DON'T do business WITHOUT IT™

Kunden-Information (Stand April 2019)

Thema "SCA" (Strong Customer Authentification) oder "2FA" (Two Factor Authentification)

EU-Thema: Eine Europäische Richtlinie über Zahlungsdienste (Payment Service Directive, PSD2) wurde überarbeitet und sieht, um die Sicherheit im Zahlungsverkehr weiter zu erhöhen, eine „starke Kundenauthentifizierung" vor.

In Folge müssen sich Kreditkartennutzer sich an eine neue Routine besonders auch bei Online-Einkäufen/Zahlungen gewöhnen müssen. Hintergrund ist der steigende Betrugsanteil bei Online-Einkäufen. Ab dem 14. September sollen Zahlungstransaktionen aller von der Regulierung erfassten Zahlungssysteme mit einer starken Authentifizierung durch die Verwendung von zwei Faktoren aus den drei unterschiedlichen Merkmalen

- etwas, das nur der Kunde weiß, wie z. B. Passwort oder PIN;
- etwas, das nur der Kunde besitzt, wie z. B. Karte oder Smartphone;
- etwas, das nur der Kunde haben kann, wie z. B. Fingerabdruck, Stimme, Gesicht

abgesichert werden.

Ab diesem Zeitpunkt müssen dann online Zahlungstransaktionen aller von der Regulierung erfassten Zahlungssysteme mit einer starken Kundenauthentifizierung (auch Zwei-Faktor-Authentifizierung oder Strong Customer Authentication, SCA) abgesichert werden. Die technischen Grundlagen hierfür wurden im November 2017 von der European Banking Authority (EBA) im sogenannten SCA-RTS (Regulatory Technical Standards) veröffentlicht.

Wer ist betroffen?

SCA/2FA betrifft alle am Kreditkarten-Bezahlprozess beteiligten Parteien, also

- Karteninhaber (muss die Zahlung mit zwei aus drei Faktoren autorisieren)
- die kartenherausgebende Bank (muss die Bezahllösung SCA-konform implementieren)
- der Handel (muss seine Bezahlprozesse SCA-konform betreiben)
- die Händlerbank (muss SCA-Konformität ihrer Händler für das verwendete Bezahlsystem sicherstellen)
- Kreditkartenorganisationen (müssen SCA konforme Prozesse/Anforderungen einhalten)

Welche Ausnahmen gibt es?

- Die Bezahlung an stationären Kreditkartenterminals ist bereits heute SCA-konform, da mit Chip & Pin zwei Faktoren abgefragt werden (Karte = Besitz, PIN = Wissen).
- Ausnahmen wie Hotelbuchungen und möglicherweise weitere Kategorien
- Man diskutiert ein „Whitelisting" z. B. von regelmäßigen genutzten Händlern/Merchants
- virtuelle Zahlungsmittel (bspw. BTA/I-BTA, vPayment, BIP) sind als Ausnahme eingestuft worden
- sog. „recurring" Zahlungen oder Mailorder-Transaktionen unterliegen ebenfalls nicht dem 2FA
- Transaktionshöhe (ab 30 EUR)

Viele Fragen hierzu können z.Zt. noch nicht beantwortet werden, der Regulierer wird hierzu weitere, verbindlichere Informationen herausgeben.

American Express Global Commercial Services April 2019

Customer Information: Strong Customer Authentification (SCA) and Two Factor Authentification (2FA)

The EU Payment Services Directive (PSD2) has been revised to provide for strong customer authentication in order to further increase the security of payment transactions.

As a result, credit card users will need to get used to a new procedure, especially for online shopping or payments. The background to this change is the increasing amount of fraud in online shopping.

From 14 September 2019, payment transactions made via all payment systems covered by the regulation must be secured by means of strong authentication using two factors from the following three categories:

- something that only the customer knows, such as their password or PIN;
- something that only the customer has, such as their card or smartphone;
- something that they are, such as their fingerprint, voice or face.

From this date onwards, online payment transactions carried out via all payment systems covered by the regulation must be secured with strong customer authentication (SCA), also known as two-factor authentication (2FA). The technical basis for this was published by the European Banking Authority (EBA) in November 2017 in the Regulatory Technical Standards (SCA-RTS).

Who does this affect?

SCA/2FA affects all parties involved in the credit card payment process, i.e.

- Cardmembers (must authorise the payment using two out of three factors)
- the card issuing bank (must implement the payment solution in a way that is SCA compliant)
- the merchant (must operate its payment processes in a way that is SCA compliant)
- the merchant's bank (must ensure SCA compliance of their merchants for the payment system used)
- Credit card organisations (must follow SCA-compliant processes/requirements)

What are the exceptions?

- Payment in person at credit card terminals is already SCA-compliant, since the use of a chip and pin means that two factors are required (card = have, PIN = know)
- Exceptions include hotel bookings and other possible categories
- There is discussion of whitelisting of, for example, regularly used merchants
- Virtual payment methods (such as BTA/I-BTA, vPayment and BIP) have been classified as exempt
- Recurring payments and mail-order transactions are not subject to 2FA
- Transaction amount (only transactions from €30 are affected)
- ...

Many questions cannot yet be answered; the regulator will provide further information where required.