Sonderbedingungen und Verfahrenshinweise für die gesicherte Authentifizierung bei Kreditkartenzahlungen im Internet

1. Verified by Visa / Mastercard SecureCode™

1.1. Nach Ziffer 4.3 der „Vertragsbedingungen für Kreditkarten" bzw. Ziffer 3.3 der „Einsatzbedingungen von Firmenkreditkarten" oder Ziffer 4.3 der „Kartenbedingungen der Visa/Mastercard BusinessCard", ist der Karteninhaber verpflichtet (Sorgfaltspflicht), zur Vermeidung von Missbräuchen gesicherte Authentifizierungsverfahren bei Internet-Zahlungen einzusetzen, sofern ein solches Verfahren von der Bank und der Kartenakzeptanzstelle angeboten wird.

1.2. **Verified by Visa** bzw. **Mastercard SecureCode™** sind solche Verfahren zur gesicherten Authentifizierung, die dazu dienen sicherzustellen, dass eine Internet-Zahlung bei einer Kartenakzeptanzstelle, die an diesem Verfahren teilnimmt, auch tatsächlich vom Karteninhaber veranlasst wurde und die Karte nicht zu Unrecht belastet wird. Hierzu bestätigt der Karteninhaber beim Bezahlvorgang gegenüber einem Dienstleister der Bank mittels Eingabe einer auf den Einzelumsatz bezogenen Transaktionsnummer (TAN) oder durch Freigabe in einer durch die Bank bereitgestellten App, dass er die Zahlung beauftragt. Die TAN wird dann an ein zum SMS-Empfang geeignetes Endgerät (z.B. Mobiltelefon) oder an eine auf dem Endgerät des Karteninhabers installierte, durch die Bank bereitgestellte App, übermittelt.

1.3. Diese Sonderbedingungen gelten ergänzend zu den „Vertragsbedingungen für Kreditkarten", bzw. den „Einsatzbedingungen von Firmenkreditkarten" bzw. den „Kartenbedingungen der Visa/Mastercard BusinessCard". Im Falle eines Widerspruchs zwischen den „Vertragsbedingungen für Kreditkarten", bzw. den „Einsatzbedingungen von Firmenkreditkarten" bzw. den „Kartenbedingungen der Visa/Mastercard BusinessCard" gehen diese den Sonderbedingungen vor.

2. Registrierung

2.1. Erforderliche Daten und technische Anforderungen

Um sich zur Teilnahme an diesen Authentifizierungsverfahren zu registrieren, benötigt der Karteninhaber

- seine Kreditkartennummer,
- ggf. weitere persönliche Daten, die während der Registrierung abgefragt werden und
- ein Endgerät (z.B. Mobiltelefon) mit der Möglichkeit des SMS-Empfangs (nachfolgend „Mobiltelefon" genannt) („SMS-Verfahren") oder
- ein anderes unterstütztes Endgerät (z.B. Smartphone / Tablet) mit der Möglichkeit der Nutzung der durch die Bank bereitgestellten App („App-Verfahren").

Die Bank behält sich das Recht vor, nicht beide vorgenannten Verfahren anzubieten oder sie durch ein anderes oder mehrere andere Verfahren zu ersetzen. Die Registrierung ist auf der Internetseite der Bank möglich. Optional kann die Registrierung während eines Bezahlvorgangs bei einem teilnehmenden Internethändler durch die Bank initiiert werden.

2.2. Registrierungsprozess für das SMS-Verfahren

Hierbei legt der Karteninhaber die Rufnummer seines Mobiltelefons fest, an das künftig die zur Zahlungsfreigabe erforderlichen TANs übermittelt werden sollen. Zur Registrierung für das Verfahren wird dem Karteninhaber postalisch ein Aktivierungscode an seine hinterlegte Anschrift übermittelt. Diesen Aktivierungscode muss der Karteninhaber zur Festlegung seiner Mobilfunknummer sowie der Antwort auf eine auszuwählende Sicherheitsfrage auf der Internetseite der Bank einmalig eingeben. Danach ist das SMS-Verfahren für die Nutzung zur gesicherten Authentifizierung freigeschaltet.

2.3. Registrierungsprozess für das App-Verfahren

Das App-Verfahren setzt voraus, dass der Karteninhaber die von der Bank bereitgestellte App auf seinem Endgerät installiert und mit seiner Kreditkarte per Aktivierungscode verknüpft. Die bei erstmaliger Nutzung der App erzeugte Kennung (die „virtuelle Handynummer"), ist bei der Registrierung anzugeben. Zur Registrierung für das Verfahren wird dem Karteninhaber postalisch ein Aktivierungscode an seine hinterlegte Anschrift übermittelt. Diesen Aktivierungscode muss der Karteninhaber zur Bestätigung der angegebenen virtuellen Handynummer auf der Internetseite der Bank einmalig eingeben. Danach ist das App-Verfahren für die Nutzung zur gesicherten Authentifizierung freigeschaltet und der Karteninhaber hat die Möglichkeit, mittels der von seiner Bank bereitgestellten App die TANs zu empfangen oder innerhalb der App freizugeben.

2.4. Weitere Informationen

Die Bank wird den Karteninhaber niemals per E-Mail oder Anruf zur Registrierung oder Bekanntgabe seiner Registrierungsdaten auffordern.

Der Ablauf der Registrierung und die Bezugsquellen der Anwendung sind in der Information „Mehr Sicherheit beim Online-Shopping" beschrieben, die dem Karteninhaber bereitgestellt wird und bei der Bank erhältlich ist.

3. Gesicherte Authentifizierung einer Verified by Visa- bzw. Mastercard SecureCode-Zahlung

3.1. SMS-Verfahren:
Sobald eine Verified by Visa / Mastercard SecureCode™ Transaktion veranlasst wird, erhält der Karteninhaber eine SMS Benachrichtigung mit Transaktionsdetails und pro Transaktion generierter TAN auf sein Endgerät zugestellt. Durch Eingabe der erhaltenen TAN und korrekter Beantwortung der Sicherheitsfrage im Kaufprozess wird die Transaktion bestätigt.

3.2. App-Verfahren:
Beim App-Verfahren handelt es sich um ein Authentifikationsverfahren, bei welchem eine pro Verified by Visa / Mastercard SecureCode™ Transaktion generierte TAN via Internet direkt an eine besonders geschützte App auf das Smartphone des Karteninhabers übermittelt wird. Sobald eine Verified by Visa / Mastercard SecureCode™ veranlasst wird, erhält der Karteninhaber auf seinem Endgerät eine Benachrichtigung. Nach Eingabe des App-Kennworts öffnet sich die App und die Transaktionsdetails sowie die pro Transaktion generierte TAN werden angezeigt. Durch Eingabe der erhaltenen TAN im Kaufprozess wird die Transaktion bestätigt.

3.3. Die Nutzung der gesicherten Authentifizierung für Internet-Zahlungen kann für bestimmte Transaktionen zur Risikoprävention eingeschränkt sein.

4. Sorgfaltsanforderungen an den Karteninhaber

4.1. Der Karteninhaber hat dafür Sorge zu tragen, dass kein Dritter zur Durchführung von Internet-Zahlungen Zugang zu seinem für das Verfahren genutzten Endgerät erlangt.

4.2. Das Endgerät, mit dem die TANs empfangen werden, darf nicht gleichzeitig für die Internet-Zahlungen genutzt werden (physische Trennung der Kommunikationskanäle).

4.3. Der Karteninhaber hat die Übereinstimmung der von der Bank dem Nutzer übermittelten Transaktionsdaten mit den von ihm für die Transaktion vorgesehenen Daten abzugleichen. Bei Unstimmigkeiten ist die Transaktion abzubrechen und die Bank zu informieren.

4.4. Der Karteninhaber hat die App nur aus offiziellen App-Stores (Apple Appstore oder Google Playstore) herunterzuladen und die für die App vorgesehenen Updates regelmäßig zu installieren.

5. Änderung der Mobilfunknummer / virtuellen Handynummer

5.1. Sollte der Karteninhaber seine für das Verfahren genutzte Kennung (Sicherheitsfrage und/oder Mobilfunknummer für SMS-Empfang bzw. virtuelle Handynummer für App-Nutzung) ändern wollen, steht ihm auf der Registrierungswebseite seiner Bank eine Funktion zur Verfügung, um seine für das TAN-Verfahren verwendete Kennung zu ändern.

5.2. Ist kein TAN-Versand an die bisher registrierte Kennung möglich (z.B. das Endgerät mit der hinterlegten Kennung wurde gestohlen), muss der Karteninhaber den Registrierungsprozess erneut durchlaufen.

6. Abmeldung vom Verfahren

6.1. Der Karteninhaber kann sich von der Teilnahme am Verfahren zur gesicherten Authentifizierung abmelden, in dem er auf der Registrierungswebseite seiner Bank den Button "Benutzerkonto löschen" betätigt.

6.2. Wenn sich der Karteninhaber abgemeldet hat, ist es ihm nicht mehr möglich, seine Kreditkarte für Internet-Zahlungen bei am gesicherten Authentifizierungsverfahren teilnehmenden Kartenakzeptanzstellen einzusetzen. Um die Kreditkarte wieder bei diesen Kartenakzeptanzstellen einsetzen zu können, ist eine Neuregistrierung für Verified by Visa / Mastercard SecureCode™ erforderlich.

7. Datenerhebung und Datenverarbeitung, Einschaltung Dritter

7.1. Die Bank bzw. der Kartenherausgeber ist berechtigt, sich zur Bewirkung der von ihr bzw. ihm im Rahmen von Verified by Visa / Mastercard SecureCode™ zu erbringenden Leistungen und zur Einforderung der vom Karteninhaber zu erbringenden Leistungen Dritter zu bedienen.

7.2. Hat ein beauftragter Dienstleister seinen Sitz in einem Land außerhalb der Europäischen Union (z.B. USA) oder außerhalb eines Landes, das dem Abkommen zum Europäischen Wirtschaftsraum beigetreten ist (z.B. Schweiz), wird die Bank bzw. der Kartenherausgeber vor der Datenübermittlung für ein angemessenes Datenschutzniveau im Sinne des Bundesdatenschutzgesetzes sorgen, es sei denn, dass bereits eine Angemessenheitsentscheidung der Europäischen Kommission gemäß Art. 25 Abs. 6 EG-DatSchRL zugunsten des Landes vorliegt, in dem dieser Dienstleister seinen Sitz hat.

7.3. Ausschließlich zum Zweck der Abwicklung des Verified by Visa / Mastercard SecureCode™ -Verfahrens werden personenbezogene Daten des Karteninhabers im Rahmen der Registrierung und bei einer Verified by Visa- bzw. Mastercard SecureCode-Kartenzahlung (z.B. Kartennummer, Geburtsdatum, die hinterlegte Mobilfunknummer / virtuelle Handynummer, Sicherheitsfrage sowie ein Protokoll der authentifizierten Transaktionen, der versendeten Nachrichten und die IP-Adresse und Geräte- / Browserdaten des aufrufenden Geräts) an den jeweiligen Dienstleister weitergegeben und von diesem verarbeitet. Spätestens mit Beendigung des Kreditkartenvertrages werden die Registrierungsdaten gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

7.4. Nimmt eine Kartenakzeptanzstelle an dem Verfahren teil, übernimmt der jeweilige Dienstleister die Authentifizierung des Karteninhabers und teilt der Kartenakzeptanzstelle mit, ob der Authentifizierungsprozess erfolgreich war. Weitere Daten werden nicht an die Kartenakzeptanzstelle übermittelt. War der Authentifizierungsprozess nicht erfolgreich, wird der Authentifizierungsvorgang abgebrochen.

8. Haftung

8.1. Die Bank kann weder einen störungsfreien noch ununterbrochenen Zugang zur App gewährleisten.

8.2. Sie trägt keine Gewähr für die ständige Verfügbarkeit des Verified by Visa / Mastercard SecureCode™ -Verfahrens und haftet nicht für Schäden infolge von Störung, Unterbrechungen (inkl. systembedingter Wartungsarbeiten) oder Überlastungen der beteiligten IT-Systeme.

8.3. Die Bank übernimmt keine Haftung bei Manipulationen des mobilen Endgerätes bzw. dessen Software, wie insbesondere einem sogenannten „Jailbreak" oder „Rooten" bzw. der Installation nicht vom Hersteller freigegebener Betriebssystemvarianten.

8.4. Die Bank haftet nicht für den Fall, dass das Endgerät verloren, gestohlen oder weitergegeben wird und dadurch Dritte Zugriff auf das vom Karteninhaber gewählte Verfahren zur gesicherten Authentifizierung erhalten und dieses ggf. unberechtigt nutzen.

Stand Februar 2017