer übernimmt die Bank keine eigene Gewährleistung oder sonstige Verantwortung für eine andauernde Eignung oder Verfügbarkeit im Zusammenhang mit einem Authentifizierungsverfahren.

3. Zugang über elektronische Medien

(1) Der Teilnehmer erhält Zugang zum Kreditkarten- und Telefon-Banking der Bank, wenn:

- dieser seine individuelle Servicekartennummer (Telefon-Banking) bzw. seinen Benutzernamen (Kreditkarten-Bankinkg) angibt und
- er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs vorliegt.

Nach Gewährung des Zugangs zum Kreditkarten- und Telefon-Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge erteilt werden.

(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z. B. zum Zweck der Änderung der Anschrift des Kunden) fordert die Bank den Teilnehmer auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Kreditkarten-Banking nur ein Authentifizierungselement angefordert wurde.

4. Aufträge

4.1 Auftragserteilung

(1) Der Teilnehmer muss einem Auftrag (z. B. Zahlungsauftrag im Rahmen des Guthabenauszahlungsservice und des Überweisungsservice) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungsmerkmale (z. B. Eingabe einer TAN oder Übertragung einer elektronischen Signatur als Nachweis des Besitzelements (BestSign)) zu verwenden. Die Bank bestätigt mittels Kreditkarten-Banking den Eingang des Auftrags.

(2) Der Teilnehmer kann Telefon-Banking-Aufträge nur nach erfolgreicher Autorisierung mit dem von ihm im Rahmen der Kartenbeantragung vergebenen Sicherheitsmerkmal erteilen. Die Bank bestätigt den Eingang des Auftrags auf dem vom Teilnehmer für den Auftrag gewählten Zugangsweg. Die zwischen der Bank und dem Kreditkarteninhaber übermittelte Telefonkommunikation wird zu Beweiszwecken automatisch aufgezeichnet und gespeichert.

4.2 Widerruf von Aufträgen

(1) Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für die Nutzung des Guthabenauszahlungsservice und des Überweisungsservice (Lufthansa Miles & More Credit Card (Kreditkarte))). Der Widerruf von Aufträgen kann nur außerhalb des Kreditkarten- und Telefon-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Kreditkarten- und Telefon-Banking ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) im Preis- und Leistungsverzeichnis für die Lufthansa Miles & More Credit Card (Kreditkarte) (nachfolgend „Preis- und Leistungsverzeichnis“) bekannt gegebenen Geschäftsta-gen im Rahmen des ordnungsgemäßen Arbeitsablaufs. Geht der Auftrag nach dem im Kreditkarten-Banking der Bank angegebenen oder im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß dem „Preis- und Leistungsverzeichnis der Lufthansa Miles & More Credit Card (Kreditkarte)“, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

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

- Der Teilnehmer hat den Auftrag autorisiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor.
- Das gesondert vereinbarte Verfügungslimit der Karte ist nicht überschritten.
- Im Telefon-Banking wird die Bank Verfügungen über das Kartenkonto, die eine Zahlung an einen Dritten (abweichende Kontonummer) enthalten, bis zu einem Betrag von insgesamt unter 50.000 Euro pro Tag ausführen, sofern nicht ein anderer Verfügungshöchstbetrag mit dem Teilnehmer vereinbart ist.
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichendes Verfügungslimit der Karte) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für die Nutzung des Guthabenauszahlungsservice und des Überweisungsservice (Lufthansa Miles & More Credit Card (Kreditkarte))) aus.

(3) Liegen die Ausführungsbedingungen nach Nummer 5.2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen und den 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 Kreditkarten- bzw. Telefon-Banking oder postalisch informieren.

6. Information des Kunden über Kreditkarten- und Telefon-Banking-Verfügungen

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

7. Sorgfaltspflichten des Teilnehmers

7.1 Schutz der Authentifizierungsinstrumente

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

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

(a) Wissenselemente, wie z. B. die PIN, sind geheim zu halten. Sie dürfen insbesondere

- nicht außerhalb des Kreditkarten-Banking mündlich, z. B. per Telefon, oder in Textform, z. B. per E-Mail, weitergegeben werden,
- nicht ungesichert außerhalb des zugelassenen Authentifizierungsverfahrens elektronisch gespeichert werden, z. B. PIN im Klartext im Computer oder im mobilen Endgerät , und
- nicht auf einem Gerät notiert sein oder als Abschrift zusammen mit einem Gerät, das als Besitzelement oder zur Prüfung des Seinselements mit Anwendung für das Kreditkarten-Bankings dient, aufbewahrt werden.

(b) Besitzelemente, wie z. B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers, z. B. Mobiltelefon (und insbesondere auf die Miles & More App), nicht zugreifen können,
- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät befindliche Anwendung für das Kreditkarten-Banking nicht nutzen können,
- ist die Anwendung für das Kreditkarten-Banking (die Miles & More App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer 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 Kreditkarten-Bankings mündlich oder in Textform weitergegeben werden und

— muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements erhalten hat, diesen vor unbefugtem Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ein Gerät als Besitzelement für das Kreditkarten-Banking des Teilnehmers aktivieren.

(c) Seinselemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Kreditkarten-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 Kreditkarten-Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Kreditkarten-Banking das von der Bank ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Beim mobileTAN-Verfahren darf das mobile Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht gleichzeitig für das Kreditkarten-Banking genutzt werden.

(4) Die für das mobileTAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Kreditkarten-Banking nicht mehr nutzt.

(5) Der Aufforderung per elektronischer Nachricht (z. B. E-Mail), eine damit übersandte Verknüpfung zum (vermeintlichen) Kreditkarten-Banking der Bank anzuwählen und darüber persönliche Zugangsdaten einzugeben, darf nicht gefolgt werden.

(6) Anfragen außerhalb der bankseitig zur Verfügung gestellten originären Zugangswege, in denen nach vertraulichen Daten wie PIN, Geheimzahl oder Passwort/TAN gefragt wird, dürfen nicht beantwortet werden.

(7) Der Teilnehmer hat vor seinem jeweiligen Zugang zum Kreditkarten-Banking sicherzustellen, dass auf dem verwendeten System handelsübliche Sicherheitsvorkehrungen wie Anti-Viren-Programm und Firewall installiert sind und diese ebenso wie die verwendete System- und Anwendungssoftware regelmäßig aktualisiert werden. Beispiele handelsüblicher Sicherheitsvorkehrungen kann der Teilnehmer den Internetseiten der Bank entnehmen.

(8) Die Softwareanwendungen der Bank sind ausschließlich direkt von der Bank oder von einem von der Bank benannten Anbieter zu beziehen.

7.2 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise auf der Internetseite der Bank, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten. Darüber hinaus hat der Kunde in eigener Verantwortung etwaige Sicherheitshinweise der Anbieter der eingesetzten Kundensysteme zu beachten (z. B. Sicherheits-Updates von Systemsoftware mobiler Endgeräte).

7.3 Prüfung durch Abgleich der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Daten (z. B. Betrag, Kontonummer des Zahlungsempfängers) über das gesondert vereinbarte Gerät des Teilnehmers an (z. B. mittels mobilem Endgerät). Der Teilnehmer ist verpflichtet, vor der Autorisierung (z. B. Eingabe der TAN) die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen. Stimmen die angezeigten Daten nicht überein, ist der Vorgang abzubrechen und die Bank unverzüglich zu informieren.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer

— den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. mobiles Endgerät) oder

— die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungselements

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

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

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

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

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

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

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

— den vom Teilnehmer bezeichneten Banking-Zugang für ihn oder alle Teilnehmer oder

— seine Authentifizierungselemente zur Nutzung des Kreditkarten-Banking.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Kreditkarten- und Telefon-Banking-Zugang für einen Teilnehmer sperren oder ein Authentifizierungselement nicht mehr zulassen, wenn

— sie berechtigt ist, den Kreditkarten- und Telefon-Banking-Vertrag aus wichtigem Grund zu kündigen,

— sachliche Gründe im Zusammenhang mit der Sicherheit seiner Authentifizierungselemente dies rechtfertigen,

— der Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines Authentifizierungselements besteht oder

— ein genutzter Zugangsweg bzw. ein im Zusammenhang mit einem Authentifizierungsverfahren zugelassenes Gerät von der Bank als unsicher eingestuft wird. Als Zugangsweg gelten auch Softwareanwendungen der Bank in allen zur Verfügung stehenden Versionen.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre postalisch, telefonisch oder online unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich. Der Teilnehmer kann eine von ihm veranlasste Sperrung nur postalisch oder mit telefonisch legitimiertem Auftrag aufheben lassen.

10. Vereinbarung eines elektronischen Kommunikationswegs

(1) Der Kunde und die Bank vereinbaren, dass die Bank mit dem Nutzer elektronisch kommunizieren kann, d. h. per E-Mail über die durch den Nutzer angegebene E-Mail-Adresse.

(2) Der Kunde ist damit einverstanden, entsprechende Mitteilungen unverschlüsselt per E-Mail zu erhalten. Insbesondere ist die Bank berechtigt, dem Kunden Änderungen ihrer Allgemeinen Geschäftsbedingungen und der besonderen Bedingungen für einzelne Geschäftsbeziehungen auf diesem Weg zu übermitteln. Personenbezogene Daten werden auf diesem Weg nicht übertragen.

11. Haftung

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

Die Haftung der Bank bei einer nicht autorisierten Kreditkarten- und Telefon-Banking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Kreditkarten-/Telefon-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für die Nutzung des Guthabenauszahlungsservice und des Überweisungsservice (Lufthansa Miles & More Credit Card (Kreditkarte)).

11.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

11.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

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

— es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung zu bemerken, oder

— der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach

— Nummer 7.1 Absatz 2

— Nummer 7.1 Absatz 3

— Nummer 7.3 oder

— Nummer 8.1 Absatz 1

dieser Bedingungen verletzt hat.

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

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

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

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

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

— Der Kunde haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

— Die Haftungsbeschränkung in Absatz 2, 1. Punkt findet keine Anwendung.

11.2.2 Haftung bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten vor der Sperranzeige

Beruhen nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten vor der Sperranzeige auf der Nutzung eines verloren gegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung

eines Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

11.2.3 Haftung der Bank ab der Sperranzeige

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

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.