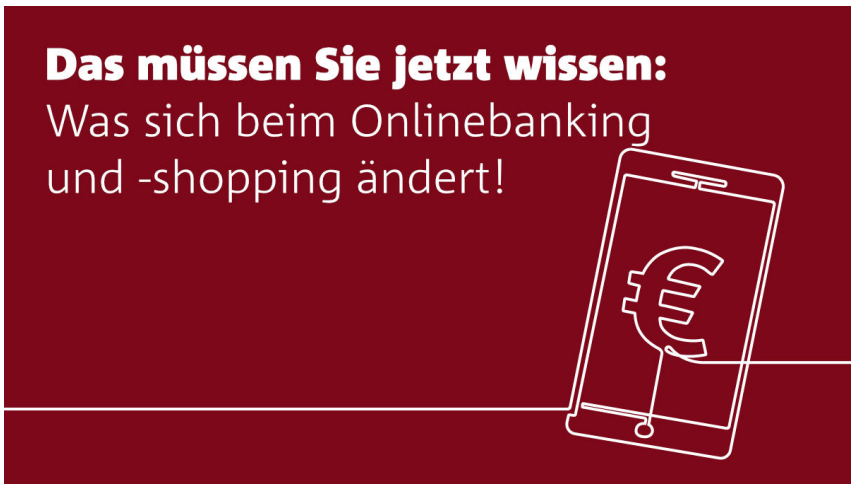
Neue Regeln bei Onlinebanking und Bezahlen im Netz: Was ändert sich?



15.05.2019
von Sylvie Ernoult

Kurzgefasst

In den kommenden Wochen erhalten alle Bankkunden Post von ihrer Bank. Dabei geht es um ein wichtiges Thema: Neue Regeln im Zahlungsverkehr, vor allem beim Onlinebanking und bei Kartenzahlungen. Die Grundlage dafür ist die Zweite europäische Zahlungsdiensterichtlinie, kurz PSD2, deren zweite Stufe am 14. September 2019 in Kraft tritt. Zu diesem Datum müssen Banken aufgrund gesetzlicher Vorgaben technische und vertragliche Anpassungen im Onlinebanking und beim Bezahlen mit Karte vornehmen.

Schlagworte

Verbraucher
Onlinebanking
PSD2
Verbraucherschutz

Warum werden die Bedingungen zum Zahlungsverkehr geändert?

Anlass der Änderungen ist die Umsetzung der zweiten Stufe der PSD2, die vor allem neue Vorgaben zur Kundenauthentifizierung und zum Zugriff auf Konten durch Drittanbieter enthält. Diese gelten ab dem 14. September 2019. Banken sind daher verpflichtet, die entsprechenden Bedingungen für das Onlinebanking und für Zahlungskarten anzupassen und ihre Kundinnen und Kunden darüber zu informieren.

Drei wesentliche Punkte sind von dieser Änderung betroffen:

1. Es gibt nun einheitliche rechtliche und technische Regeln für den Online-Zugriff von sogenannten Drittdienstleistern, wenn der Kunde diese auf sein Konto zugreifen lassen möchte.
2. Beim Zugriff auf Informationen zum Konto mittels Onlinebanking muss sich der Kunde grundsätzlich mit zwei Faktoren authentifizieren.
3. Kartenzahlungen, die im Internet getätigt werden, müssen künftig ebenfalls mit zwei Faktoren freigegeben werden.

Was ändert sich im Bereich der Drittdienstleister?

Unter Drittdiensten versteht man Dienstleister, die Bankinfrastrukturen nutzen, ohne selbst solche zu betreiben. Die PSD2 unterscheidet drei Arten von Drittanbietern und stellt für diese besondere Regeln auf: Zahlungsauslösedienste, Kontoinformationsdienste und kartenausgebende Drittdienstleister.

Ein Zahlungsauslösedienst wird vom Bankkunden beauftragt, per Onlinebanking eine Überweisung zulasten des Bankkontos auszulösen (z. B. zur Bezahlung eines Einkaufs im Internet über einen auf der Händlerseite angebotenen Zahlungsauslösedienst).

Kontoinformationsdienste sind in der Lage, Kontoinformationen wie Umsätze, Salden und Vormerkposten abzurufen, sofern der Kunde am Onlinebanking seiner Bank teilnimmt. Dies ist insbesondere dann interessant, wenn ein Kunde Konten bei mehreren Banken hat und sich einen besseren Überblick über seine Kontenlage verschaffen möchte.

Ein Kartenausgebedienst kann, wie der Name schon sagt, Kunden Karten zur Verfügung stellen, mit deren Hilfe Zahlungen vom Bankkonto des Kunden bewirkt werden können. Kartenausgebende Drittdienstleister können mit Zustimmung des Kunden die Verfügbarkeit von Beträgen auf dessen Girokonto abfragen. Die Abfrage erfolgt, wenn man mit der Karte bezahlen möchte. Konkrete Anwendungsfälle in Deutschland sind noch nicht bekannt geworden, gleichwohl hat sich die Kreditwirtschaft auf diese neue Anforderung vorbereitet.

Auch in der Vergangenheit konnten Dritte ihre Dienste bereits anbieten, die PSD2 sorgt nun auf rechtlich abgesicherter Grundlage für EU-einheitliche Vorgaben.

Was bedeuten die neuen Vorschriften zu Drittdienstleistern für Bankkunden?

Bankkunden können bei Online-Überweisungen Drittdienstleister damit beauftragen, Zahlungen vorzunehmen oder Kontoinformationen abzurufen (beispielsweise für die Finanzplanung). Die Bank ist verpflichtet, den von den Kunden beauftragten Dienstleistern Zugang zu ihrem Zahlungskonto zu gewähren. Diese Dienstleister unterliegen der Bankenaufsicht.

Auf welche Kontodaten darf der Drittdienstleister zugreifen?

Nur der Kunde entscheidet, ob und gegebenenfalls welche Kontodaten der Drittdienst zur Erbringung seiner Dienstleistung einsehen darf.

Werden Drittdienste beaufsichtigt?

Die Drittdienstleister unterliegen der Bankaufsicht und müssen hohe Anforderungen erfüllen. Entsprechend benötigen Zahlungsauslösedienste und Kontoinformationsdienste für ihre Tätigkeit eine Zulassung von der zuständigen nationalen Aufsichtsbehörde. Das ist in Deutschland die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Kartenausgebedienste brauchen eine Zulassung als Zahlungsinstitut. Kreditinstitute sind berechtigt, ebenfalls als Zahlungsauslösedienst, Kontoinformationsdienst und Kartenausgebedienst aktiv zu werden.

Wie kann ich als Kunde erkennen, ob der Drittdienstleister gesetzlich anerkannt ist und der Bankenaufsicht unterliegt?

Die Europäische Bankenaufsichtsbehörde (EBA) und die BaFin führen hierzu Verzeichnisse, die auch über das Internet einsehbar sind.

Wie ist der Zeitplan für die Umsetzung der PSD2-Schnittstelle?

Die sogenannte PSD2-Schnittstelle sorgt für eine sichere technische Kommunikation zwischen dem Drittdienst und der Bank; sie wird von den Banken bis zum 14. September 2019 umgesetzt. Bereits ab dem 14. Juni 2019 stellen sie den Drittdiensten die Schnittstelle zum Testen zur Verfügung, damit zum Stichtag alles reibungslos funktioniert. Viele Banken und Sparkassen in Deutschland arbeiten gemeinsam an einer europaweit einheitlichen Schnittstellenspezifikation. Damit besteht die Chance, ein möglichst einheitliches digitales Umfeld zum Vorteil der Verbraucher und Unternehmen zu schaffen.

Was ist eine starke Kundenauthentifizierung?

Ab dem 14. September 2019 gilt die gesetzliche Pflicht zur starken Kundenauthentifizierung. Bankkunden müssen dann grundsätzlich jede Online-Überweisung oder Karten-Zahlung mit einer solchen starken Kundenauthentifizierung freigeben. Darunter versteht man eine Authentifizierung bei der mindestens zwei sogenannte „Faktoren“ zum Einsatz kommen. Grundsätzlich gibt es drei mögliche Faktoren:

- den Faktor „Sein“ (biometrische Merkmale wie zum Beispiel der Fingerabdruck),
- den Faktor „Wissen“ (zum Beispiel eine PIN),
- den Faktor „Besitz“ (zum Beispiel ein Smartphone).

Darüber hinaus wird die Transaktionsbindung bei Zahlungsauslösungen verpflichtend. Das heißt, dass eine generierte „TAN“ jeweils nur für die ausgelöste Transaktion nutzbar ist. Statische Verfahren wie die iTAN-Liste, bei der die TAN schon vorher bekannt ist und nicht speziell für die Zahlung generiert wird, sind dann für die Freigabe von Zahlungen nicht mehr zulässig.

Doch nicht nur bei Zahlungen, auch für das Log-in in das Onlinebanking werden in Zukunft grundsätzlich zwei Faktoren erforderlich sein.

Was ändert sich bei Zahlungen im Onlinebanking?

Bei Onlineüberweisungen ist die sogenannte Zwei-Faktor-Authentifizierung bereits heute Pflicht. Das bedeutet, dass die Authentifizierung über zwei Faktoren erfolgen muss, die durch Wissen (z. B. PIN), Besitz (z. B. Smartphone) oder Sein (z. B. Fingerabdruck) vermittelt werden. Ab dem 14. September 2019 sind für die Zahlungsauslösung allerdings nur noch TAN-Verfahren erlaubt, bei denen für jede Transaktion jeweils eine TAN neu generiert wird (das sogenannte dynamische TAN-Verfahren). Die Banken müssen daher bis zu diesem Datum alle iTAN-Listen für den Zahlungsverkehr abgeschaltet haben.
Beim Log-in darf die ITAN noch weiter benutzt werden. Von der Verpflichtung einer starken Kundenauthentifizierung kann es vereinzelte Ausnahmen geben, etwa bei der Bezahlung kleiner oder wiederkehrender Beträge.

Und wie funktioniert künftig das Login beim Onlinebanking?

Für den Bankkunden bedeutet die Umsetzung der PSD2 vor allem in einem Punkt eine wesentliche Veränderung: Auch beim Log-in in das Onlinebanking oder beim Zugriff auf sensible persönliche Daten wird grundsätzlich eine Zwei-Faktor-Authentifizierung nötig sein. So kann für das Log-in neben der Eingabe von Benutzerkennung und Onlinebanking-PIN zukünftig eine TAN abgefragt werden

Was ändert sich bei Kartenzahlungen?

Bei der Zahlung im Supermarkt oder an der Ladenkasse ändert sich nichts – schon heute werden hier die Anforderungen durch Karte und PIN erfüllt. Beim Bezahlen im Internet wird es zu Anpassungen bei den Sicherheitsverfahren kom-

men. Auch hier benötigt der Kunde künftig zur Freigabe der Zahlung zwei Faktoren. So kann z. B. bei teilnehmenden Online-Händlern die Freigabe der Internetzahlungen mit Karte über eine Banking-App oder per SMS-basierter TAN erfolgen.

Kann ich den Änderungen in den Bedingungen widersprechen? Bis wann?

Ja, man kann den Änderungen in den Bedingungen vor dem 14. September 2019 widersprechen oder den zugrundeliegenden Vertrag kündigen. Andernfalls gilt die Zustimmung als erteilt. Allerdings sollten Bankkunden beachten, dass die Vertragsänderungen aufgrund gesetzlicher Vorgaben vorgenommen werden, d. h., alle Banken und Sparkassen sind verpflichtet, ihre Vertragswerke anzupassen. Wichtig: Bei einem Widerspruch kann die Bank viele Dienstleistungen nicht mehr anbieten.

Wird es die Sms-Tan in Zukunft noch geben?

Die SMS-TAN wird von der BaFin derzeit noch als konform angesehen, sodass sie grundsätzlich noch genutzt werden darf.

Wie gestaltet sich in Zukunft das Log-In? Was ist die 90-Tage-Regel?

Grundsätzlich ist bei jedem Log-In eine starke Kundenauthentifizierung erforderlich. Dann kann der Kunde in der gleichen Session auch sensible Daten, z. B. seine Kontaktdaten, oder die gesamte Umsatzübersicht einsehen.

Von dieser Vorgabe gibt es eine Ausnahme nach Art. 10 der RTS, die als 90-Tage-Regel bekannt ist: Wendet die Bank diese Regel an, muss sich der Kunde spätestens alle 90 Tage mit Starker Kundenauthentifizierung einloggen. Bei Anwendung der 90-Tage-Regel dürfen dem Nutzer nach dem Log-In mit einem Faktor jedoch keine sensiblen Daten und auch keine Umsätze, die älter als 90 Tage sind, ange-

zeigt werden. Hierfür müsste er dann in der Session eine starke Kundenauthentifizierung ausführen.

Mit der Starken Kundenauthentifizierung bei jedem Log-In hat der Kunde also direkt einen umfassenden Zugriff auf Kontoinformationen, während bei Anwendung der 90-Tage-Regel nur ein eingeschränkter Zugriff ermöglicht wird.

Am 13. August 2019 wurde der Blog aktualisiert.