1. Jg. | 27.2.2020 | Seiten 1–72 | www.rdz-online.de

Erstausgabe

Recht der Zahlungsdienste

1. 2020

Betriebs-Berater Geldverkehr

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Invisible Payments – aufsichtsrechtliche Einordnung von interaktionslosen Zahlungsprozessen

In vielen Bereichen des täglichen Lebens können Zahlungen zukünftig vollständig automatisch abgewickelt werden. Der Kunde wird dabei keinen aktiven Zahlungsvorgang mehr durchlaufen müssen: Neue Zahlungsverfahren ermöglichen es vielmehr, dass der Kunde Dienstleistungen in Anspruch nehmen oder sich Waren aneignen kann, während die entsprechenden Zahlungsprozesse unsichtbar im Hintergrund ablaufen. Der nachfolgende Beitrag gibt einen Überblick über die aufsichtsrechtlichen Rahmenbedingungen von sog. Invisible Payments und untersucht die rechtlichen und praktischen Umsetzungsmöglichkeiten in unterschiedlichen Konstellationen. Er richtet sich sowohl an rechtswissenschaftlich interessierte Leser als auch an praktische Anwender von Zahlungslösungen.

Alexander Gebhard, LL.M. (London), RA, und Jonas Sturies, RA

I. Einleitung

Das Internet war der realen Welt lange Zeit voraus, wenn es um die Schnelligkeit und Bequemlichkeit von Zahlungsvorgängen geht. Sog. One-Click Payments, d. h. Online-Transaktionen, bei denen Bestell- und Zahlungsvorgang durch einen einzigen Klick ausgelöst werden, sind in vielen Bereichen mittlerweile zum Standard geworden. Auch im Präsenzgeschäft (point of sale – POS) haben sich abseits des Bargelds Zahlungsmethoden entwickelt, die den Zahlungsvorgang möglichst bequem und friktionslos ablaufen lassen. Für POS-Zahlungen haben sich hier insbes. Mobile-Payment-Verfahren etabliert,[1] bei denen der Zahlungsauftrag durch ein mobiles mit Near-Field-Communication- (NFC-)Controller ausgestattetes Endgerät ausgelöst wird.[2] All diesen Zahlungsmethoden ist jedoch gemein, dass die Zahlung vom Zahler separat und aktiv ausgelöst werden muss. Ausgerechnet die reale Welt könnte nun die Vorreiterrolle für Zahlungsmethoden einnehmen, bei denen auch dieser letzte Akt der aktiven Interaktion zukünftig der Vergangenheit angehört. Den logisch nächsten Schritt stellt insoweit die vermehrte Auslösung von Zahlungsvorgängen durch die bloße Inanspruchnahme von Leistungen dar.[3]

Die Idee hinter der „unsichtbaren" Auslösung von Zahlungsvorgängen (invisible payments) ist es, den Zahlungsvorgang vollständig im Hintergrund ablaufen zu lassen, ohne dass es einer aktiven Handlung des Zahlers bedarf. Der Grundgedanke findet sich schon bei klassischen Abonnement-Modellen. Während bei diesen typischerweise auf Grund einer einmal erfolgten Zustimmung des Zahlers zur Kontenbelastung regelmäßig erbrachte, gleichartige Hauptleistungen erfolgen, kommen jetzt Modelle auf, bei denen die Zahlung automatisch erst in Folge der Inanspruchnahme der Hauptleistung ausgelöst wird und es zukünftig also keines konkreten Check-Out-Verfahrens mehr bedarf. Diese Verfahren funktionieren im Grundsatz gleichermaßen am POS wie auch für Fernzahlungsvorgänge, wobei sich hier in den Details der Umsetzung Unterschiede ergeben können.

1. Automatisierung im Einzelhandel

Naheliegend sind zunächst Modelle im Einzelhandel: Ein noch relativ neues Beispiel sind hier Supermärkte in den USA, in welchen man sich an einem Eingangsportal mittels Smartphone ausweist und danach die in den Regalen liegenden Produkte herausnehmen und ohne Weiteres den Laden verlassen kann. Kameras und Sensoren liefern Daten an einen lernenden Algorithmus, der erkennt, welche Waren aus dem Regal genommen wurden. Die Bezahlung wird mit Verlassen des Ladens für die vom Kunden mitgenommenen Produkte automatisch über einen auf dem Smartphone des Kunden hinterlegten Account ausgeführt.

2. Flexible Abrechnung von Leistungen

Im Bereich Mobilität sticht zum einen die Entwicklung neuer Möglichkeiten zur Zahlungsauslösung aus dem Kraftfahrzeug

1 Vgl. hierzu auch *Pratz/Michna*, Digital Payments – Revolution im Zahlungsverkehr, 2016, S. 155, 159; s. a. Deutsche Bundesbank, Zahlungsverhalten in Deutschland 2017, abrufbar unter https://www.bundesbank.de/resource/blob/634056/8e22ddcd69de76ff40078b31119704db/mL/zahlungsverhalten-in-deutschland-2017-data.pdf (Abruf: 14.1.2020), S. 21, 26; Deutsche Bundesbank, Der Zahlungsverkehr der Zukunft – wohin bewegen sich Deutschland und Europa?, 7.2.2019, abrufbar unter https://www.bundesbank.de/de/presse/reden/der-zahlungsverkehr-der-zukunft-wohin-bewegen-sich-deutschland-und-europa–776224 (Abruf: 14.1.2020).

2 *Harman*, BKR 2018, 457,459; *Danwerth*, ZB 2015, 119, 121.

3 Ein Abriss zur historischen Entwicklung von Geldübertragungsmechanismen findet sich bei *Omlor*, ZIP 2016, 558, 559.

heraus.[4] Zum anderen zeigt die Abrechnung der Inanspruchnahme von Carsharing-Fahrzeugen oder E-Scootern Vorteile der inzwischen technisch möglichen entformalisierten Zahlungsauslösungsverfahren, welche diesen kulturell Akzeptanz verschaffen werden und eine Ausweitung auch auf weitere Branchen absehbar machen:

Während beim Erwerb von Waren nach wie vor einzelne Waren oder Warenkörbe abgerechnet werden, lässt sich bei der Inanspruchnahme von Dienstleistungen die Struktur von Abrechnungen neu gestalten. Durch die genaue Erfassung des Umfangs der Inanspruchnahme einer Dienstleistung kann die Abrechnung auf die tatsächlich in Anspruch genommene Leistung zugeschnitten werden. Sharing-Modelle zur Vermietung von E-Scootern und Mietwagen etwa sehen bereits die Möglichkeit der minutengenauen Abrechnung der Miete vor – nicht an einen vorher festgelegten Zeitraum, sondern flexibel an die tatsächliche Nutzungsdauer angepasst.[5] Entsprechend könnte etwa auch der Preis für die Nutzung öffentlicher Verkehrsmittel an die tatsächlich zurückgelegte Strecke angepasst werden oder der Preis für Online-Publikationen an z. B. die tatsächlich gelesenen Seiten.[6] Auch wenn die Identifizierung des Kunden über das Smartphone als besonders nutzerfreundlich angesehen wird,[7] muss diese natürlich nicht zwingend über eine App bzw. das Smartphone ablaufen. Insbes. biometrische Verfahren, wie Gesichtserkennung oder Scan des Fingerabdrucks, können den Kunden eindeutig zu allen nachfolgenden Handlungen zuordnen. Hierbei gilt die Identifizierung über den Fingerabdruck und den Iris-Scan als besonders sicher.[8]

Dieser Aufsatz untersucht die Umsetzbarkeit und die aufsichtsrechtlichen Anforderungen an Invisible Payments anhand unterschiedlicher Anwendungsbeispiele.[9]

II. Grundlagen interaktionsloser Zahlungsprozesse

Aus zivilrechtlicher Sicht sind grundsätzlich mehrere Rechtsgeschäfte voneinander zu unterscheiden: Erstens ist ein schuldrechtlicher Vertrag hinsichtlich des Erwerbs einer Ware oder Dienstleistung erforderlich, zweitens – im Falle eines Kaufvertrags – ein dinglicher Erfüllungsvertrag gerichtet auf die Übereignung der Waren, drittens ein dinglicher Erfüllungsvertrag gerichtet auf Übereignung eines Geldbetrags in Höhe des Kaufpreises vom Kunden an den Zahlungsempfänger.

Wichtig für die Durchführbarkeit von Invisible Payments ist dabei die rechtliche Möglichkeit, dass alle drei Geschäfte zur selben Zeit abgeschlossen werden können. Erforderlich ist, die jeweils zugrundeliegenden Willenserklärungen an bestimmte Handlungen anzuknüpfen. Im Bereich von POS-Zahlungen im Retail-Bereich können etwa Ladenbetreiber und Kunde vereinbaren, dass mit Verlassen des Ladens durch den Kunden sowohl ein Kaufvertrag zwischen beiden hinsichtlich der vom Kunden eingepackten Waren zustande kommt, als auch, dass das Eigentum an diesen Waren auf den Kunden übergeht sowie im Ergebnis die Zahlung des Kaufpreises erfolgt. Der Inhalt einer entsprechenden Vereinbarung kann sich aus Allgemeinen AGB ergeben (s. Abschn. III. 4.).

Da der Leistungsaustausch bei Invisible-Payment-Geschäften typischerweise nicht Zug-um-Zug abgewickelt wird, stellt sich für den Zahlungsempfänger in besonderem Maße die Frage nach der Sicherheit, die geschuldete Geldzahlung auch tatsächlich zu erhalten. Dies hängt in entscheidendem Maße von der Auswahl des zugrundeliegenden Zahlungsverfahrens ab (s. Abschn. III. 3.). Ein wesentliches Grundprinzip von Invisible Payments ist zudem, dass in irgendeiner Form das Verhalten des Kunden überwacht wird – sei es etwa durch visuelle Erfassung des Kunden selbst, GPS-Überwachung des Standorts oder die Erfassung des Aufrufens von IP-Adressen.

III. Rechtliche Einordnung

Aus aufsichtsrechtlicher Sicht ist die Ausgestaltung von Invisible Payments insbes. mit den Vorgaben des Zahlungsdiensteaufsichtsgesetzes (ZAG) in Einklang zu bringen (hierzu Abschn. III. 1.). Die aufsichtsrechtliche Einordnung hängt dabei auch von der Auswahl der zugrundezulegenden Zahlungsmethode ab – und diese Auswahl wiederum von zivilrechtlichen Erwägungen (hierzu Abschn. III. 2.). Eine lösbare Herausforderung stellt die Einhaltung der in § 55 ZAG sowie den in den auf Grundlage der Payment Services Directive II (PSD II)[10] erlassenen tech-

4 Hierzu ausführlich *Linardatos*, RdZ 2020, 36 ff., und *Korschinowski*, RdZ 2020, 66 ff. (beide in diesem Heft).

5 Gemäß den Allgemeinen Geschäftsbedingungen (AGB) der Fahrzeugvermieter verpflichtet sich der Kunde vor Fahrtantritt zur Zahlung der jeweiligen Miete. Die jeweils geltenden Endpreise und Gebühren für den Einzelmietvertrag gemäß der gültigen Tarif- und Kostenordnung werden dem Kunden vor Abschluss eines Einzelmietvertrags inklusive der gesetzlich vorgeschriebenen Umsatzsteuer auf dem Smartphone angezeigt. Die Zahlung ist mit Beendigung des Einzelmietvertrags fällig und wird mit Abstellen des Fahrzeugs dem Kunden automatisch in Rechnung gestellt und ihm entsprechend seiner hinterlegten Zahlungsmethode belastet.

6 Vgl. zum Thema der blockchainbasierten Nanopayments auch *Omlor*, MMR 2018, 428.

7 PwC, Biometrische Identifizierungsverfahren, abrufbar unter www.pwc.de/de/Finanzdienstleistungen/pwc-biometrische-Authentifizierungverfahren.pdf (Abruf: 14.1.2020).

8 Bitcom, Jeder Zweite würde per Iris-Scan Zahlungen bestätigen, 25.2.2019, abrufbar unter www.bitkom.org/Presse/Presseinformation/Jeder-Zweite-wuerde-Iris-Scan-Zahlungen-bestaetigen (Abruf: 14.1.2020).

9 Zu den zivilrechtlichen Fragen spezifisch im Zusammenhang mit Invisible Payments am Beispiel von In-Car-Payments s. *Linardatos* (Fn. 4), 36–38.

10 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, ABlEU vom 23.12.2015, L 337, 35.

nischen Regulierungsstandards[11] enthaltenen Vorgaben für die Anforderungen an die starke Kundenauthentifizierung bei Zahlungsauslösung dar (hierzu Abschn. III. 3. und 4.).

1. Einordnung relevanter am Zahlungsprozess beteiligter Akteure in aufsichtsrechtliche Kategorien

Sofern sich Invisible-Payment-Modelle bereits abzeichnen, kann eine erste Zuordnung zu den aufsichtsrechtlichen Tatbeständen vorgenommen werden:

a) Zahlungsdienstnutzer

Mit Blick auf den Kunden als Zahlungsdienstnutzer ist zunächst zu unterscheiden, welches konkrete Zahlungsverfahren dieser nutzt und in welcher Form er Zahlungen initiiert. Relevant für den Bereich von Invisible Payments sind insoweit (elektronische) Nah- sowie (elektronische) Fernzahlungen.

Als elektronische Nahzahlungen (auch proximity payments) werden solche Zahlungen am POS verstanden, die typischerweise per NFC- oder (QR-)Code-Verfahren ausgelöst werden, wobei sowohl die stationäre Kasse im Geschäft selbst als auch das Smartphone/mobile Endgerät eines Kunden zur Zahlung verwendet wird.[12] Hierbei kommen sowohl Lastschriftverfahren (§ 1 Abs. 1 S. 2 Nr. 3a ZAG) als auch Überweisungen (§ 1 Abs. 1 S. 2 Nr. 3c ZAG) in Betracht. Sofern eine Debitkarte oder Kreditkarte für Proximity Payments verwendet wird, liegt ein Zahlungskartengeschäft nach § 1 Abs. 1 S. 2 Nr. 3b ZAG vor. Der Zahler schließt zuvor einen Zahlungsdiensterahmenvertrag mit dem Anbieter des Mobile Payment (Zahlungsinstitut oder Mobilfunkprovider, § 675f Abs. 2 BGB). Der über das Internet oder das mobile Endgerät ausgelöste Zahlungsvorgang stellt einen Zahlungsauftrag des Zahlers dar (§ 675f Abs. 4 S. 2 BGB). Typischerweise liegt hierin zugleich auch eine Autorisierung i. S. v. § 675j BGB.[13] Die Zahlungssysteme des Mobile Payment greifen sodann z. B. auf das Lastschriftverfahren, die Kartenzahlung einschließlich der Girocard oder Systeme des E-Gelds zurück.

Bei einem elektronischen Fernzahlungsvorgang (remote payments, § 1 Abs. 19 ZAG) wird der Zahlungsvorgang räumlich getrennt von dem erworbenen Gut oder der erworbenen Dienstleistung durch Dateneingabe über das Internet oder mittels eines Geräts, das für die Fernkommunikation verwendet werden kann, ausgelöst. Der aufsichtsrechtlich relevante Unterschied zu Nahzahlungen besteht insbes. darin, dass in diesem Fall die starke Kundenauthentifizierung nach § 55 Abs. 2 ZAG Elemente zu umfassen hat, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen (s. Abschn. IV. 4. b) bb) (8)).

b) Zahlungsdienstleister

Die Einordnung der an einem Invisible-Payment-Prozess beteiligten Zahlungsdienstleister hängt davon ab, mittels welcher Zahlungsmethode der interaktionslos ausgelöste Zahlungsprozess letztlich abgewickelt wird. Traditionelle zahlungsaufsichtsrechtliche Kategorien müssen dabei mit dem Wandel schritthalten, dem die Zahlungsabwicklung in der Praxis unterworfen ist. Durch die PSD II ist das ZAG dabei bereits teilweise auf eine Zukunft vorbereitet worden, in welcher Zahlungen ohne Verwendung einer Chipkarte, eines Smartphone, einer Smartwatch o. Ä. ausgelöst werden: In der auf die Regulierung von Händlerbanken (acquirern) zielenden Norm (jetzt § 1 Abs. 1 S. 2 Nr. 5 Var. 2 i. V. m. Abs. 35 S. 1 ZAG) wurde die Bezugnahme auf Zahlungsauslösung „mit Zahlungsauthentifizierungsinstrumenten“ gestrichen. Annahme und Abrechnung von Zahlungsvorgängen unterliegen nunmehr auch dann als Akquisitionsgeschäft dem ZAG, wenn diese sich auf Zahlungsvorgänge beziehen, welche ohne Authentifizierungsinstrument – d. h. invisible – ausgelöst werden. Mit Verbreitung von interaktionslosen Zahlungsauslösungsmechanismen werden möglicherweise auch Anpassungen an den Tatbeständen Zahlungskartengeschäft (§ 1 Abs. 1 S. 2 Nr. 3 b ZAG) und Ausgabe von Zahlungsinstrumenten (§ 1 Abs. 1 S. 2 Nr. 5 Var. 1 ZAG) erforderlich – jedenfalls sofern die entsprechenden Dienstleister nicht ohnehin über den generalklauselartig weit ausgestalteten Tatbestand Finanztransfergeschäft (§ 1 Abs. 1 S. 2 Nr. 6 ZAG) erfasst sind.

c) Zahlungsempfänger

Aufsichtsrechtlich unproblematisch ist i. d. R. die Rolle des Zahlungsempfängers. Der stationäre Händler oder Dienstleister, der einen Zahlungsdienst für die Erfüllung seiner Forderung nutzt, erbringt i. d. R. nicht selbst erlaubnispflichtige Zahlungsdienste – es sei denn, er führt Zahlungen, autorisiert durch den Kunden, ausnahmsweise selbst aus.

d) Rolle des technischen Infrastrukturdienstleisters (§ 58a n. F. ZAG)

Relevant für die Umsetzung von Invisible-Payment-Modellen dürfte der im Rahmen des Gesetzes zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie[14] neu in das ZAG eingefügte § 58a zur Regulierung sog. Systemunternehmen

11 Delegierte Verordnung (EU) 2018/389 vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation, ABlEU vom 13.3.2018, L 69, 23.

12 *Herresthal*, in: K. Schmidt (Hrsg.), Münchener Kommentar zum HGB, Bd. 6, 4. Aufl. 2019, Rn. 79, 80; *Söbbing*, WM 2016, 1066, 1067.

13 *Omlor*, in: Staudinger, BGB, 2020, § 675f, Rn. 147.

14 Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie vom 12. Dezember 2019, BGBl. I 2019, 2602 ff.

werden. Wie auch der Tatbestand des technischen Dienstleisters i. S. d. § 2 Abs. 1 Nr. 9 ZAG steht § 58a ZAG nach der Gesetzesbegründung in einem Exklusivitätsverhältnis zu den Zahlungsauslöse- oder Kontoinformationsdiensten i. S. d. § 1 Abs. 1 S. 2 Nr. 7, 8 ZAG. Die Vorschrift soll den Zugang zu technischen Schnittstellen ermöglichen, die von Bedeutung für das Erbringen von Zahlungsdiensten oder das Betreiben des E-Geld-Geschäfts sind.[15] Hiermit sind insbesondere die Schnittstelle für die kontaktlose Kommunikation mit dem mobilen Endgerät bei Bezahlvorgängen am POS (NFC-Schnittstelle) oder für Audio- bzw. Pay-Per-Voice-Anwendungen gemeint. Damit versucht die Regelung, das Spannungsfeld zwischen Zahlungsdienstleistern und Telekommunikationsanbietern zu entschärfen, welches im Bereich Mobile Payment existiert. Zugang zu technischen Schnittstellen eines Systemunternehmens ermöglicht zunächst die Entwicklung von Mobile-Payment-Lösungen durch Drittunternehmen (hier wird jedoch der Vorsprung der Systemunternehmen hinsichtlich Marktdurchdringung schwer einzuholen sein), im nächsten Schritt möglicherweise aber auch die Entwicklung etwa von smartphone-/geotrackingbasierten Invisible-Payment-Modellen. Inwieweit der Begriff des Systemunternehmens nach § 58a ZAG mit dem sehr weiten Anwendungsbereich des technischen Dienstleisters i. S. d. § 2 Abs. 1 Nr. 9 ZAG gleichzusetzen ist, ist jedoch bislang ungeklärt.

e) Zahlungsauslösedienste (§ 1 Abs. 1 S. 2 Nr. 7 ZAG i.V.m. § 1 Abs. 33 ZAG)

Unter den mit Umsetzung der PSD II eingeführten Tatbestand des Zahlungsauslösedienst fallen nach § 1 Abs. 1 S. 2 Nr. 7 ZAG i.V.m. § 1 Abs. 33 ZAG Dienste, bei denen auf Veranlassung des Nutzers ein Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto ausgelöst wird.[16] Dabei nimmt der Zahlungsauslösedienstleister eine Vermittlerposition zwischen dem Nutzer und dem kontoführenden Zahlungsinstitut ein.[17] Anders als Abonnement-Dienste, die häufig das Lastschriftverfahren nutzen, besteht hier zwar der Vorteil, dass der Zahlungsempfänger unmittelbar Gewissheit über die Erteilung des Zahlungsauftrags hat.[18] Denn über den Zahlungsauslösedienstleister wird grundsätzlich eine Überweisung ausgelöst, welche im Gegensatz zu Lastschriftverfahren keinem Erstattungsanspruch unterliegt (zum Erstattungsanspruch nach § 675x Abs. 2 BGB s. Abschn. III. 2. a)).

Insoweit wäre die Einschaltung eines Zahlungsauslösedienstleisters grundsätzlich gut geeignet, um Invisible Payments auf Grundlage von Überweisungen abzubilden. Zu beachten ist jedoch, dass der BGH es unter Verweis auf § 312a Abs. 4 BGB für unzulässig erachtet hat, als einzige entgeltfreie Zahlungsmöglichkeit die Zahlung unter Zuhilfenahme von Zahlungsauslösediensten anzubieten.[19] Daher kann ein Zahlungssystem unter Einschaltung eines Zahlungsauslösediensts immer nur zusammen mit einer weiteren Zahlungsmethode angeboten werden.

2. Auswahl der zugrundeliegenden Zahlungsmethode

Der Unterschied zwischen Invisible Payments und anderen Zahlungsmethoden liegt allein im Front-End, d. h. der Art und Weise, wie der Kunde den Zahlungsauftrag gegenüber dem Zahlungsdienstleister erteilt. Diese wird grundsätzlich im sog. Zahlungsdiensterahmenvertrag zwischen Kunde und Zahlungsdienstleister vereinbart. Durch bloße Inanspruchnahme von Leistungen ausgelöste Zahlungsvorgänge können daher grundsätzlich über alle klassischen Formen der Zahlungsabwicklung durchgeführt werden. Für die bargeldlose, elektronische Erfüllung der Zahlungsverpflichtung der Kunden bieten sich insbesondere folgende Zahlungswege: (i) Zahlung per Überweisung, (ii) Zahlung per Lastschrift, (iii) Zahlung per Kreditkarte/Kreditkarteninformationen, (iv) Zahlung mit E-Geld, (v) Abrechnung über die Mobilfunkrechnung und (vi) Zahlung über Wallets. Für die Auswahl des zugrundeliegenden Zahlungsmittels dürfte aus Sicht des Zahlungsempfängers neben den mit dem Zahlungsinstrument verbundenen Kosten entscheidend sein, ob er im Zeitpunkt der Erteilung des Zahlungsauftrags Gewissheit über die Erfüllung seines Anspruchs hat und wieviel Flexibilität das Zahlungsinstrument bei der Ausführung des Zahlungsauftrags bietet.

a) Überweisung/Lastschrift

Die kostengünstigsten Varianten dürften hierbei die Zahlung per Überweisung und die Zahlung per Lastschrift sein. Gem. § 1 Abs. 21 ZAG ist eine Lastschrift ein Zahlungsvorgang zur Belastung des Zahlungskontos des Zahlers, bei dem der Zahlungsvorgang vom Zahlungsempfänger aufgrund der Zustimmung des Zahlers gegenüber dem Zahlungsempfänger, dessen Zahlungsdienstleister oder seinem eigenen Zahlungsdienstleister ausgelöst wird. Zwar bieten Lastschriften in Bezug auf die Anforderungen der starken Kundenauthentifizierung Erleichterungen (s. Abschn. III. 4. b) bb) (1)). Lastschriftverfahren haben jedoch wegen des zwingenden gesetzlichen Erstattungsanspruchs nach § 675x Abs. 2 BGB bei Verbrauchern regelmäßig den entscheidenden Nachteil, dass der Zahlungsempfänger im Zeitpunkt der Erteilung des Zahlungsauftrags keine Gewissheit über die Erfüllung erhält.[20] Lediglich

15 BT-Drs. 19/15196, 53.
16 BT-Drs. 18/11495, 107; vgl. auch *Omlor*, FinTech-Handbuch 2019, S. 141; *Zahrte*, NJW 2018, 337, 338.
17 *Omlor*, JuS 2019, 289; *Harman* (Fn. 2), 460.
18 *Omlor* (Fn. 17), Rn. 11.
19 Dies gilt jedenfalls, solange dies einem erheblichen Teil der Kunden ein vertragswidriges Verhalten abverlangt, weil Banken AGB verbreitet die Weitergabe von Bankdaten seitens Kunden an Zahlungsauslösedienste untersagen: BGH, 18.7.2017 – KZR 39/16, BB 2017, 2575, zur „Sofortüberweisung" als einzige Zahlungsmöglichkeit im Onlineshop.
20 *Zahrte* (Fn. 16), 341.

gegenüber Unternehmern lässt sich dieser Anspruch ausschließen (§ 675e Abs. 4 BGB), damit kommen Lastschriftverfahren letztlich nur in Modellen mit Corporate-Kunden in Betracht. Gleiches gilt in Bezug auf die Überweisung. Zwar sind Überweisungen nach Erteilung des Überweisungsauftrags im Gegensatz zur Lastschrift nicht mehr widerruflich (§ 675p Abs. 1 BGB), jedoch gilt auch hier, dass der Zahlungsempfänger im Zeitpunkt der Erteilung des Überweisungsauftrags keine Garantie für die Erfüllung seines Zahlungsanspruchs hat. Zudem sind Invisible Payments gerade dann interessant, wenn der konkrete Zahlungsbetrag zum Zeitpunkt der Erteilung des Zahlungsauftrags flexibel ist und nicht konkret vorab mitgeteilt werden muss, was jedoch Voraussetzung für die Zahlung per Überweisung ist.

b) Kreditkarte

Mit Blick auf das Vorstehende dürften Zahlungen per Kreditkarte die bevorzugte Methode darstellen. Bei Auslösung einer autorisierten Kartenzahlung steht dem Zahlungsdienstleister nach § 675x Abs. 1 S. 1 BGB auch dann ein Erstattungsanspruch gegen den Zahler zu, wenn der konkrete Zahlungsbetrag dabei nicht angegeben wird. Abseits hiervon kommen zudem auch andere Formen des digitalen Zahlungsverkehrs in Betracht, etwa blockchainbasierte Zahlungsmittel.[21]

3. Auslösung des Zahlungsvorgangs

Die Auslösung eines Zahlungsvorgangs setzt die Erteilung eines Zahlungsauftrags voraus (§ 675f Abs. 4 S. 2 BGB). Als empfangsbedürftige Willenserklärung setzt der Zahlungsauftrag damit eine Erklärungshandlung des Zahlers gegenüber dem Zahlungsdienstleister voraus.[22] Ein Zahlungsvorgang ist gegenüber dem Zahler darüber hinaus nur wirksam, wenn der Zahler diesen autorisiert, d. h. diesem zugestimmt hat. Nur in diesem Fall steht dem Zahlungsdienstleister ein Erstattungsanspruch nach §§ 675c Abs. 1, 670 BGB gegen den Zahler für die Ausführung des Zahlungsauftrags zu. Die Zustimmung kann entweder als Einwilligung oder, sofern zwischen dem Zahler und seinem Zahlungsdienstleister zuvor vereinbart, als Genehmigung erteilt werden. Art und Weise der Erteilung des Zahlungsauftrags sowie Art und Weise der Zustimmung (§ 675j Abs.1 S. 3 BGB) können zwischen dem Zahler und seinem Zahlungsdienstleister im Zahlungsdiensterahmenvertrag vereinbart werden. In diesem Zusammenhang kann vereinbart werden, dass auch ein bestimmtes schlüssiges Verhalten für die Erklärung (und Autorisierung) des Zahlungsauftrags genügt. Hierbei wird regelmäßig eine einzige Erklärung für Erteilung und Autorisierung des Zahlungsvorgangs ausreichen.[23] Eine solche schlüssige Handlung kann etwa im Verlassen eines Shop mitsamt den erworbenen Waren liegen, in der Nutzung eines öffentlichen Verkehrsmittels oder in dem Aufrufen einer bestimmten Internetseite. Entscheidend ist insoweit aus Sicht des Zahlungsempfängers, dass die Handlung konkret genug beschrieben und vereinbart ist, um ihr den gewünschten Erklärungsgehalt zuzumessen.

Insbes. kann vereinbart werden, dass die Zustimmung mittels eines bestimmten Zahlungsinstruments erteilt werden kann (§ 675j Abs. 1 S. 4 BGB). Zahlungsinstrument ist dabei jedes personalisierte Instrument oder Verfahren, dessen Verwendung zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister vereinbart wurde und das zur Erteilung eines Zahlungsauftrags verwendet wird (§ 1 Abs. 20 ZAG). Der Auftrag kann dabei also entweder durch den Kunden (etwa über die Smartphone App), über den Zahlungsempfänger oder (alternativ) über einen Zahlungsauslösedienst ausgelöst werden, der den Zahlungsauftrag des Kunden zur Zahlung des Kaufpreises an die Zahlstelle übermittelt. Zwar kann die Zustimmung vom Zahler durch Erklärung gegenüber dem Zahlungsdienstleister so lange widerrufen werden, wie der Zahlungsauftrag dem Zahlungsdienstleister des Zahlers nicht zugegangen ist. Gibt der Kunde als Zahler den Zahlungsauftrag aber unmittelbar schlüssig ab (z. B. durch Verlassen des Shop), welcher seinen Zahlungsdienstleister elektronisch wenige Sekunden später erreicht, so ist ein Widerruf nicht mehr möglich.

Wählt man zur Erfüllung der Zahlungspflicht die Variante der Überweisung (insbes. unter Einschaltung eines Zahlungsauslösediensts, vgl. Abschn. III. 1. e)), so muss der Zahlungsmechanismus so gestaltet sein, dass der Kunde seinem kontoführenden Zahlungsdienstleister (Zahlstelle) mit Vornahme der entsprechenden schlüssigen Handlung einen Zahlungsauftrag dahingehend erteilt, einen Betrag in Höhe des jeweiligen Kaufpreises an den Zahlungsempfänger zu überweisen.

Wählt man zur Erfüllung die Variante des Lastschriftmandats oder der Kartenzahlung, so kann der POS der Zahlstelle des Kunden den Zahlungsauftrag zur Zahlung des Kaufpreises für die vom Kunden genommenen Sachen (oder in Anspruch genommenen Leistungen) aufgrund eines Lastschriftmandats bzw. einer autorisierten Kartenzahlung selbst erteilen und so die Zahlung auslösen, sobald der Kunde die im Zahlungsdiensterahmenvertrag vereinbarte Handlung vornimmt, also etwa den Laden verlässt.

4. Kundenauthentifizierung und Ausnahmen – Anwendbarkeit auf verschiedene Geschäftsmodelle

a) Zuordnung der in Anspruch genommenen Leistung zum jeweiligen Kunden

Unabhängig von der aufsichtsrechtlichen Pflicht zur Authentifizierung des Zahlers ist zunächst erforderlich, die in Anspruch ge-

21 Vgl. hierzu *Omlor* (Fn. 17).
22 *Zahrte*, BKR 2016, 315, 316; s. auch *Linardatos* (Fn. 4), 36, 38.
23 *Omlor*, BKR 2019, 105, 108.

nommene Leistung dem jeweiligen Kunden zuzuordnen. Zur Identifizierung sind verschiedenen Methoden in Erprobung. Zunächst können Kunden über die Lokalisation ihres Smartphones identifiziert werden. Noch unmittelbarer ist die Identifikation mittels biometrischer Verfahren, wie Sprach- und Gesichtserkennung oder Scan des Fingerabdrucks. Zahlungsinstrumente können grundsätzlich technologieneutral mit verschiedenen biometrischen Erkennungsverfahren kombiniert werden.[24] Von entscheidender Bedeutung für die Auswahl des biometrischen Verfahrens sind insbesondere die Sicherheit des Verfahrens sowie die Akzeptanz durch den Kunden. Als wenig sicher gilt die Stimmerkennung (pay per voice), da es technisch vergleichsweise einfach ist, Stimmproben mit hoher Qualität aufzuzeichnen. Zudem dürfte es jedenfalls im öffentlichen Raum schwierig sein, Stimmmuster eindeutig zuzuordnen.[25] Demgegenüber gelten die Identifizierung über den Fingerabdruck, den Iris-Scan und die Gesichtserkennung als besonders sicher und kundenfreundlich.[26] Anbieter in China erlauben etwa Zahlungsauslösung am POS Terminal per Gesichtserkennung – wird diese Gesichtserkennung nicht mehr erst am Terminal ausgeführt, erfolgt die Zahlungsauslösung gänzlich im Hintergrund, d. h. „invisible".

b) Aufsichtsrechtliche Vorgaben

Aufsichtsrechtlich ist der Zahlungsdienstleister verpflichtet, eine starke Kundenauthentifizierung durchzuführen, wenn der Zahler (i) online auf ein Konto zugreift (§ 55 Abs. 1 Nr. 1 ZAG), (ii) elektronisch einen Zahlungsvorgang auslöst (§ 55 Abs. 1 Nr. 2 ZAG) oder (iii) sonst über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehrs oder anderen Missbrauchs beinhaltet (§ 55 Abs. 1 Nr. 3 ZAG). Diese muss zwei der drei Elemente des Wissens (etwas, das der Nutzer weiß), des Besitzes (etwas, das der Nutzer besitzt) und der Inhärenz (etwas, das der Nutzer ist) umfassen.[27] Bei Kartenzahlungen etwa werden die Anforderungen des Besitzes und des Wissens dadurch erfüllt, dass der Nutzer die Karte besitzt und seine PIN-Nummer in das Terminal am POS eingibt.

Wie aber passt das angestrebte Schutzniveau durch Einführung der starken Kundenauthentifizierung zu der Idee eines völlig interaktionslosen Zahlungsvorgangs? Invisible Payments lassen sich nur dann sinnvoll umsetzen, wenn entweder auch der Prozess der Kundenauthentifizierung unsichtbar abläuft oder aber aufgrund des Vorliegens einer der gesetzlichen Ausnahmen von der Pflicht zur starken Kundenauthentifizierung nicht durchgeführt werden muss.

aa) Kundenauthentifizierung im Hintergrund

Die Durchführung einer starken Kundenauthentifizierung lässt sich nur dann mit dem Prinzip von Invisible Payments vereinbaren, wenn auch diese ohne aktive Handlung innerhalb des eigentlichen Zahlungsprozesses abläuft. Soll ein Zahlungsvorgang, ohne dass es neben der Inanspruchnahme der Leistung einer weiteren aktiven Handlung des Nutzers zur Auslösung des Zahlungsvorgangs bedarf, ausgelöst werden, scheidet eine Kundenauthentifizierung mittels eines Elements des Wissens aus. Denkbar ist jedoch eine Kundenauthentifizierung mittels Besitz und Inhärenz, etwa anhand eines NFC-fähigen Gegenstands, den der Kunde bei sich trägt (z. B. ein Smartphone), in Kombination mit einem biometrischen Element (z. B. Gesichtserkennung).

bb) Ausnahmen von den Vorschriften zur starken Kundenauthentifizierung

Unter bestimmten Voraussetzungen können Zahlungsdienstleister auch auf eine der Ausnahmen zur starken Kundenauthentifizierung zurückgreifen. Die Anforderungen an die konkrete Ausgestaltung der starken Kundenauthentifizierung sowie Ausnahmen sind in dem auf Grundlage von Art. 98 PSD II erlassenen technischen Regulierungsstandard (RTS)[28] festgelegt. Gem. Art. 55 Abs. 5 ZAG i.V.m. den RTS kann die starke Kundenauthentifizierung insbesondere in bestimmten Fällen komplett entfallen, wenn nach der Verordnung einzuhaltende Überwachungspflichten hinsichtlich der abgewickelten Zahlungsvorgänge eingehalten werden.

(1) Lastschriftverfahren

Unabhängig von den gesetzlich ausdrücklich vorgesehenen Ausnahmen hat die BaFin in einem Hinweis für Verbraucher klargestellt, dass Lastschriftzahlungen im Internet i. d. R. keine starke Kundenauthentifizierung gem. § 55 Abs. 1 Nr. 3 ZAG voraussetzen. Der Zahler erteilt ein Lastschriftmandat nämlich lediglich gegenüber dem Zahlungsempfänger. Der Zahlungsdienstleister des Zahlers wird in den Zahlungsauslösungsvorgang nicht unmittelbar eingebunden und kann somit keine Kundenauthentifizierung durchführen. Auch die Zahlungsauslösung erfolgt ohne direkte Verbindung von Zahler und Zahlungsdienstleister, sondern über die entsprechende Aufforderung vom Zahlungsempfänger an den Zahlungsdienstleister. Eine unmittelbare Einbindung des Zahlungsdienstleisters durch den Zahler liegt lediglich im Falle einer Lastschrift durch E-Mandat des SEPA-Regelwerks vor.

24 BT-Drs. 18/11495, 110.
25 Vgl. zu den Anforderungen an das Endgerät bei Inhärenzelementen auch *Linardatos* (Fn. 4), 36, 40 ff.
26 S. PwC (Fn. 7) und Bitcom (Fn. 8).
27 Zu den Anforderungen an die starke Kundenauthentifizierung ausführlich *Omlor*, RdZ 2020, 20 ff. (in diesem Heft).
28 S. Delegierte Verordnung (EU) 2018/389 (Fn. 11).

(2) Kontaktlose Nahzahlungen und Kleinstbetragszahlungen

Von der Pflicht zur Durchführung einer starken Kundenauthentifizierung ausgenommen sind zudem bestimmte Kleinstbetragszahlungen. Hiervon umfasst sind nach Art. 11 RTS zunächst kontaktlose Nahzahlungen (z. B. mittels Smartphone oder NFC-fähiger Zahlungskarte am POS) bis zu einem Betrag von 50 Euro je Zahlung, sofern nicht mehr als fünf frühere kontaktlose Zahlungen erfolgt sind oder diese einen Betrag von 150 Euro überschreiten. Des Weiteren ausgenommen sind nach Art. 16 RTS Fernzahlungen bis zu einem Betrag von 30 Euro je Zahlung, sofern nicht mehr als fünf frühere kontaktlose Zahlungen erfolgt sind oder diese einen Betrag von 100 Euro überschreiten. Der Anwendungsbereich dieser Ausnahmen dürfte für reine Invisible-Payment-Prozesse eher begrenzt sein. Die Idee etwa von kassenlosen Shops oder der bloßen Inanspruchnahme von Leistungen – d. h. ein Erfüllungsprozess, der vollständig ohne Check-Out-Handlung auskommt – würde in der Praxis erheblich eingeschränkt werden, wenn in regelmäßigen Abständen gleichwohl Authentifizierungsverfahren durchzuführen wären.

(3) Transaktionsrisikoanalyse

Sofern durch eine Transaktionsrisikoanalyse sichergestellt ist, dass das konkrete Betrugsrisiko gering ist, kann nach Art. 18 RTS im Falle elektronischer Fernzahlungsvorgänge auf eine starke Kundenauthentifizierung ebenfalls verzichtet werden. Indizien für ein erhöhtes Risiko können Abweichungen vom üblichen Verhalten des Zahlers oder Ähnlichkeiten zu bekannten Betrugsmustern sein. Aufgrund des mit diesem Verfahren verbundenen hohen technischen Aufwands dürfte diese Ausnahme eher geringe praktische Relevanz für Invisible-Payment-Lösungen entfalten.

Für die Ausnahmeregelung entscheidend ist, dass bei dem individuellen Zahlungsdienstleister in der jeweiligen Kategorie von Zahlungen eine bestimmte Betrugsquote nicht überschritten werden darf. Die Höchstquoten für die einzelnen Kategorien von Zahlungen sind in den RTS festgelegt und hängen von der Höhe der Zahlungen ab, für die der betroffene Zahlungsdienstleister die Ausnahme nutzen will.[29]

(4) Wiederkehrende Zahlungsvorgänge

In Fällen wiederkehrender Zahlungsvorgänge müssen Zahlungsdienstleister nur bei der Erstellung, Änderung oder der erstmaligen Auslösung einer Serie wiederkehrender Zahlungsvorgänge (z. B. in Form von Daueraufträgen) mit demselben Zahlungsbetrag und demselben Zahlungsempfänger eine starke Kundenauthentifizierung durchführen. Diese Ausnahme ist mit der Situation bei klassischen Abonnements zu vergleichen. Im Umkehrschluss bedeutet dies, dass in diesen Fällen auch dann grundsätzlich nur eine initiale Kundenauthentifizierung erforderlich ist, wenn der Zahlung nur Lastschriftverfahren zugrunde liegen. Aus praktischer Sicht dürfte die Ausnahme für wiederkehrende Zahlungen eher begrenzte Wirkung haben, da diese aufgrund der Einschränkung auf denselben Zahlungsbetrag nur starr angewandt werden kann.

(5) Verkehrsnutzungsentgelte und Parkgebühren

Gem. Art. 12 RTS dürfen Zahlungsdienstleister unter Einhaltung der in Art. 2 RTS festgelegten Anforderungen von der Vorgabe einer starken Kundenauthentifizierung absehen, wenn der Zahler an einem unbeaufsichtigten Terminal einen elektronischen Zahlungsvorgang auslöst, um ein Verkehrsnutzungsentgelt oder eine Parkgebühr zu zahlen.[30] Diese Bereichsausnahme wird für den gesamten Bereich der In-Car-Payments von Bedeutung sein.[31]

(6) Whitelisting

Von erheblicher praktischer Bedeutung dürfte hingegen die Ausnahme des sog. Whitelisting sein. Nach Art. 13 RTS ist eine starke Kundenauthentifizierung nicht erforderlich, sofern die allgemeinen Anforderungen an die Authentifizierung erfüllt und der Zahlungsempfänger auf einer zuvor vom Zahler erstellten Liste vertrauenswürdiger Empfänger geführt wird. Bei der erstmaligen Erstellung oder der Erweiterung einer solchen Liste muss der Zahlungsdienstleister jeweils eine starke Kundenauthentifizierung durchführen. Einträge auf der Liste vertrauenswürdiger Empfänger dürfen dabei nicht – etwa auf Grundlage von AGB – durch den Zahlungsempfänger selbst vorgenommen werden, sondern müssen direkt vom Zahler gegenüber dem Zahlungsinstitut mitgeteilt werden. Zahlungen an einen gelisteten vertrauenswürdigen Empfänger können danach grundsätzlich ohne starke Kundenauthentifizierung durchgeführt werden. Das Element der Vertrauenswürdigkeit ist dabei rein formal zu betrachten, d. h. eine materielle Prüfung der Vertrauenswürdigkeit des Zahlungsempfängers durch den Zahlungsdienstleister findet nicht statt.[32]

Bei Betrachtung der Whitelisting-Ausnahme wird deutlich, dass die Anwendung dieser Ausnahme einerseits sehr effektiv ist, um die Pflicht zur Durchführung einer starken Kundenauthentifizierung zu vermeiden. Das Whitelisting wirkt insoweit zunächst dauerhaft und unabhängig von Betragsgrenzen oder der Anzahl von Einzelzahlungen. Zum anderen kann das Whitelisting sowohl im

29 Vgl. auch BaFin, Starke Kundenauthentifizierung: Neue Pflicht wirkt sich auf Online-Banking und Bezahlen im Internet aus, 15.6.2018, abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2018/fa_bj_1806_Starke_Kundenauthentifizierung.html (Abruf: 14.1.2020).

30 *Omlor* (Fn. 13), § 675v, Rn. 40.

31 Ausführlich zu den zahlungsdiensterechtlichen Fragen bei In-Car-Payments *Linardatos* (Fn. 4), 36, 38–40.

32 Ebenso *Omlor* (Fn. 27), 20, 25.

Bereich der POS-Zahlungen als auch im E-Commerce effektiv eingesetzt werden. Auf der anderen Seite bevorzugt das Whitelisting offenkundig große Händler bzw. Dienstleister. Es ist insoweit anzunehmen, dass Kunden einen Zahlungsempfänger nur dann aktiv und unter Anwendung der starken Kundenauthentifizierung auf eine Whitelist aufnehmen, wenn hinsichtlich dieses bestimmten Zahlungsempfängers zukünftig mit regelmäßigen Zahlungen zu rechnen ist und der Zahlungsempfänger auch im Übrigen zweifellos als vertrauenswürdig anzusehen ist. Für gelegentliche Einzeltransaktionen insbesondere an kleinere Einzelhändler dürfte dieses Verfahren hingegen an seine Grenzen stoßen.

(7) Dedizierte Zahlungsprozesse

Gem. Art. 17 RTS können Zahlungsdienstleister bei juristischen Personen, die elektronische Zahlungsvorgänge über dedizierte (d. h. eigens hierfür eingerichtete) Zahlungsprozesse oder -protokolle auslösen, die nur Zahlern zur Verfügung stehen, bei denen es sich nicht um Verbraucher handelt, von der Vorgabe einer starken Kundenauthentifizierung absehen, wenn die zuständigen Behörden der Auffassung sind, dass diese Prozesse oder Protokolle mindestens ein vergleichbares Sicherheitsniveau wie das in der PSD II vorgesehene gewährleisten. Diese Ausnahme dürfte für die breite Praxis von eher untergeordneter Bedeutung sein.

(8) Dynamische Verknüpfung bei elektronischen Fernzahlungsvorgängen

Handelt es sich bei dem ausgelösten elektronischen Zahlungsvorgang um einen elektronischen Fernzahlungsvorgang, d. h. um einen Zahlungsvorgang, bei dem nicht am POS gezahlt wird, hat der Zahlungsdienstleister eine starke Kundenauthentifizierung zu verlangen, die Elemente umfasst, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen. Das bedeutet, dass dem Zahler mitgeteilt werden muss, für welchen Betrag und welchen Zahlungsempfänger diese bestimmte Authentifizierung gelten soll. Jede Änderung der Zahlungsdaten würde die verwendete Authentifizierung ungültig machen.[33] Da im Bereich von Invisible Payments die Zahlungsauslösung bzw. Autorisierung typischerweise gerade ohne solche konkrete Bezugnahme auskommen soll, wird die Umsetzung von Invisible Payments bei elektronischen Fernzahlungen typischerweise nur dann in Betracht kommen, wenn die Pflicht zur Durchführung einer starken Kundenauthentifizierung durch Anwendung einer Ausnahme vollständig entfällt.

ZUSAMMENFASSUNG

1. Zahlungssysteme unterliegen intensivem technologischem Wandel. Im Rahmen der weiteren Entwicklung werden Modelle Verbreitung finden, bei denen neben der Inanspruchnahme der Leistung keine weitere Handlung des Nutzers zur Auslösung des Zahlungsvorgangs erforderlich ist.
2. Invisible-Payment-Lösungen können in vielen Bereichen am POS, in begrenztem Umfang auch im Bereich des E-Commerce eingesetzt werden. Die konkrete Umsetzung von Invisible-Payment-Prozessen, insbes. mit Blick auf die starke Kundenauthentifizierung bzw. die anwendbaren Ausnahmen, hängt vom jeweiligen Geschäftsmodell und einer Reihe von externen Faktoren ab. Hierzu gehören insbes. die Investition in die erforderlichen IT-Infrastrukturen, aber auch das Vertrauen der Kunden in biometrische Verfahren und die ggf. gesteigerte Überwachung des Nutzungsverhaltens.
3. Rechtlich setzt die wirksame Auslösung eines Zahlungsvorgangs durch den Zahler dessen Erklärung und Zustimmung voraus. Beides kann sich auch aus schlüssigem Verhalten ergeben.
4. Da reine Invisible-Payment-Systeme – insbes. bei elektronischen Fernzahlungsvorgängen, deren Authentifizierungsprozess eine dynamische Verknüpfung insbes. mit einem bestimmten Betrag erfordert – sinnvollerweise nur unter Anwendung der Ausnahmeregelungen von den Vorschriften zur starken Kundenauthentifizierung umgesetzt werden können, bleibt die Umsetzung auf bestimmte Geschäftsmodelle beschränkt. Die Auswahl einer konkreten Ausnahmeregelung hängt von den jeweiligen Umständen des Geschäftsmodells ab. Im Bereich der Ausnahme des Whitelisting dürfte eine Konzentration auf große und zentrale Händler und Dienstleister bzw. Vermittler zu beobachten sein.

AUTOREN

***Alexander Gebhard**, LL.M. (London), ist Partner im Frankfurter Büro von Schalast Rechtsanwälte und Notare. Der Schwerpunkt seiner Tätigkeit liegt in der Beratung zum Bank- und Zahlungsdiensteaufsichtsrecht.*

***Jonas Sturies** ist Associate im Frankfurter Büro von Schalast Rechtsanwälte und Notare. Der Schwerpunkt seiner Tätigkeit liegt in der Beratung zur Regulierung technologischer Innovation.*

33 Vgl. BaFin (Fn. 29).