Die Starke Kundenauthentifizierung im Handel

#WIRsindHANDEL

Durch die rasante Veränderung im Zahlungsverkehr entstanden neue elektronische Zahlungsdienste, die nicht in den bestehenden Rechtsrahmen integriert waren. Die dynamische Entwicklung in der Fin-Tech-Branche machte es daher erforderlich, das Zahlungsdienstegesetz aus dem Jahr 2009 durch die zweite Zahlungsdiensterichtlinie zu modernisieren. Das Zahlungsdienstegesetz 2018 (Umsetzung der 2. EU-Zahlungsdiensterichtlinie) ist bereits am 01.06.2018 in Kraft getreten. Ein für den Handel wichtiger Punkt wird mit 14. September 2019 anwendbar: **die „Starke Kundenauthentifizierung" (auch Zwei-Faktor-Authentifizierung oder strong customer authentification, SCA genannt).**

Durch Bemühungen der EuroCommerce und der Bundessparte Handel hat die Europäische Bankenaufsichtsbehörde am 21.06.2019 den national zuständigen Aufsichtsbehörden die Option geboten, eine zusätzliche Übergangszeit einzuräumen, da aufgrund der Komplexität der Zahlungsmärkte die Umsetzung der Starken Kundenauthentifizierung bis 14.09.2019 nicht flächendeckend möglich ist. Nach konstruktiven Gesprächen der WKÖ mit der zuständigen Aufsichtsbehörde FMA teilte diese mit, dass die von der Europäischen Bankenaufsicht in Aussicht gestellte aufsichtsrechtliche Nachsicht bei der Umsetzung der starken Kundenauthentifizierung in Österreich tatsächlich zur Anwendung gelangen wird. Die

Nachsichtsfrist betrifft ausschließlich Kartenzahlungen über das Internet (somit nicht das Online-Banking oder Kartenzahlungen, die unmittelbar in einem Geschäft an der Kassa vorgenommen werden). Sobald die genauen weiteren Rahmenbedingungen für die Übergangsfrist von der Behörde festgelegt sind, werden wir Sie umgehend darüber informieren. Wir empfehlen aber, sich schon jetzt mit der Thematik zu beschäftigen, auch um eventuelle Haftungsrisiken zu vermeiden.

Sie finden die FAQ´s der WKO unter diesem Link, die laufend aktualisiert werden. Die nachstehenden Ausführungen beruhen auf der Grundlage unseres Verständnisses per August 2019.

1. Warum ist eine Starke Kundenauthentifizierung notwendig?

Um die Sicherheit bei Online- und Kartenzahlungen zu gewährleisten und das Betrugsrisiko zu minimieren, schreibt der Gesetzgeber eine Starke Kundenauthentifizierung vor.

Die Notwendigkeit einer Starken Kundenauthentifizierung wird damit begründet, dass alle elektronisch angebotenen Zahlungsdienste sicher abgewickelt werden und den ständig ändernden Betrugsmethoden standhalten müssen. Dabei sollen Technologien eingesetzt werden, die eine sichere Authentifizierung des Nutzers gewährleisten und das Betrugsrisiko möglichst weitgehend einschränken.

2. Was ist die Starke Kundenauthentifizierung?

Der Zahlungsdienstleister muss das Risiko (sicherheits-)technisch gering halten und mehrere Sicherheitsabfragen machen, damit Kundendaten vor Betrug und Missbrauch besser geschützt sind. Die Risikominimierung erfolgt durch die Starke Kundenauthentifizierung, die vorsieht, dass sich der Kunde mit mindestens zwei aus folgenden drei Faktoren authentifiziert:

- Faktor „Wissen“ - Etwas, das nur der Benutzer weiß, z.B. geheime Codes und Passwörter. Beispiele hierfür sind: Pin bei Zahlungskarten, Secure Code für Online-Kartenzahlungen, Zugangscode für das Online-Banking.

  Hinweis: *Mit dem ZaDiG 2009 war es zum Beispiel zulässig, bei Kreditkartenzahlungen im Internet oder am Telefon die Kundenauthentifizierung lediglich anhand der Kartennummer, des Verfallsdatums und der Prüfzahl vorzunehmen. Diese Daten sind auf der Karte aufgedruckt und damit zwangsläufig nicht geheim. Die Europäische Bankaufsichtsbehörde ist derzeit der Ansicht, dass die Kartennummer, das Verfallsdatum und die Prüfzahl nicht zur „Wissenskategorie“*

gehören. In Zukunft werden Lösungen wie im Online-Banking notwendig sein, z.B. die Eingabe eines Passworts und einer TAN.

- Faktor „Besitz“ - Etwas, das nur der Benutzer besitzt, z.B. ein Mobiltelefon, auf dem dem Nutzer der für die Freigabe einer Internetzahlung notwendige TAN mitgeteilt werden oder Instrumente wie Zahlungskarten, TAN-Generatoren oder Token.

- Faktor „Inhärenz“ - Etwas, das der Benutzer ist z.B. die Verwendung von biometrischen Daten wie Fingerabdruck, Gesichts-, Iris- oder Stimmerkennung. Praktisch bedeutsam ist derzeit die Gesichtserkennung oder der Fingerabdruck, der beim Mobilbanking per App für die Identifikation des Kunden verwendet wird.

Der Gesetzgeber fordert, dass die zwei (von den möglichen drei) erforderlichen Authentifizierungsfaktoren verschiedenen Kategorien angehören und die ausgewählten Faktoren voneinander unabhängig sein müssen. Es muss daher sichergestellt werden, dass zwei getrennte Schutzmechanismen eingreifen damit eine Zahlung als sicher eingestuft wird.

***Beispiel**: Die Bezahlung an stationären Kreditkartenterminals ist bereits heute gesetzeskonform, da mit Kartenchip und Pin zwei Faktoren abgefragt werden (Kartenchip = Besitz, Pin = Wissen). Es bestehen daher zwei getrennte Schutzmechanismen, die betrügerische Zahlungstransaktionen begrenzen.*

Technisch gesehen muss der Authentifizierungsvorgang einen nur einmalig verwendbaren Authentifizierungscode generieren und gewährleisten, dass keine Rückschlüsse auf die Elemente Wissen, Besitz und Inhärenz hergestellt werden.

3. Wann muss eine starke Kundenauthentifizierung durchgeführt werden?

Der Zahlungsdienstleister muss dann eine starke Kundenauthentifizierung verlangen, wenn der Zahler

1. online auf sein Zahlungskonto zugreift

   Beispiel: Die Beauftragung einer Überweisung im Online-Banking. Dabei ist die starke Kundenauthentifizierung wie auch in den anderen genannten Fällen mit einer sogenannten dynamischen Verknüpfung in Bezug auf Empfänger und Betrag zu erweitern. Daher muss etwa bei Übersendung einer TAN mittels SMS oder einer Push-Nachricht über eine App dem Nutzer mitgeteilt werden, für welchen Betrag und Zahlungsempfänger die starke Kundenauthentifizierung gilt

2. einen elektronischen Zahlungsvorgang auslöst

Beispiel: Die Bezahlung mit Karte und PIN an der Ladekasse ist ein elektronischer Zahlungsvorgang.

3. über einen Fernzugang eine Handlung vornimmt, die ein Betrugs- oder Missbrauchsrisiko in sich birgt

4. Wann muss keine starke Kundenauthentifizierung durchgeführt werden bzw. wann ist das Gesetz nicht anwendbar?

In folgenden Fällen gilt das Gesetz über die Starke Kundenauthentifizierung nicht:

- nicht für Transaktionen mit Bezahlkarten aus dem Nicht-EWR Bereich (z.B. ein amerikanischer oder asiatischer Käufer bestellt eine Ware über seine ausländische Kreditkarte)
- nicht für Transaktionen über Telefon bzw. postalische Bestellung, wo ein Mitarbeiter die Eingabe übernimmt (E-Mail-Bestellung/Telefonbestellung im Versandhandel, TV-Home-Shopping per Anruf)
- nicht bei anonymen Bezahlkarten (prepaid cards)
- nicht bei vom Händler initiierten (Folge)transaktionen aufgrund eines bestehenden Vertrages (Kunde ermächtigt Händler, bei weiteren Käufen Kreditkarte zu belasten).
- Gutscheinkarten, die ein Unternehmen ausgibt und nur bei diesen online eingelöst werden können (begrenzte Netze)

5. Wann muss keine starke Kundenauthentifizierung aufgrund einer Ausnahmebestimmung durchgeführt werden?

In folgenden Fällen können Zahlungsdienstleister auf eine Starke Kundenauthentifizierung verzichten.

5.1. Wiederkehrende Transaktionen (Daueraufträge)

Wenn ein Verbraucher eine wiederkehrende Transaktion desselben Betrags und für denselben Händler einrichtet, kann ein Zahlungsdienstleister (Payment Service Provider, PSP) bei Folgetransaktionen von der Starken Kundenauthentifizierung absehen, wenn die erste Zahlung entsprechend authentifiziert bzw. historisch übernommen wurde.

5.2. Kleinbetragszahlungen

Elektronische Ferntransaktionen, die die folgenden Bedingungen erfüllen, können ebenfalls von der Starken Kundenauthentifizierung ausgenommen werden:

- Der Betrag darf EUR 30 nicht überschreiten

- Der kumulierte Betrag beträgt weniger als EUR 100 oder überschreitet nicht 5 aufeinander folgende Transaktionen

5.3. Vertrauenswürdig eingestufte Zahlungsempfänger oder „Weiße Liste“

Die Starke Kundenauthentifizierung wird nicht benötigt, wenn der Händler (Zahlungsempfänger) in einer Liste vertrauenswürdiger Begünstigter aufgeführt ist. Der Karteninhaber (Kunde) kann verschiedene Händler auf die Liste der vertrauenswürdigen Empfänger setzen lassen, bei denen die Geldinstitute oder Kartenherausgeber (Emittenten) auf die Zwei-Faktor-Authentifizierung verzichten können.

Beispiel: Ein Kunde bestellt regelmäßig bei einem Online-Portal und setzt das Online-Portal auf seine „White-List“. Damit kann die Bank auf die Zwei-Faktor-Authentifizierung verzichten.

5.4. Betrugsraten und Transaktionsrisikoanalyse (TRA)

Für Transaktionen, bei denen ein geringes Betrugsrisiko angenommen wird, müssen Zahlungsdienstleister keine Starke Kundenauthentifizierung anwenden. Dies betrifft Transaktionen bis zu einem Wert von 500 EUR.

5.5. Andere Ausnahmen

Weitere Ausnahmen sind für Transaktionen wie kontaktloses Bezahlen, sichere Überweisungen von Unternehmenszahlungen, Zugriff auf Zahlungskontoinformationen oder für Überweisung auf ein anderes Konto enthalten, das von derselben Person mit demselben Zahlungsdienstleister geführt wird.

Bitte beachten Sie, dass die Ausnahmen 5.1 bis 5.5 nicht verpflichtend angewendet werden müssen. Zahlungsdienstleister (also Kartenherausgeber und Acquirer) können sich auch dazu entscheiden, grundsätzlich mit der Starken Kundenauthentifizierung zu arbeiten. Unternehmen können daher diese Befreiung nicht direkt anwenden, sondern müssen sich darauf verlassen, dass ihr Karten-Acquirer oder Zahlungsdienstleister die Befreiung anwendet.

Wer ist von der Umsetzung der Starken Kundenauthentifizierung betroffen?

Davon betroffen sind insbesondere Zahlungsdienstanbieter, die zwischen einem Online-Händler und der Bank eines Käufers stehen und die Überweisung über das Internet ermöglichen. Die Starke Kundenauthentifizierung betrifft aber alle am Kreditkarten-Bezahlprozess beteiligten Parteien:

- Karteninhaber: muss die Zahlung mit zwei aus drei Faktoren autorisieren

- die kartenherausgebende Bank: muss die Bezahllösung SCA-konform (SCA= strong customer authentifaction) 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

6. Warum sollte die Starke Kundenauthentifizierung Händler interessieren?

Die Starke Kundenauthentifizierung wird grundsätzlich am 14.9.2019 in der EU und im gesamten Europäischen Wirtschaftsraum in Kraft treten. Die Europäische Bankenaufsichtsbehörde hat den für die Zahlungsdienstleistungen zuständigen nationalen Aufsichtsbehörden am 21.6.2019 die Möglichkeit eingeräumt, die Umsetzung durch die Zahlungsdienstleister hinauszustrecken, soweit diese Migrations- und Informationspläne vorlegen. Weil die Umsetzung der neuen Vorgaben technische Nachrüstungen erfordert, hat sich die Wirtschaftskammer erfolgreich für einen zeitlichen Aufschub eingesetzt. Nach konstruktiven Gesprächen der WKÖ mit der zuständigen Aufsichtsbehörde FMA teilte diese nun mit, dass die von der Europäischen Bankenaufsicht in Aussicht gestellte aufsichtsrechtliche Nachsicht bei der Umsetzung der starken Kundenauthentifizierung in Österreich tatsächlich zur Anwendung gelangen wird. Die Nachsichtsfrist betrifft ausschließlich Kartenzahlungen über das Internet. Sobald die genauen weiteren Rahmenbedingungen für die Übergangsfrist von der Behörde festgelegt sind, werden wir Sie umgehend darüber informieren. Wir empfehlen aber, sich schon jetzt mit der Thematik zu beschäftigen und – soweit möglich - eine baldige Umsetzung in Abstimmung mit ihren Zahlungsdienstleistern anzustreben, auch um eventuelle Haftungsrisiken, die bei missbräuchlicher Verwendung von Zahlungsinstrumenten nicht ausgeschlossen werden können, zu vermeiden.

- Bis 14.09.2019 bzw. bis zu der neuen Umsetzungsfrist müssen von den Händlern alle erforderlichen Maßnahmen umgesetzt sein, da sonst Kartenzahlungen abgelehnt oder Zahlvorgänge abgebrochen werden können.

- Um weiterhin ein reibungsloses Einkaufserlebnis zu schaffen, müssen Kunden sensibilisiert und informiert werden. Stellen Sie daher sicher, dass Ihre Kunden über die Neuerungen informiert sind und weisen Sie Ihre Kunden darauf hin, dass sich der Zahlungsprozess in Zukunft durch die Starke Kundenauthentifizierung ändern wird.

7. Was sind die wichtigsten nächsten Schritte für Händler?

1. Händler müssen sich der bevorstehenden Änderungen bewusst sein und sich mit ihrem Kartenacquirier bzw. Zahlungsdienstleister austauschen, die für die Implementierung einer starken Kundenauthentifizierung verantwortlich sind. Die Händler sollten die verfügbaren Lösungen untersuchen, diskutieren und

klar definieren, welche vorbereitenden Schritte sie unternehmen müssen, um sicherzustellen, dass ihre Kunden weiterhin ein reibungsloses und nahtloses Einkaufserlebnis erhalten.

2. Wenn dies nicht bereits geschehen ist, sollten Händler im Online-Handel EMV 3D Secure 2.1 (3DS) verwenden, da die Genehmigungsraten wahrscheinlich sinken, wenn keine Authentifizierung verwendet wird. Einige Emittenten lehnen Transaktionen möglicherweise sogar systematisch ab, ohne dass 3D-Secure aktiviert wird, weil sie befürchten, dass die Regelungen hinsichtlich der Starken Kundenauthentifizierung nicht eingehalten werden.

   Erklärung: EMV 3D-Secure ist ein globaler Branchenstandard und unterstützt Händler und Kartenherausgeber bei der Authentifizierung von E-Commerce-Zahlungen. Der neue Standard ersetzt u.a. statische Passwörter durch eine stärkere Zwei-Faktor-Authentifizierung und ist damit ein sicherer Authentifizierungsstandard. Beispielsweise erfüllen SafeKey von American Express, Mastercard und Visa diese Sicherheitsstandards bereits heute.

   ***Empfehlung**: Wenden Sie sich daher rechtszeitig an Ihren Zahlungsdienstleister und beantragen Sie die Anmeldung Ihres Onlineshops für die entsprechenden Sicherheitsverfahren der Kreditkartenanbieter.*

3. Wenn der Emittent EMV 3D-Secure noch nicht unterstützt, sollten Händler versuchen, mit 3DS v1.0 höhere Genehmigungsraten zu erzielen.

4. Händler sollten weitgehend die Ausnahmebestimmungen (siehe oben Punkt 5) in Anspruch nehmen. Besprechen Sie daher die für Sie möglichen Ausnahmen mit ihrer Händlerbank (Acquirer)/Zahlungsdienstleister.

5. Stationäre Händler müssen sicherstellen, dass ihr verwendetes Kassensystem/Terminal auf dem Stand der neuen Richtlinie ist, da bei kontaktlosen Bezahlungen nach dem Erreichen einer Gesamtsumme von EUR 150 – auch durch mehrere Einzelzahlungen – der Karteninhaber zu einer Pin-Zahlung angewiesen wird und eine Authentifizierung durchführen muss. Konkret müssen dafür durch den Anbieter des Kassensystems oder des Kartenlesegerätes Updates durchgeführt werden, damit das System die Karteninhaber bei Bezahlungen ab Erreichen einer Summe von 150 Euro anweisen kann, sich mit dem Pin zu authentifizieren. Wenden Sie sich an den Anbieter Ihres Kassensystems oder an Ihren Zahlungsdienstleister, damit diese Updates rechtzeitig vorgenommen werden. Zudem ist es ratsam, Ihre Mitarbeiter zu schulen.

6. Darüber hinaus sollten Händler in Abstimmung mit ihren Zahlungsdiensteanbietern ihre Payment-Schnittstellen adaptieren und in

Erfahrung bringen, welche Daten für Zwecke der Zwei-Faktor-Authentifizierung an die Zahlungsdiensteanbieter übermittelt werden (z.B. Kreditkartendaten, Rechnungs- und Lieferadresse). Auf den Datentransfer zwischen Händler und Zahlungsdiensteanbeiter sollten Kunden aus datenschutzrechtlichen Gründen informiert werden. Überprüfen und ergänzen Sie daher juristisch Ihre Datenschutzrichtlinie und Ihre AGBs in Hinblick auf die erweiterte Datenübermittlung.

Impressum

Medieninhaber und Herausgeber:
Wirtschaftskammer Österreich, Wiedner Hauptstraße 63,
1045 Wien, Bundessparte Handel
Verfasser: Sinan Ibili, MSc

Die in diesen Dokumenten enthaltenen Informationen wurden nach bestem Wissen erstellt und stellen keine Rechtsberatung dar. Die Auslegung des SCA-Regelungen (SCA= strong customer authentifaction) kann zwischen den Mitgliedstaaten variieren. Die Ausführungen beruhen auf der Grundlage unseres Verständnisses per August 2019. Nachfolgende Änderungen der Rechtslage führen zu keinerlei Nachbesserungs- und Informationspflichten von WKO.

Alle Angaben erfolgen trotz sorgfältiger Bearbeitung ohne Gewähr. Eine Haftung der Wirtschaftskammer Österreich und deren Mitarbeiter ist ausgeschlossen.

Um eine leichtere Lesbarkeit des Textes zu gewährleisten, wurde auf die explizit geschlechtsspezifische Schreibweise verzichtet.