Bundesministerium
der Finanzen

eu2020.de

Sarah Ryglewski
Parlamentarische Staatssekretärin

POSTANSCHRIFT Bundesministerium der Finanzen, 11016 Berlin

Mitglied des Deutschen Bundestages
Herrn Stefan Liebich
Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Wilhelmstraße 97
10117 Berlin
TEL +49 (0) 30 18 682-4245
FAX +49 (0) 30 18 682-4404
E-MAIL Sarah.Ryglewski@bmf.bund.de
DATUM 18. September 2020

BETREFF **Ihre schriftliche Frage Nr. 165 für den Monat September 2020**

GZ **VII A 3 - WK 7031/20/10010 :001**
DOK **2020/0948707**
(bei Antwort bitte GZ und DOK angeben)

Sehr geehrter Herr Kollege,

Ihre Frage,

„Wie ist nach Kenntnis der Bundesregierung der aktuelle Stand der Umsetzung der PSD-II-Richtlinie in Deutschland (bitte für einzelne Bereiche aufschlüsseln), insbesondere hinsichtlich der Anwendung von Sicherheitsanforderungen (Zwei-Faktor-Authentisierung) bei Kartenzahlungen, und welche Folgen hätte eine weitere Verschiebung der Umsetzung bzw. eine unzureichende Umsetzung aus Sicht der Bundesregierung für Verbraucherinnen und Verbraucher, insbesondere bezüglich der Gefahr, dass zukünftig Zahlungen abgelehnt werden könnten (vgl. BEUC, COVID-19 cannot be an excuse to delay making online payments safer, 5/2020)?“,

beantworte ich wie folgt:

Die Zweite Zahlungsdiensterichtlinie (PSD 2, Richtlinie (EU) 2015/2366, ABl. L 337 vom 23. Dezember 2015, S. 35) ersetzt ihre Vorgängerrichtlinie mit der Zielsetzung, Innovationen im Zahlungsverkehr zu fördern, die Sicherheit von Zahlungen zu verbessern und die Rechte der Kundinnen und Kunden von Zahlungsdienstleistern (bspw. Banken) zu stärken. Es handelt sich um eine vollharmonisierende, europäische Richtlinie, weswegen es den Mitgliedstaaten grundsätzlich nicht erlaubt ist, von den Bestimmungen der Richtlinie abweichende innerstaatliche Rechtsvorschriften beizubehalten oder einzuführen.

Die Vorgaben der PSD 2 wurden durch das Gesetz zur Umsetzung der Zweiten Zahlungsdiensterichtlinie vom 17. Juli 2017 (BGBl. I S. 2446) bereits in nationales Recht umgesetzt. Das Gesetz trat gestaffelt in Kraft. Grundsätzlich gelten die neuen Vorschriften für Zahlungsdienste ab dem 13. Januar 2018. Ausgenommen sind ausgewählte aufsichtsrechtliche Vorgaben wie bspw. zur starken Kundenauthentifizierung (§ 55 des Zahlungsdiensteaufsichtsgesetz, ZAG). Diese Vorschriften gelten ab dem 14. September 2019 zusammen mit der sie konkretisierenden Delegierten Verordnung (EU) 2018/389 (ABl. L 69 vom 13. März 2018, S. 23).

§ 55 ZAG gibt vor, dass Zahlungsdienstleister eine starke Kundenauthentifizierung - Heranziehen von mindestens zwei Elementen der Kategorie Wissen, Besitz oder Inhärenz (ständiges Merkmal des Kunden, z. B. Fingerabdruck) - verlangen müssen, wenn der Zahler beispielsweise einen elektronischen Fernzahlungsvorgang auslöst oder online auf sein Zahlungskonto zugreift. Bei einem elektronischen Zahlungsvorgang muss der Authentifizierungsprozess Elemente umfassen, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen. Des Weiteren sieht § 675v Absatz 4 des Bürgerlichen Gesetzbuchs (BGB) vor, dass Kundinnen und Kunden ihren Zahlungsdienstleistern nicht zum Schadensersatz verpflichtet sind, wenn eine starke Kundenauthentifizierung durch die Bank des Zahlers nicht verlangt bzw. durch die Vertragspartner des Zahlers (Zahlungsempfänger) oder deren Banken nicht akzeptiert wird.

Die Anforderungen an eine starke Kundenauthentifizierung sowie Ausnahmen davon werden in der Delegierten Verordnung (EU) 2018/389 konkretisiert. Im Vordergrund steht hierbei die Sicherheit der Gelder und Zahlungsinformationen der Nutzer. Die einschlägige Delegierte Verordnung (EU) 2018/389 gibt nicht vor, auf welche konkrete technische Art die Sicherheitsanforderungen erfüllt werden müssen. Sie ist technikneutral ausgestaltet. Die technischen Umstellungen obliegen den Marktakteuren d.h. den jeweiligen Zahlungsdienstleistern (bspw. der Bank).

Die Europäische Bankenaufsichtsbehörde (EBA) hat mit ihrer Stellungnahme vom 21. Juni 2019 (EBA-Op-2019-06) den nationalen Aufsichtsbehörden die Möglichkeit eingeräumt, im Hinblick auf die komplexe Implementierung der starken Kundenauthentifizierung bei kartenbasierten Internet-Zahlungen unter bestimmten Voraussetzungen für gewisse Zeit von aufsichtsrechtlichen Beanstandungen abzusehen. Hierzu müssen von den Zahlungsdienstleistern Migrationspläne erstellt und mit den nationalen Aufsichtsbehörden abgestimmt werden. Darüber hinaus hat die EBA in einer weiteren Stellungnahme vom 16. Oktober 2019 (EBA-Op-2019-11) den nationalen Aufsichtsbehörden empfohlen, von der Möglichkeit eines Absehens von aufsichtsrechtlichen Beanstandungen bei kartenbasierten Internet-Zahlungen zeitlich längstens bis zum 31. Dezember 2020 Gebrauch zu machen. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat die Vorgaben der EBA zur Sicherstellung eines

reibungslosen Übergangs auf die neuen Anforderungen und zur Verhinderung von Störungen bei kartenbasierten Internet-Zahlungen in ihre Aufsichtspraxis übernommen (vgl. zu Einzelheiten die BaFin-Mitteilungen vom 21. August 2019 und vom 17. Oktober 2019, abrufbar von der Internetseite der BaFin). Insoweit unberührt bleiben die zivilrechtlichen Haftungsregelungen nach dem BGB bspw. zwischen Kundinnen und Kunden sowie Banken (vgl. §§ 675u bis 675w BGB).

Für einzelne Bereiche stellt sich der Stand der PSD 2-Umstellungen nach Kenntnis der BaFin folgendermaßen dar:

Zahlung mit Karte im Internet: Für den Bereich der Kartenzahlung im Internet bieten inzwischen alle deutschen Zahlungsdienstleister, die Karten mit Internet-Zahlungsfunktion ausgeben, ihren Kundinnen und Kunden grundsätzlich die Möglichkeit, kartenbasierte Internet-Zahlungen mit starker Kundenauthentifizierung durchzuführen. Das für die Durchführung einer starken Kundenauthentifizierung bereits verwendete Kommunikations-protokoll soll in der aktuellsten Version voraussichtlich bis Ende des dritten Quartals 2020 flächendeckend bei Zahlungsdienstleistern eingeführt sein und steht auch den Zahlungs-empfängern (Händlern) für eine Implementierung zur Verfügung. Die aktualisierte Version erlaubt es auch, einschlägige Ausnahmen nach Maßgabe der Delegierten Verordnung (EG) 2018/389 zu nutzen. Damit können bei Implementierung der aktualisierten Version alle im Internet üblichen Geschäftsvorfälle einer Kartenzahlung entsprechend der Delegierten Verordnung (EU) 2018/389 vollends durchgeführt werden.

Zahlung mit Karte vor Ort: Für den Bereich der Kartenzahlung vor Ort, bspw. an der Ladenkasse im Supermarkt, wurden die PSD 2-Vorgaben rechtzeitig in der Anwendungspraxis umgesetzt. Hier waren nur geringfügige Anpassungen notwendig, da für diese Zahlungen die starke Kundenauthentifizierung (Karte und PIN = Persönliche Identifikationsnummer) schon seit längerem praktiziert wird. Es lässt sich mit Blick auf die Corona-Pandemie beobachten, dass zur Infektionsvermeidung häufiger kontaktlos mit Karte vor Ort bezahlt wird. Für derartige kontaktlose Zahlungen hat die Deutsche Kreditwirtschaft in ihrem Girocard-System das Limit von bislang 25 Euro auf 50 Euro je Zahlung erhöht, bei der eine starke Kundenauthentifizierung nicht erforderlich ist. Damit hält sich die Deutsche Kreditwirtschaft innerhalb des Rahmens auf, der von der Delegierten Verordnung (EU) 2018/389 vorgegeben wird.

Zahlung im Online-Banking: Für den Bereich der Zahlung im Online-Banking bspw. mittels Überweisung ist bei Zahlungsdienstleistern eine vollständige PSD 2-Implementierung erreicht. So lässt sich bspw. vollends die Abschaffung von papierhaften TAN-Listen (= Listen mit Transaktionsnummern) beobachten. Derartige in der Vergangenheit von Banken noch verwendete Listen erfüllen die oben genannten Anforderungen für Fernzahlungsvorgänge

nach § 55 ZAG nicht: Es konnten die aufgedruckten TANs für beliebige Zahlungen verwendet werden und die Listen waren leicht zu kopieren. Auf Basis der PSD 2-Vorgaben existieren je nach Zahlungsdienstleister verschiedene Verfahren der starken Kunden-authentifizierung wie bspw. unter Nutzung von Mobilfunkgeräten oder unter Zuhilfenahme von sog. TAN-Generatoren.

Zahlung mit Lastschrift: Im Bereich der Zahlung mit Lastschrift sind die Vorgaben zur starken Kundenauthentifizierung grundsätzlich nicht einschlägig, da Lastschriften vom Zahlungsempfänger (Händler) ausgelöst werden. Das gilt auch für Lastschriften im Internet, wenn bei der elektronischen Erteilung des Lastschriftmandats der Zahlungsdienstleister des Zahlers nicht eingebunden ist (vgl. die BaFin-Mitteilung vom 17. April 2019, abrufbar von der BaFin-Internetseite). Bei Lastschriftzahlungen hat es daher in Bezug auf die starke Kundenauthentifizierung keinen Umstellungsbedarf gegeben.

Kundinnen und Kunden können zudem über die Wahl des Zahlungsdienstleisters bzw. ihres Vertragspartners (dem Zahlungsempfänger) auch die verschiedenen Zahlmethoden bzw. die Verfahren der starken Kundenauthentifizierung auswählen.

Nach der Überprüfungsklausel in der PSD 2 wird die Europäische Kommission die Anwendung der PSD 2 und deren Auswirkungen evaluieren.

Mit freundlichen Grüßen

Sarah Rychlik