Sonderbedingungen für das 3D Secure-Verfahren bei Karten-Online-Transaktionen

Die folgenden Bedingungen gelten für die Teilnahme am 3D Secure-Verfahren bei Online-Kartentransaktionen mit einer von der Solarisbank AG (nachfolgend „Bank“ genannt) ausgegebenen Zahlungskarte:

1. Gegenstand, Definition

1.1 Die Bank ermöglicht den Inhabern ihrer für die Online-Nutzung zugelassenen Karten die Teilnahme am 3D Secure-Verfahren, das Händler im Internet zur Absicherung einer Online-Kartentransaktion vorsehen können.

1.2 Das 3D Secure-Verfahren (bei Mastercard als „Mastercard Identity Check“, bei VISA als „VISA SECURE“ bezeichnet) ist ein Verfahren zur Authentifizierung des/der Karteninhaber*in bei Online-Kartentransaktionen.

1.3 Zur Autorisierung von Online-Kartentransaktionen muss der/die Karteninhaber*in bestimmte Authentifizierungselemente verwenden (vgl. Ziffern 4.1 und 7.1 der Bedingungen für das Online Banking).

1.4. Diese Authentifizierungselemente sind z.B. eine dem/der Karteninhaber*in von der Bank via SMS (Short Message Service) auf sein Mobiltelefon übermittelte mobile Transaktionsnummer (nachfolgend „mobileTAN“); die In-App-Authentifizierung, bei der der/die Karteninhaber*in auf die Banking-Applikation des Kooperationspartners der Bank umgeleitet wird (nachfolgend: "In-App-Authentifizierung"); oder Sicherheitsfragen, die nur der/die Karteninhaber*in beantworten kann.

1.5 Die Bank ist berechtigt, einen Kartenumsatz im Internet abzulehnen, wenn Händler im Internet nicht am 3D Secure-Verfahren teilnehmen.

2. Teilnahmevoraussetzungen

2.1 Jeder/jede Inhaber*in einer gültigen und nicht gesperrten Karte nimmt automatisch am 3D Secure-Verfahren teil. Die Anmeldung erfolgt bei Kartenaktivierung. Es ist keine separate Registrierung erforderlich.

2.2 Um die bei einer 3D Secure-Kartenzahlung per mobileTAN erfolgende Authentifizierung vornehmen zu können, muss bei der Bank über deren Kooperationspartner für den/die Karteninhaber*in eine Mobiltelefonnummer hinterlegt worden sein. Diese ist jederzeit änderbar.

2.3 Um eine Authentifizierung per 3D Secure über In-App-Authentifizierung durchführen zu können, muss der/die Karteninhaber*in das mobile Gerät erfolgreich an das mit der Zahlungskarte verbundene Konto gebunden haben.

3. Authentifizierung per 3D Secure

3.1 Die per SMS übermittelte, mindestens sechsstellige mobileTAN ist dann zur Authentifizierung der Online-Kartentransaktion einzugeben. Zum Abgleich werden dem/der Karteninhaber*in auf dem Bildschirm die letzten Stellen der Mobiltelefonnummer angezeigt, an die die mobileTAN per SMS übermittelt wird.

3.2 Die SMS wird von der Bank kostenlos zur Verfügung gestellt.

3.3 Für die In-App-Authentifizierung muss sich der/die Karteninhaber*in in die Banking-Applikation des Kooperationspartners der Bank einloggen, zu der der/die Karteninhaber*in weitergeleitet wird, und die Online-Kartentransaktion bestätigen.

3.4. Für die Authentifizierung durch Beantwortung einer Sicherheitsabfrage muss der/die Karteninhaber*in eine Frage richtig beantworten, die nur er beantworten kann.

4. Sorgfaltspflichten des/der Karteninhaber*in

4.1 Der/die Karteninhaber*in hat dafür Sorge zu tragen, dass kein Dritter zur Durchführung von Online-Kartentransaktionen Zugang zu seinem Mobiltelefon erlangt. Die Bank wird den/die Karteninhaber*in weder per E-Mail noch telefonisch zur Anmeldung oder Bekanntgabe seiner Registrierungsdaten auffordern.

4.2 Für die Sicherheit von SMS, die auf dem Mobiltelefon eingehen, hat der Kunde durch geeignete Maßnahmen (z. B. durch eine passwortgeschützte Zugangssperre) zu sorgen. Die Bank haftet nicht für den Fall, dass das Mobiltelefon verloren, gestohlen oder weitergegeben wird und dadurch Dritte ggf. Zugriff auf SMS erhalten und sich deren Inhalt zu Nutze machen. Gleiches gilt für Authentifizierungselemente, die zur Anmeldung in der Banking-Applikation des Kooperationspartners der Bank verwendet werden (vgl. allgemein Ziffer 7.1 der Bedingungen für das Online-Banking).

4.3 Der/die Karteninhaber*in hat die ihm/ihr von der Bank per SMS übermittelten Daten (s. Ziffer 3.2) auf Übereinstimmung abzugleichen. Bei Unstimmigkeiten ist die Transaktion abzubrechen und die Bank zu informieren.

5. Datenverarbeitung und Dienstleister

5.1 Bei einer 3D Secure-Kartenzahlung werden die Kartennummer, Umsatzdatum und -zeitpunkt, der Transaktionsbetrag, Händlerinformationen (Name, ID, URL) sowie die IP-Adresse, von der aus der Kartenumsatz initiiert wurde, gespeichert.

5.2 Die Bank ist berechtigt, zur Abwicklung des 3D Secure-Verfahrens Dienstleister zu beauftragen. Die Bank stellt diesen Dienstleistern personenbezogene Daten des/der Karteninhaber*in (z.B. Kreditkartennummer) ausschließlich im Rahmen der Zweckbestimmung des Vertragsverhältnisses zur Verfügung.