Institut für Bankrecht, Universität Bern

SBT 2018 – Schweizerische Bankrechtstagung 2018

Zahlungsverkehr

herausgegeben von Susan Emmenegger

mit Beiträgen von

Marianne Wildi

Susan Emmenegger

Fabian Schmid

Cornelia Stengel

Bettina Hürlimann-Kaup

Martin Hess/Stephanie Lienhard

Harald Bärtschi/Nicolas Jacquemart/Stephan D. Meyer

Helbing Lichtenhahn Verlag

Bibliographische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Die Druckvorlagen wurden von der Herausgeberin reprofertig geliefert.

ISBN 978-3-7190-4138-0

www.helbing.ch

Unautorisierte Transaktionen im Zusammenhang mit Dritten Zahlungsdienstleistern

Susan Emmenegger*

Inhaltsverzeichnis

* Prof. Dr. iur., LL.M., ordentliche Professorin an der Universität Bern, Direktorin des Instituts für Bankrecht.

I. Dritte Zahlungdienstleister

Zu den zentralen Neuerungen der PSD2 gehört, dass sie ihren Anwendungsbereich auf sogenannte «dritte Zahlungsdienstleister» (ZDL) erweitert hat.[1] Dritte Zahlungsdienstleister erbringen kontobezogene, einen

[1] Im Hinblick auf die Zahlungsauslösedienste (ZADs) wurde dies auch von der EU-Kommission prominent in den Vordergrund gestellt, siehe den Vorschlag für eine Richtlinie, COM(2013) 547 final vom 24.07.2013, S. 8. Siehe auch Erw. 27 ff. PSD2 – Richtlinie (EU) 2015/2366 vom 25. November 2015 über Zahlungsdienste im Binnenmarkt [...] (ABl Nr. L 337 v. 23.12.2015, S. 35).

Zugriff auf das Konto voraussetzende Dienstleistungen, ohne dass sie dieses Konto selbst führen. Dritte Zahlungsdienstleister, die in der PSD2 geregelt sind, sind die Drittemittenten von Zahlungskarten, die Kontoinformationsdienste und die Zahlungsauslösedienste.

1. Drittemittenten von Zahlungskarten

Mit der Regelung von Drittemittenten von Zahlungskarten verfolgt die PSD2 das Ziel, das Angebot von Zahlungsinstrumenten zu erweitern.[2] Das Modell basiert auf den bestehenden Kreditkarten- bzw. Debitkarten-Schemes und soll insbesondere neuen Kartenanbietern den Marktzutritt ermöglichen. Bisher sind die Kartenherausgeber mit den Banken verbunden.[3] Mit der PSD soll der Markt auch für solche Drittemittenten geöffnet werden, die eigenständig agieren wollen. Es handelt sich um eine antizipierende Regulierung, bislang haben sich solche Akteure noch nicht etabliert.[4]

Weil die Drittemittenten Zahlungskarten ausgeben, ohne gleichzeitig das Konto des Zahlers zu führen, wird die Zahlung auch nicht direkt vom Konto des Zahlers abgebucht, sondern sie erfolgt zunächst durch den Drittemittenten selbst. Dieser verlangt dann einen Aufwendungsersatz vom Zahler. Der Aufwendungsersatz erfolgt durch die Einziehung des Betrages bei der Bank. Damit der Kartenemittent sicherstellen kann, dass eine Deckung vorhanden ist, muss er die Deckung bei der Bank abfragen können – und zwar auch dann, wenn er nicht schon (von vornherein) mit den Banken verbunden ist, wie das bei den traditionellen Kartenherausgebern (Visa, Mastercard) der Fall ist. Dieser Zugang auf das Kundenkonto wird ihm durch die PSD2 gewährt.[5]

---

2 Erw. 67 PSD2. Siehe hierzu auch TERLAU, ZBB 2/2016, S. 137.

3 In der Schweiz sind das z.B. Swisscard, Viseca Card Services, UBS Card Center und Cornèr Card. Siehe dazu und zur Funktionsweise von Zahlungskartensystemen STENGEL, Unautorisierte Transaktionen, S. 119 ff.

4 BÖGER, Neue Rechtsregeln, S. 282; SPINDLER/ZAHRTE, BKR 2014, S. 268. Die Irrelevanz der Dritten Zahlungsemittenten zeigt sich plastisch daran, dass sie – anders als die KIDs und die ZADs – noch nicht einmal über ein Akronym verfügen!

5 Art. 65 Abs. 1 PSD2.

2. Kontoinformationsdienste

Die PSD2 beschreibt die Kontoinformationsdienste (KIDs) als «Online-Dienst zur Mitteilung konsolidierter Informationen über ein Zahlungskonto oder mehrere Zahlungskonten, das/die ein Zahlungsdienstnutzer entweder bei einem anderen Zahlungsdienstleister oder bei mehr als einem Zahlungsdienstleister hält.»[6] Anders ausgedrückt bieten die Kontoinformationsdienste der Bankkundin einen Gesamtüberblick über ihre gesamten Kontobeziehungen, indem die Konten gebündelt dargestellt und meist auch mobil abgefragt werden können.[7] Diese Dienste werden regelmässig ergänzt durch weitere Dienstleistungen, z.B. Budgetierungstools oder Liquiditätspläne.[8]

Auch die Kontoinformationsdienste müssen für ihre Dienstleistung auf die Bankkonten ihrer Kundinnen zugreifen können. Mit Blick auf die Dienstleistung beschränkt sich der notwendige Zugriff allerdings auf den Informationsabruf.

3. Zahlungsauslösedienste

Zahlungsauslösedienste (ZADs) spielen insbesondere im Online-Handel eine Rolle. Sie schlagen eine Softwarebrücke zwischen der Webseite eines Online-Händlers und dem Webportal der Bank. Die Kundin autorisiert die Überweisung, indem sie in die Maske des Zahlungsauslösedienstes die entsprechenden Kontozugangsdaten eingibt. Die Daten des Händlers und der Betrag werden vom Dienstleister im Hintergrund hinzugefügt. In diesem Verfahren nimmt der Zahlungsauslösedienst die Zugangsdaten entgegen und leitet sie an die Hausbank weiter. Damit «löst» der Dienstleister den Zahlungsauftrag gegenüber der Bank aus. Sobald dies erfolgt ist, bestätigt er gegenüber dem Online-Händler, dass die Zahlung initiiert ist.[9]

---

6 Art. 4 Ziff. 16 PSD2.

7 Erw. 28 PSD2. Siehe auch LINARDATOS, WM Heft 7/2014, S. 300.

8 TRÜEB/KEISER, Dritte Zahlungsdienstleister, S. 166. Ein in der Schweiz aktiver Kontoinformationsdienstleister ist z.B. Qontis. In Deutschland ist es beispielsweise die «Star Finanz».

9 Beschreibung des Vorgangs bei BÖGER, Neue Rechtsregeln, S. 264. Detaillierte Beschreibung auch im Entscheid des deutschen Bundeskartellamtes zur Rechtswidrigkeit von Verboten in Bank-AGB betreffend die Weitergabe von Zugangsdaten an solche Dienstleister: BKartA-Beschl. B4-71/10 vom 29.06.2016, Rz. 20.

So funktioniert beispielsweise die in der Schweiz tätige SOFORT GmbH.[10] Sie gehört seit 2014 zum Konzern der schwedischen Klarna-Bank und tritt heute vermehrt unter dem Namen bzw. Logo der Klarna auf. Andere Dienstleister hingegen beschränkten sich darauf, die Kundin von der Internetseite des Händlers in das Online-Banking seiner Hausbank weiterzuleiten; dort löst die Kundin dann selbst die Zahlung aus. Dieses System verwenden z.B. die Unternehmen giropay, iDeal, eps und Paydirekt.[11] Sie gelten unter der PSD2 nicht als Zahlungsaulösedienste.[12]

Welche Vorteile sind mit der Sofortüberweisung verbunden? Aus Sicht der Kundinnen fallen die Gebühren für die Kreditkartennutzung weg; die Direktüberweisungen per Zahlungsauslösedienst sind (bislang) kostenlos. Der Vorgang spart auch Aufwand, weil die Eingabe der Zahlungsdaten des Händlers automatisiert durch den ZAD eingefügt werden. Zudem spart die Kundin Zeit, denn der Händler erhält eine Echtzeitbestätigung des Überweisungsauftrags. Er kann daher die Bestellung sofort bearbeiten und die Ware direkt verschicken. Im Fall einer Online-Überweisung durch die Kundin würde die Zahlung regelmässig am nächsten Tag ausgelöst, dann muss sie beim Händler noch gutgeschrieben und der Zahlungseingang überprüft werden. Zwar könnte die Schweizer Kundin die Zahlung bis zu dessen effektiver Auslösung am Ende des Geschäftstages wieder stornieren.[13] Allerdings wird sie dies nicht wiederholt tun können, denn der Zahlungsdienstleister wird diese Information erhalten und diese Kundin sperren. Zudem setzt sich eine solche Kundin dem Betrugsvorwurf und dem Vorwurf der Leistungserschleichung aus. Kurz: die Risiken einer Stornierung halten sich in Grenzen.

---

10 Webseite: <www.sofort.de>.

11 Zu beiden Verfahren siehe TERLAU, jurisPR-BKR 2/2016, Anm. 1, S. 3. Zu Paydirekt BÖGER, Neue Rechtsregeln, S. 266. Beschreibung auch in BKartA-Beschl. B4-71/10 vom 29.06.2016, Rz. 146 f.

12 TERLAU, jurisPR-BKR 2/2016 Anm. 1, S. 6.

13 Anders die Rechtslage in der EU. Gemäss Art. 80 PSD2 (früher: Art. 66 PSD1) kann der Zahler den Zahlungsauftrag nicht mehr widerrufen, sobald er beim Zahlungsdienstleister eingeht. Gemäss Art. 470 Abs. 2bis OR kann die Anweisung im zahlungslosen Bargeldverkehr nicht mehr widerrufen werden, sobald der Betrag dem Konto des Zahlers belastet ist. Die Belastung erfolgt in der Schweiz jeweils zum Tagesende (24 Uhr). Bis dann bleiben die Zahlungsaufträge pendent und können wieder gelöscht werden. Zur Rechtslage in Deutschland siehe etwa LINARDATOS, WM Heft 7/2014, S. 300.

Für den Händler liegt der Vorteil in der vergleichsweise geringen Gebühr, die er dem Zahlungsauslösedienst entrichten muss. Er weiss zudem dank der Echtzeitbestätigung des Transaktionsauftrags, dass der Zahlungsauftrag angenommen wurde und somit eine genügende Deckung besteht und dass auch keine anderen Hinderungsgründe für die Zahlungsausführung bestehen.[14] Insofern kommt der Vorgang einer Vorkasse (Vorauszahlung) nahe.[15] Die Echtzeitbestätigung bringt im Vergleich zur Vorkasse den Vorteil, dass der Händler den Verwaltungsaufwand zur Kontrolle des Zahlungseingangs spart und die Ware sofort versenden kann. Mit der schnellen Lieferung erreicht er eine grössere Kundenzufriedenheit. Schliesslich kann ein Online-Händler – etwa im Geschäft mit Online-Downloads oder Event-Tickets – auf diese Art auch neue Kundenkreise erschliessen, namentlich solche Kunden, die über keine Kreditkarte verfügen.[16] Zu denken ist angesichts der Beispiele vor allem auch an die jüngere Kundschaft.

II. Kritik an den Dritten Zahlungsdienstleistern

Im Zusammenhang mit den Dritten Zahlungsdienstleistern bestehen eine Reihe von Bedenken. Die Diskussionen beschränken sich auf die beiden Dienstleister, die bereits auf dem Markt tätig sind, also die Kontoinformationsdienste (KIDs) und die Zahlungsauslösedienste (ZADs). Unter den beiden Diensten sind die Bedenken zudem bei den Zahlungsauslösediensten besonders ausgeprägt – und zwar durchaus auch bei den Aufsichtsbehörden.[17]

1. Sicherheitsrisiken: Unautorisierte Transaktionen

Der am häufigsten genannte Kritikpunkt im Zusammenhang mit den Dritten Zahlungsdienstleistern ist das zusätzliche Sicherheitsrisiko. Denn

---

14 Siehe BÖGER, Neue Rechtsregeln, S. 264. Siehe auch BKartA-Beschl. B4-71/10 vom 29.06.2016, Rz. 139. In der EU wird zudem der Zahlungsauftrag unwiderrufbar, er kommt daher einer Vorkasse nahe.

15 Allerdings kann die Schweizer Kundin den Auftrag noch bis zum Ende des Tages stornieren, siehe Fn. 13.

16 Erw. 29 PSD2. Siehe auch OMLOR, ZIP 12/2016, S. 561.

17 Siehe etwa den Fachartikel der deutschen BaFin aus dem Jahr 2014 (noch vor der definitiven Fassung der PSD2): BAFIN, Zahlungsdiensterichtlinie II: Risiken und schwerwiegende Folgen für Nutzer und Kreditinstitute.

aktuell erfolgt deren Kontozugriff standardmässig über Weitergabe der persönlichen Kontozugangsdaten, welche die Kundin den Dritten ZDL zur Verfügung stellt, indem sie diese auf deren Webportal in die dort vorgesehene Maske eingibt (sog. Screen Scraping). Darin wird ein erhöhtes Risiko für die Durchführung unautorisierte Transaktionen gesehen.

Im schweizerischen Recht ist die unautorisierte Transaktion nicht definiert. In Lehre und Rechtsprechung wird der Begriff des Legitimationsmangels verwendet. Damit sind aber regelmässig nur Zahlungen gemeint, bei denen der Zahlungsempfänger in betrügerischer Absicht gehandelt und eine unbefugte Zahlung an sich selbst bewirkt hat.[18] Die PSD2 fasst unter dem Begriff der unautorisierten Transaktion alle Zahlungen, die ohne Zustimmung des Zahlers erfolgen.[19] Der Begriff deckt also mehr als nur den Legitimationsmangel ab, er umfasst unter anderem auch die Doppelausführung oder versehentliche Ausführung von Überweisungen, die Vertretung ohne Vertretungsmacht, die Zahlung trotz Widerrufs, die Zahlung an einen falschen Empfänger wegen falscher IBAN-Angabe oder die mangelnde Geschäftsfähigkeit.[20]

Die hier angesprochenen Sicherheitsrisiken betreffen unautorisierte Transaktionen, bei denen sich betrügerisch handelnde Unbefugte Zugang zu einem fremden Konto verschaffen. Das sind im schweizerischen Verständnis die klassischen Legitimationsmängel.

a) Man-in-the-Middle-Angriffe

Bei den unbefugten Zugriffen auf die Bankkonten von Kundinnen, welche die Dienste von Dritten Zahlungsdienstleistern in Anspruch nehmen, steht nicht das Risiko im Vordergrund, dass der Dritte Zahlungsdienstleister den Kontozugang nutzen könnte, um selbst betrügerische Transaktionen zu seinen Gunsten zu tätigen. Diesbezüglich übt der Markt sowohl auf der Händler- als auch auf der Kundenseite eine genügende Kontrolle aus.

Im Zentrum der Sicherheitsdebatte stehen vielmehr die sogenannten «Man-in-the-Middle-Angriffe».[21] Bei solchen Angriffen schiebt sich der Angreifer (selbst oder über eine schädliche Software) zwischen die Kommuni-

---

18 Zu den verschiedenen Konstellationen siehe SCHALLER, Legitimationsmängel, S. 49 f.

19 Art. 64 Abs. 2 PSD2.

20 Beispiele bei BAUMBACH/HOPT HGB-HOPT, Bankgeschäfte, C/57.

21 Ausführlich dazu BAFIN, Zahlungsdiensterichtlinie II, Risiken und schwerwiegende Folgen für Nutzer und Kreditinstitute, S. 4 f.

kationspartner und leitet die Datenpakete auf ein drittes System um. Dabei spiegelt er den Kommunkationspartnern jeweils die Identität des anderen vor. Er kann die Datenpakete anschauen und verändern, bevor er sie an die Endstelle weiterleitet.[22] Der Angriff kann die Hardware jedes Kommunikationspartners (z.B. Computer, Handy), aber auch auf den Kommunikationsweg (WLAN, Angriff auf die HTTPS-Verbindung) gerichtet sein.

Bei der Einschaltung eines Dritten Zahlungsdienstleisters wird ein erhöhtes Risiko darin gesehen, dass es keine direkte Kommunikationslinie zwischen der Kundin und der Bank gibt, sondern dass sich andere Akteure dazwischenschieben. Damit werden zusätzliche Angriffspunkte für Man-in-th-Middle-Angriffe geschaffen.

b) Einschätzung des Risikos

Wie hoch ist das Risiko einer Man-in-the-Middle-Attacke im Falle der Nutzung eines Dritten Zahlungsdienstleisters, insbesondere eines Zahlungsauslösedienstes? Unstreitig schieben sich im Vergleich zu einem direkten Verbindungsaufbau zur kontoführenden Bank weitere Akteure in die Verbindung ein. Diese Akteure – also die Händler und insbesondere auch die Zahlungsauslösedienste – können selbst Zielscheibe eines Angriffs sein. Es entstehen also zusätzliche Angriffsstellen für Hacker-Angriffe.

Zu bedenken ist allerdings Folgendes: Der typische Risikofall bei Man-in-the-Middle-Angriffen ist der Angriff auf das IT-Umfeld der Bankkundin. Ein Angriff auf die Kunden-Hardware ist viel einfacher als ein Angriff auf die Sicherheitssysteme und die verschlüsselten Kommunikations-

---

[22] Siehe z.B. SCHAMAUN PHILIPP, Man-in-the-Middle-Angriffe (Stand: Dezember 2017), unter: www.sicherheitskultur.at/man_in_the_middle.htm. Siehe auch die Beschreibung bei BKartA-Beschl. B4-71/10 vom 29.06.2016, Rz. 53 Fn. 39: «Ziel eines Man-in-the-Middle-Angriffs ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer 'in die Mitte' der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und dem Empfänger gegenüber als Sender ausgibt. Als erstes leitet der Angreifer eine Verbindungsanfrage des Senders zu sich um. Im nächsten Schritt baut der Angreifer eine Verbindung zu dem eigentlichen Empfänger der Nachricht auf. Wenn ihm das gelingt, kann der Angreifer unter Umständen alle Informationen, die der Sender an den vermeintlichichen Empfänger sendet, einsehen oder manipulieren, bevor er sie an den richtigen Empfänger weiterleitet. Auf Antworten des Empfängers kann der Angreifer wiederum zugreifen, wenn nicht entsprechende Schutzmechanismen wirksam sind.».

kanäle von professionellen Marktteilnehmern. Der typische Man-in-the-Middle-Angriff verläuft dergestalt, dass der Angreifer der Kundin vorspiegelt, sie erhalte eine Kommunikation ihrer Bank. In diesem Zusammenhang wird die Kundin dann aufgefordert, eine Software herunterzuladen, die es dem Angreifer beim nächsten Zahlungsvorgang erlaubt, die Zugangsdaten abzufangen und die Zahlung zu manipulieren.[23] Oder aber die Kundin wird auf eine falsche Internetseite gelockt und dort aufgefordert, ihre Zugangsdaten einzugeben.[24]

Für einen Angreifer ist ein Angriff auf der Kundenseite auch deshalb viel einfacher als ein Angriff auf einen Zahlungsauslösedienst, weil er nur den Zahlungsvorgang einer einzigen Bank abbilden muss – er muss also nur wissen, wie das Login-Verfahren und die Zahlungsauslösung bei einer einzigen Bank funktioniert. Bei einem Angriff auf einen Zahlungsauslösedienst müsste er hingegen die Kommunikationsstruktur aller Banken nachbilden, was einen enormen Aufwand bedeuten würde. Hinzu kommt, dass Zahlungsauslösedienste im Zusammenhang mit dem Online-Handel zum Einsatz kommen. Die Kundin erwartet unmittelbar im Anschluss an die Zahlung eine Ware oder eine Dienstleistung. Das Zeitfenster für erfolgreiche Angriffe ist also deutlich kleiner als bei sonstigen Überweisungen.

Nach Angaben der hierzulande bekannten Klarna (früher: SOFORT GmbH) ist es seit der ersten Anwendung des Zahlungsverfahrens im Jahr 2005 im Rahmen der über 100 Millionen Transaktionen noch zu keinem Betrugsfall zu Lasten eines Kunden gekommen.[25] In einem Urteil des Oberlandesgerichts Frankfurt vom August 2016 heisst es, die Geltendmachung des Risikos einer Man-in-the-Middle-Attacke im Zusammenhang mit den Dienstleistungen der SOFORT GmbH bleibe «im abstrakten Bereich».[26]

---

23 So etwa der Sachverhalt in den Entscheiden des LG Darmstadt, siehe LG Darmstadt, Urteil vom 28. August 2014, 28 O 36/14 = WM 2014, S. 2323 ff.

24 So etwa der Sachverhalt im Entscheid des LG Köln, siehe LG Köln, Urteil vom 26. August 2014, 3O 390/13 = WM 2014, S. 2372 ff.

25 SCHOOR, Sofortüberweisung, S. 3. Siehe dazu OLG Frankfurt, 11 U 123/15 (Kart) vom 24.08.2016 = BKR 2017, S. 129 Rz. 40.

26 OLG Frankfurt, 11 U 123/15 (Kart) vom 24.08.2016 = BKR 2017 S. 129 Rz. 40. Der Streit handelte darüber, ob es zumutbar sei, wenn zur Erfüllung der gesetzlich geforderten kostenlosen Zahlungsmöglichkeit einzig die Zahlung über die SOFORT GmbH anbieten dürfe. Das OLG Frankfurt hat dies bejaht, der BGH hat dies im Rahmen der Anschlussberufung verneint. Zur Frage der Sicherheitsrisiken äusserte sich der BGH nicht. Siehe BGH, Urteil vom 18. Juli 2017 KZR 39/16 = NJW 2017, S. 3289. Unter der PSD2 hat sich die Frage erledigt.

c) Fazit

Insgesamt ist das erhöhte Risiko von Angriffen, insbesondere solchen, die eine unbefugte Zahlung auslösen würden, mehr gefühlter als tatsächlicher Natur. Nicht von der Hand zu weisen ist allerdings, dass die Nutzung von Zahlungsauslösediensten und überhaupt von Dritten Zahlungsdiensten dazu beiträgt, die Hemmschwelle für die Weitergabe von persönlichen Legitimationsmitteln (TAN[27], PIN[28]) herabzusetzen. Damit vergrössert sich mittelbar auch das Risiko, dass Unbefugte Kenntnis dieser Legitimationsmittel erhalten.

2. Datenschutz

a) Einblick in das Zahlungsprofil

Ein weiterer Kritikpunkt, der gegenüber den Dritten Zahlungsdienstleistern geäussert wird, betrifft den Datenschutz. Die Dritten Zahlungsdienstleister erhalten Zugriff auf die Kontodaten ihrer Nutzer. Im Falle von Kontoinformationsdienstleistern ergeben sich daraus sehr detaillierte Zahlungsprofile. Aber auch im Fall der Zahlungsauslösedienste besteht dieser Zugriff. Die in der Schweiz tätige Klarna (früher: SOFORT GmbH) weist denn auch ausdrücklich darauf hin, dass sie die Kontodeckung überprüft und die Überweisungen der letzten 30 Tage daraufhin untersucht, ob Überweisungen mit Klarna getätigt wurden. Tatsächlich erhalten Klarna und andere Zahlungsauslösedienste einen weit grösseren Zugriff; sie können die Zahlungshistorie soweit zurückverfolgen wie die Kundin selbst, und dies für alle Konten der Kundin bei der betroffenen Bank. Der Zugriff auf die gesamte Zahlungshistorie bzw. den kompletten Finanzstatuts der Kundin[29] erlaubt die Aus-

---

27 Transaction Number (Transaktionsnummer). TANs werden in verschiedenen Verfahren verwendet: Reguläre TAN: Man kann die TAN aus einer Liste auswählen (veraltet). Indizierte TAN (iTAN): Benutzer wählt eine vom Institut vorgegebene TAN aus einer TAN-Liste aus. Mobile TAN (mTAN): Dem Benutzer wird vor der Transaktion eine TAN als SMS übertragen. Smart TAN (sTAN): Erzeugung der TAN durch einen TAN-Generator. ChipTAN (chipTAN): Die TAN wird vom Institut als Balkencode übermitteld unt auf einem TAN-Generator angezeigt. Quelle: <https://www.itwissen.info/PIN-TAN-Verfahren-PIN-TAN-methode.html>.

28 Personal Identification Number (Persönliche Identifikationsnummer).

29 Gemäss der Stellungnahme der deutschen Kreditwirschaft wird diese Durchleuchtung bei einigen Dritten Zahlungsdienstleistern intensiv praktiziert, und zwar automatisiert und in Sekundenschnelle. Siehe DEUTSCHE KREDITWIRTSCHAFT, Stellungnahme, S. 7.

wertung der Kontoinformationen für Bonitätsprüfungen oder für die Erstellung eines Verhaltensprofils, das dann selbst eingesetzt werden kann, etwa zur zielgerichteten Bewerbung von Finanzprodukten, oder an Dritte weiterveräussert werden kann.[30]

b) Einschätzung des Risikos

Unbestrittenermassen haben die Dritten Zahlungdienstleister Zugriff auf die Zahlungshistorien ihrer Nutzerinnen und Nutzern. Der Zugriff auf diese Daten erfolgt allerdings nicht unreguliert. Es gilt in der Schweiz das schweizerische Datenschutzgesetz, das den Dritten Zahlungsdienstleistern den Rahmen setzt. Das DSG gilt für die Dritten Zahlungsdienstleister genauso wie für die Banken. Letztere lassen sich im Rahmen der AGB durchweg ermächtigen, die im Rahmen ihrer Dienstleistung erlangten Daten über die Bankbeziehung(en) mit Kundinnen und Kunden für Marketingzwecke zu verwenden.

Hinzu kommt, dass die bislang in der Schweiz tätigen Dritten Zahlungsdienstleister entweder aus der Schweiz oder aus dem europäischen Ausland stammen. In Europa gilt ab dem 25. Mai 2018 die Datenschutzgrundverordnung, die deutlich strengere Anforderungen an die Datennutzung und Datenverarbeitung stellt als das schweizerische Datenschutzgesetz, und dies selbst bei Berücksichtigung der aktuellen Revision des DSG.

c) Fazit

Insgesamt hält sich im Zusammenhang mit den Dritten Zahlungsdienstleistern auch das *rechtliche* Risiko der Datensicherheit in Grenzen. Es ist denn auch weniger der rechtliche Rahmen, der in diesem Zusammenhang Probleme schafft, sondern vielmehr die Tatsache, das gewisse Nutzerinnen und Nutzer mit beachtlicher Leichtigkeit alle möglichen Zustimmungs-Buttons im Internet anklicken. Das ist allerdings ein generelles Problem, das nicht spezifisch mit dem Dienstleistungsangebot der Dritten Zahlungsdienstleister zusammenhängt.

---

30 SPINDLER/ZAHRTE, BKR 2014, S. 267 f. Siehe auch BÖGER, Neue Rechtsregeln, S. 267 m.w.N.

3. Wettbewerbsverzerrungen

Schliesslich wird geltend gemacht, dass Dritte Zahlungsdienstleister sich als Trittbrettfahrer betätigen, weil sie die von der Bank entwickelte und von ihr unterhaltende Online-Zahlungs- und Datenbankinfrastruktur, inklusive der kostenintensiven Sicherheitsstruktur, nutzen, ohne sich an den Kosten zu beteiligen.[31] Die Online-Händler sind nur deswegen bereit, für die Nutzung eines Zahlungsauslösedienstes ein Entgelt zu zahlen, weil sie eine Bestätigung über die tatsächliche Auftragsentgegennahme von der Bank erhalten. Für diese Dienstleistung bezahlen die Dritten Zahlungsdienstleister aber nichts.

Dieser Kritikpunkt lässt sich nicht abstreiten – im aktuellen System nutzen die Dritten Zahlungsdienstleister den Kontozugang, ohne dass die Bank dies erkennen kann. Insofern fehlt auch die Möglichkeit, eine Entgeltzahlung zu fordern.

Allerdings ist die Identifikation der Dritten Zahlungsdienstleister durch die Bank nicht zwingend mit einer Entgeltzahlung verbunden. Das zeigt sich am Regime der PSD2: Der Zugang der Dritten Zahlungdienstleister auf die Kundenkonten wird künftig über eine separate Schnittstelle erfolgen, so dass die Dritten Zahlungsdienstleister für die Bank erkennbar sind.[32] Die umfangreichen Kooperationspflichten der Bank sind aber gerade nicht an eine Entgeltzahlung gekoppelt; vielmehr bestehen die Kooperationspflichten der Bank unabhängig vom Bestand einer vertraglichen Beziehung zum Zahlungsauslösedienst.[33]

4. Fazit

An den Dritten Zahlungsdienstleistern wird regelmässig Kritik geübt. Im Vordergrund steht jeweils die Kritik bezüglich der fehlenden Datensicherheit und des fehlenden Datenschutzes. Diese Kritikpunkt halten einer

---

31 Siehe dazu DEUTSCHE KREDITWIRTSCHAFT, Stellungnahme, S. 6. Siehe auch BÖGER, Neue Rechtsregeln, S. 265.

32 Siehe Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 (ABl Nr. L 69 v. 13.03.2018, S. 23), Art. 30, 31. Zum Verbot des Screen Scraping siehe den ausdrücklichen Hinweis im Kommissionsentwurf C(2017) 7782 final S. 3. Siehe dazu auch hinten IV.3 (Marktzutritt zum Preis der Regulierung).

33 Art. 66 Abs. 5 PSD2.

näheren Betrachtung nur bedingt stand. Hingegen ist offensichtlich, dass die Dritten Zahlungsdienstleister für ihre gewinnorientierten Dienste die Zahlungsinfrastruktur der Banken nutzen, ohne die Banken dafür zu entschädigen.

III. Haftung bei unautorisierten Transaktionen

Gemäss den obenstehenden Überlegungen besteht ein geringes Risiko, dass die Online-Verbindung der Kundin zu einem Dritten Zahlungsdienstleister für eine Hacking-Attacke genutzt wird. Dennoch soll hier solches Szenario im Hinblick auf die Schadens- bzw. Haftungsverteilung näher untersucht werden.

1. Beispiel: Man-in-the-Middle-Angriff auf den Zahlungsauslösedienst

Den Ausgang bildet folgendes Fallbeispiel: Eine Man-in-the-Middle-Attacke gegen einen Zahlungsauslösedienst ist erfolgreich verlaufen und ein falscher Zahlungsauslösedienst hat mithilfe der Zugangscodes, welchen die Kundin in die falsche Zahlungsmaske eingegeben hat, eine unautorisierte Zahlung ausgelöst. Die Kundin bemerkt die falsche Zahlung, weil die Ware nicht geliefert wird. Sie konsultiert online ihr Konto und stellt fest, dass eine Zahlung von CHF 3'000 an eine ihr unbekannte Gesellschaft in Georgien geleistet wurde. Sie beanstandet die falsche Belastung bei seiner Bank, erstattet Strafanzeige gegen Unbekannt und macht den fehlenden Betrag auch beim gehackten Zahlungsauslösedienst geltend. Die Frage ist, ob die Kundin die von ihr geltend gemachten Ansprüche erfolgreich durchsetzen kann.

2. Anspruch gegen die Bank

Gegenüber der Bank wird die Kundin einen Erstattungsanspruch geltend machen. Die Bank hat an einen Unbefugten geleistet. Entsprechend hat sie

nicht gehörig erfüllt und ist zur Leistung nach wie vor verpflichtet.[34] Sie hat aber ihrerseits einen verschuldensabhängigen Schadenersatzanspruch gegen die Kundin, falls diese am unbefugten Zahlungsvorgang ein Verschulden trifft.[35] Diese Regelung wird aber in den Banken-AGB durchweg modifiziert.

a) Legitimationsabrede

Die in der hier interessierenden Konstellation anwendbaren AGB zum Online-Banking sehen durchweg vor, dass Aufträge und Mitteilungen von Personen, die sich mit dem vorgesehenen Legitimationsverfahren Zugang zu den Online-Dienstleistungen der Bank verschaffen, als vom Kunden verfasst bzw. als von ihm autorisiert gelten und dass die Bank ermächtigt ist, diesen Instruktionen Folge zu leisten.[36]

Somit kann die Bank bereits gestützt auf die Legitimationsabrede geltend machen, dass sie keine Erstattungspflicht trifft. Ob die Legitimationsabrede vor einer gerichtlichen AGB-Kontrolle Bestand hat, wurde noch nicht getestet. Nach der hier vertretenen Auffassung verstösst sie gegen Art. 8 UWG. Denn eine Legitimationsabsprache, die selbst im Fall eines erfolgreichen Angriffs auf die Online-Banking-Systeme der Bank das Risiko auf die Kundin abwälzt, schafft ein erhebliches und ungerechtfertiges Missverhältnis zwischen den vertraglichen Rechten und Pflichten im Bank/Kundenverhältnis zum Nachteil der Konsumentinnen und Konsumenten.

Unter der Annahme, dass die AGB zum Online-Banking die Frage der Legitimationsmängel abschliessend regeln, führt der Verstoss der gängigen Legitimationsabsprache gegen Art. 8 UWG zum Fehlen einer AGB-

---

34 BGE 112 II 450 E. 4 S. 457; 132 III 450 E. 2 S. 452; BGer Urteil 4C.377/2000 vom 8. März 2001 E. 1b; 4C.28/2003 vom 15. Dezember 2003 E. 3.2.1; 4A_386/2016 vom 5. Dezember 2016 E. 2.2.2. Aus jüngerer Zeit zudem SCHALLER, Legitimationsmängel, S. 46 f. m.w.N.

35 BGer 4A_438/2007 vom 29. Januar 2008 E. 5.1; SCHALLER, Legitimationsmängel, S. 46 f. m.w.N.

36 AGB-Beispiel: «Jede Person, die sich mit den persönlichen Legitimationsmitteln und dem in der «Anleitung» beschriebenen Legitimationsverfahren erfolgreich Zugang zu [Bank] Digital Banking verschafft (Selbstlegitimation), gilt der [Bank] gegenüber als zugriffsberechtigt; dies gilt unabhängig davon, ob es sich bei dieser Person tatsächlich um den Zugriffsberechtigten handelt bzw. diese vom Vertragspartner entsprechend autorisiert wurde. Sämtliche bei [Bank] über [Bank] Digital Banking eingehenden Weisungen und Instruktionen gelten als vom Zugriffsberechtigten verfasst. [Bank] gilt als beauftragt, im Rahmen des üblichen Geschäftsgangs diese Weisungen auszuführen sowie den Mitteilungen nachzukommen, sobald diesen eine korrekte Legitimationsprüfung zugrunde liegt.» (Stand: 1. Juni 2018).

Regelung. Es greift dann der Grundsatz, dass die Bank der Kundin den unbefugt abgebuchten Betrag wieder gutschreiben muss.

b) Sorgfaltspflichten des Nutzers/der Nutzerin

Zwar hat die Bank nach dem Gesagten den Schaden aus einer unbefugten Zahlung selbst zu tragen. Sie hat aber ihrerseits einen Schadenersatzanspruch gegen die Kundin, falls diese an der unbefugten Zahlung ein Verschulden trifft.

Die AGB der Banken zu den Online-Dienstleistungen sehen vor, dass die Legitimationsmittel «keinesfalls weitergegeben oder in einer anderen Weise anderen Personen zugänglich gemacht werden» dürfen.[37] Zudem wird teilweise ausdrücklich erwähnt, dass die Anmeldung (das Login) immer nur auf der Bankseite erfolgen darf und nie auf der Drittseite eines Drittanbieters.[38] In diesem Zusammenhang wird dann auch ausgeführt, dass der Nutzer die Risiken trägt, die sich aus der Verletzung der genannten Sorgfaltspflichten ergeben.[39]

Die Nutzung von Zahlungsauslösediensten gilt mithin – falls sie nicht von der Bank anderweitig genehmigt wird – als Vertragsverletzung. Falls also der Zahlungsauslösedienst einer erfolgreichen Hacking-Attacke zum Opfer fällt, so liegt an deren Ursprung eine Vertragsverletzung durch die Kundin, für die sie sich nicht exkulpieren kann. Entsprechend kann die Bank den Schaden, den sie aufgrund einer unautorisierten Zahlung tragen muss, als Schadenersatz gestützt auf Art. 97 OR gegenüber der Kundin geltend machen. Ein Eigenverschulden der Bank wird man in diesem Fall nicht annehmen können. Also schuldet die Kundin den vollen Ersatz – im Ergebnis kann also die Bank den streitigen Betrag abbuchen.

---

37 AGB-Beispiel: «Die Zugangsmittel (insbesondere PIN/Passwort, Sicherheitscode und Kartennummer oder Accesss Card) dürfen keinesfalls weiteregeben oder auf andere Weise anderen Personen zugänglich gemacht werden.».

38 Diese Klausel hat das deutsche Bundeskartellamt verboten, weil hierdurch ein Wettbewerbsnachteil zu anderen Zahlungdiensten entstehen würde. Siehe SCHOOR, Sofortüberweisung, S. 3. Siehe auch den Beschluss BKartA-Beschl. B4-71/10 vom 29.06.2016.

39 AGB-Beispiel: «Der Kunde/die Kundin trägt sämtliche Risiken, die sich aus der Preisgabe oder Aufzeichnung seiner/ihrer Legitimationsmittel ergeben.».

c) Fazit

Resultiert im Zusammenhang mit der Nutzung eines Zahlungsauslösedienstes eine unautorisierte Abbuchung, so hat zwar die Bank diesen Schaden in einem ersten Schritt zu tragen. In einem zweiten Schritt kann sie allerdings gegenüber der Kundin einen Schadenersatzanspruch aus Vertragsverletzung geltend machen (Art. 97 OR), denn die AGB untersagen es den Kundinnen und Kunden der Bank durchweg, ihre Legitimationsmittel an Dritte weiterzugeben oder sie auf einer anderen als der bankeigenen Webseite einzugeben.

3. Anspruch gegen den Zahlungsauslösedienst

Da bei der vorliegenden Konstellation der Zahlungsauslösedienst erfolgreich angegriffen wurde, liegt bei ihm auch der Ursprung für die unautorisierte Zahlung. Entsprechend stellt sich die Frage, ob die Kunding gegenüber dem ZAD einen Schadenersatzanspruch geltend machen kann.

a) Zahlungsauslösedienstleister als Beauftragter

Zwischen der Nutzerin und dem Zahlungsauslösedienstleister besteht nach schweizerischem Recht ein Auftragsverhältnis. Das verdient deshalb besondere Erwähnung, weil in Deutschland teilweise vertreten wird, es bestehe kein (Geschäftsbesorgungs-)Vertrag zwischen dem ZAD und dem Nutzer. Vielmehr handle sich um einen Vertrag zu Gunsten Dritter, der zwischen dem Händler und dem ZAD zugunsten des Nutzers geschlossen werde. Allerdings soll auch in dieser Konstellation ein Recht des Zahlers vereinbart sein, vom ZAD die Auslösung des Zahlungsvorgangs (direkt) zu fordern (§ 328 Abs. 1 BGB), und der ZAD wäre verpflichtet, sorgfältig mit den Zugangsdaten umzugehen.[40] Als Begründung für diese rechtliche Einordnung wird angeführt, dass die Zahlungsauslösung für den Kunden

[40] TERLAU, jurisPR-BKR 2/2016, S. 11. Wohl befürwortend OLG Frankfurt, 11 U 123/15 (Kart) vom 24.08.2016, S. 9 («Soweit dieser Vertrag als Vertrag zu Gunsten Dritter im Sinne des § 328 BGB ausgestaltet sein dürfte ...»). Anders aber z.B. SPINDLER/ZAHRTE, BKR 2014, S. 269 (ausdrückliche Bezugnahme auf den «Vertrag» zwischen Zahler und TPP).

kostenlos sei. Zudem würden sich die ZAD selbst als Dienstleister des Händlers sehen.[41]

Aus schweizerischer Sicht ist die Rechtslage – jedenfalls im Hinblick auf die hier aktive Klarna (früher SOFORT GmbH) – anders zu beurteilen. Ein Vertrag kommt gemäss Art. 1 OR gestützt auf einen tatsächlichen oder rechtlichen Konsens zustande. Soweit hier ein tatsächlicher Konsens vom ZAD bestritten würde, wäre ein solcher gestützt auf das Vertrauensprinzip anzunehmen. Die Kundin wählt für den Zahlungsvorgang den ZAD. Dieser präsentiert sich ihr gegenüber als Dienstleister: Er stellt Masken zur Verfügung, welche die Kundin für den Bezahlvorgang nutzen kann. Gleichzeitig handelt es sich ersichtlich um einen unabhängigen Dritten und nicht um den Händler selbst. Die Kundin kann als vernünftige Person davon ausgehen, dass der ZAD ihm gegenüber eine Dienstleistung erbringt und über den entsprechenden Geschäfts- und Abschlusswillen[42] verfügt. Die Dienstleistung besteht – wie schon erwähnt – darin, dass der ZAD für die Kundin den Zahlungsvorgang erleichtert und anstösst, indem er als Erklärungsbote die Zahlung in Auftrag gibt. Dass kein separates Entgelt für die Dienstleistung des ZAD ausgewiesen ist, zerstört das Vertrauen über das Vorliegen eines Auftrags nicht, da das Obligationenrecht den Auftrag vermutungsweise als unentgeltliches Geschäft qualifiziert (Art. 394 Abs. 3 OR). Tatsächlich wird die Kundin nicht zu Unrecht davon ausgehen, dass solche Dienstleistungen vom Händler gesamthaft eingepreist sind.

Hinzu kommt, dass – jedenfalls im Fall der Klarna – im Rahmen der FAQ die Dienstleistung gegenüber der Kundin konkretisiert wird. Dort werden unter dem dem Titel «Unser Versprechen», verschiedene Zusicherungen gemacht. Die wichtigste Zusicherung besteht in der «Verpflichtung» (*sic*) einer Schadensfreistellung im Fall des Datenmissbrauchs (dazu unten). Diese Versprechen richten sich, da sie auf der Seite des Zahlvorgangs erscheinen, zwangsläufig an die Nutzerin dieses Dienstes. Wer in dieser Weise etwas verspricht, gibt einen vertraglichen Bindungswillen kund – tatsächlich, mindestens aber vertrauenstheoretisch.

Schliesslich scheint auch die PSD2 als «Geburtshelferin» der Dritten Zahlungsdienstleister von einer vertraglichen Rechtsbeziehung zwischen dem

---

41 TERLAU, jurisPR-BKR 2/2016, S. 10, unter Hinweis auf die allgemeinen Geschäftsbedingungen der SOFRT GmbH bei Registrierung (der Händler) und die allgemeinen Geschäftsbedingungen eines Online-Händlers (OBI E-Commerce GmbH).

42 Siehe hierzu GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT I, Rn. 171, Rn. 308.

ZAD und den Nutzerinnen und Nutzern auszugehen; sie definiert den Zahlungsauslösedienst als Dienst, der «auf Antrag des Zahlungsdienstnutzers einen Zahlungsauftrag.... auslöst.»[43] Zudem spricht sie vom «Vertrag zwischen dem Zahler und dem Zahlungsauslösedienstleister» (Art. 73 Abs. 3 PSD2).

Im Ergebnis besteht zwischem dem ZAD und der Kundin ein Auftragsverhältnis im Sinne von Art. 398 ff. OR.

b) Schadensfreistellung in den AGB

Im Fall der in der Schweiz tätigen Klarna richtet sich der Schadenersatzanspruch zunächst nach der vertraglichen Vereinbarung zwischen ihr und der Kundin. Die Klarna sichert unter der Sparte FAQ «Unser Versprechen» den Zahlern eine «Schadensfreistellung für den unwahrscheinlichen Fall eines Datenmissbrauchs» zu.[44] Wörtlich heisst es, dass sich die Sofort GmbH verpflichtet, den «Endkunden, die PIN und TAN in unser System eingeben, von etwaigen Vermögensschäden freizustellen, die dem Endkunden möglicherweise dadurch entstehen, dass seine über unser System geroutete PIN- und TAN-Daten missbraucht werden und dem Endkunden durch die Verwendung der über unser System gerouteten PIN und TAN ein Schaden entsteht.»[45] Der Freistellungsanspruch ist betraglich nicht limitiert; eine Begrenzung ergibt sich aus dem Kausalzusammenhang zwischen der missbräuchlichen Verwendung der Zugangsdaten und dem Schaden.

Dass im Falle einer Man-in-the-Middle-Attacke die Zugangsdaten nicht über das System der Sofort GmbH geroutet werden, weil sie vorher abgefangen und umgeleitet werden, steht dem Freistellungsanspruch nicht entgegen. Nach dem Vertrauensprinzip liegt darin eine umfassende Schadensfreistellung für Datenmissbrauch im Einflussbereich des Zahlungsauslösedienstes.

c) Haftung aus Auftragsrecht

Andere Zahlungauslösedienste können andere AGB enthalten oder den Fall der Legitimationsmängel gar nicht regeln. Dann kommt als Auffangordnung

---

43 Art. 4 Ziff. 15 PSD2.

44 FAQ Sofort GmbH, auch einsehbar bei der Demo-Version:< https://www.sofort.com/payment/multipay/go/login>.

45 *Id.*

das Auftragsrecht zur Anwendung. Danach haftet der ZAD der Kundin für die getreue und sorgfältige Ausführung des ihm übertragenen Geschäfts (Art. 398 Abs. 2 OR). Gelingt es einem Angreifer, den ZAD erfolgreich zu hacken und sich als Man-in-the-Middle zwischen den ZAD und den Kunden zu stellen und so den Datenzugang abzufangen, so ist auf eine Sicherheitslücke beim ZAD zu schliessen. Dass diese auf die Unsorgfalt des ZAD zurückgeht, muss der Kunde nachweisen. An den Nachweis sind aber keine hohen Anforderungen zu stellen – zumal etwa im Fall der Klarna der ZAD damit wirbt, zu den sichersten Bezahlverfahren weltweit zu gehören. Das fehlende Verschulden ist sodann vom ZAD nachzuweisen. Die Umstossung der Vermutung dürfte ihm aber kaum gelingen.

d) Fazit

Wird der Zahlungsauslösedienst erfolgreich gehackt, führt dies zu einem Schadenersatz seitens der Kundin. Die in der Schweiz tätige Klarna verpflichtet sich sodann gegenüber dem Nutzer zur unlimitierten Schadensfreistellung für den Fall eines Datenmissbrauchs in ihrem Einflussbereich. Für das hier gewählte Szenario einer erfolgreichen Man-in-the-Middle-Attacke auf den ZAD bedeutet dies, dass der ZAD der Kundin den aus dem Datenmissbrauch entstandenen Schaden ersetzen wird.

4. Ergebnis

Im Ergebnis muss also die Kundin gegenüber der Bank einen ZAD-relevanten Schaden tragen, aber sie hat gegenüber dem ZAD gestützt auf dispositives Gesetzesrecht oder einzelfallsweise gestützt auf die vertragliche Vereinbarung einen Anspruch auf Schadenersatz. Das erscheint sachgerecht, es blendet allerdings eine Schwierigkeit aus: Wenn das Konto der Kundin aufgrund eines betrügerischen Eingriffs belastet wird, so ist es für die Kundin sehr schwer erkennbar, wo der Angriff stattgefunden hat. Dies umso mehr, als die Kundin zwar gegenüber ihren Beauftragten (Bank, ZAD) Informationsansprüche hat und diese ihr Rechenschaft über den ordnungsgemässen Zahlungsablauf schulden. Aber diese Pflichterfüllung muss die Kundin zunächst geltend machen und allenfalls gerichtlich einklagen.

IV. Haftungsregelung unter der PSD2

Es wurde bereits darauf hingewiesen, dass die Aufnahme der Dritten Zahlungsdienstleister in den Anwendungsbereich der PSD2 zu den Hauptpunkten der Revision gehörten. Zu den Regelungspunkten zählen selbstredend auch die Haftungsfragen im Zusammenhang mit einem möglichen Datenmissbrauch, der zu einer unautorisierten Transaktion führt. Die Haftungsfrage ist aber eingebettet in einen generellen Regulierungsrahmen, der im Blick bleiben muss, wenn man die Haftunsfragen genauer anschaut.

1. Unterscheidung zwischen Aussen- und Innenverhältnis

a) Aussenverhältnis: Erstattungspflicht der Bank

Erfolgt im Zuge der Nutzung eines Zahlungsauslösedienstes eine unautorisierte Zahlung, so sind aus der Sicht der Kundin zwei Dienstleister involviert und zwei Fehlerquellen möglich: Die Bank und der Zahlungsauslösedienst. Die aus schweizerischer Sicht bestehende Schwierigkeit für die Kundin, die Fehlerquelle zu identifizieren, wird in der PSD2 mit einer wichtigen Weichenstellung ausgebügelt. Gegenüber der Kundin ist allein die Bank die Ansprechpartnerin. Sie haftet für Legitimationsmängel in gleicher Weise, wie wenn kein Dritter Zahlungsdienstleister an der Transaktion beteiligt gewesen wäre. Es gilt also das reguläre Haftungsregime der PSD2:[46] Bei einer Zahlung an einen Unbefugten hat die Kundin einen unverzüglichen Erstattungsanspruch gegenüber der Bank.[47] Die Bank hat ihrerseits für den Schaden, der ihr aufgrund der unverzüglichen Erstattungspflicht entsteht, grundsätzlich einen Schadenersatzanspruch gegenüber der Kundin. Dieser ist stufenweise geregelt:

– Die Kundin haftet voll, wenn sie in betrügerischer Absicht gehandelt hat.[48]

---

46 Art. 73, 74 PSD2. Siehe dazu EMMENEGGER, Eckpunkte, S. 53 ff.

47 Art. 73 Abs. 2 PSD2 hält die unverzügliche Erstattungspflicht der Bank für Zahlungen unter Nutzung eines ZAD ausdrücklich fest. Die Erstattung hat bis zum nächsten Geschäftstag zu erfolgen. Eine Ausnahme gilt, wenn die Bank berechtigte Gründe für den Verdacht hat, dass seitens der Kundin ein Betrug vorliegt. Selbst in diesem Fall darf sie die Gutschrift nur verweigern, wenn sie der Behörde eine entsprechende Meldung erstattet (Art. 73 Abs. 1 PSD2).

48 Art. 74 Abs. 1. Dabei gilt als Beweislastregel, dass die ordnungsgemässe Authetifizierung und die ordnungsgemässe Aufzeichnung des Zahlungsvorgangs nicht genügt, um der Kundin eine betrügerische Absicht zu unterstellen. Die PSD2 hält weiterge-

- Die Kundin haftet voll, wenn sie grobfahrlässig ihre Sicherungs- und Anzeigepflichten verletzt hat.[49] Allerdings verliert die Bank selbst in diesem Fall ihren Schadenersatzanspruch, wenn sie ihrerseits keine starke Kundenauthentifizierung verlangt hat.[50]
- Die Kundin haftet mit einem Höchstbetrag von 50 Euro, wenn sie an der unautorisierten Zahlung ein leichtes Verschulden trifft.[51]
- Trifft die Kundin kein Verschulden, so enfällt der Schadenersatzanspruch der Bank. [52]

b) Innenverhältnis: Regressansprüche gegen den Zahlungsauslösedienst

Die Bank trifft im Fall der Zahlung an einen Unbefugten gegenüber dem Kunden zwar auch dann eine unverzügliche Erstattungspflicht, wenn ein Zahlungsauslösedienst genutzt wurde. Hingegen kann sie im Innenverhältnis auf den Zahlungsauslösedienst Regress nehmen, wenn der Fehler in der Ausführung des Zahlungsvorgangs in dessen Verantwortungsbereich fällt.[53] Es gibt also für die Bank eine Möglichkeit der Schadensabwälzung; allerdings trägt sich im Innenverhältnis nach wie vor das Insolvenzrisiko des Zahlungsauslösedienstes.[54] Dieses Risiko ist zwar durch die Versicherungspflicht des Zahlungsauslösedienst reduziert,[55] aber nicht völlig ausgeschlossen.

Im Falle eines Regressanspruchs der Bank muss der Zahlungsauslösedienst nachweisen, dass der Zahlungsvorgang ordnungsgemäss ausgeführt wurde. Das bedeutet konkret: Der Zahlungsauslösedienst muss nachweisen, dass der Zahlungsvorgang innerhalb seines Zuständigkeitsbereichs authentifiziert, ordnungsgemäss aufgezeichnet und nicht durche eine technische

---

hend fest, dass die Bank «unterstützende Beweismittel» vorlegen muss, wenn sie den Betrug der Kundin nachweisen will, Art. 72 Abs. 2 PSD2.

49 Art. 74 Abs. 1 Unterabsatz 3.

50 Art. 74 Abs. 2 PSD2. Zur starken Kundenauthentifizierung siehe SCHMID, (Starke) Kundenauthentifizierung, passim.

51 Art. 74 Abs. 1 PSD2.

52 Art. 74 Abs. 1 lit. a PSD2: «wenn der Verlust, der Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstruments für den Zahler vor einer Zahlung *nicht bemerkbar* war, es sei denn, der Zahler hat selbst in betrügerischer Absicht gehandelt.».

53 Art. 73 Abs. 2 Unterabs. 2 PSD2; Erw. 73 PSD2.

54 OMLOR, ZIP 12/2016, S. 562; BÖGER, Neue Rechtsregeln, S. 277.

55 Art. 5 Abs. 2 PSD2.

Panne oder einen anderen Mangel im Zusammenhang mit seiner Dienstleistung beeinträchtigt wurde.[56] Der Zahlungsauslösedienst hat also einen Anreiz, seine Tätigkeit zu dokumentieren, um sich gegen mögliche Regressansprüche der Bank zu wappnen. Damit erhöht sich auch die Sicherheit seiner Prozesse, und damit die Sicherheit des Zahlungsverkehrs allgemein.[57]

c) Weitergehende Ansprüche der Kundin

Die Richtlinie regelt lediglich den Erstattungsanspruch der Kundin für Zahlungen an Unbefugte. Für weitere Schadenersatzansprüche, etwa für Folgeschäden oder sonstige mittelbare Beeinträchtigungen, verweist sie auf das anwendbare nationale Vertragsrecht.[58] Dabei wird ausdrücklich auf den Vertrag der Kundin mit der Bank, aber auch auf den Vertrag der Kundin mit dem Zahlungsauslösedienst verwiesen.

In der Doktrin wird diese Regelung dahingehend interpretiert, dass die Kundin gegenüber dem Zahlungsauslösedienst nicht nur Schadenersatzposten geltend machen kann, die über die Erstattungspflicht der Bank hinausgehen, sondern dass sie auch für den fehlenden Kontbetrag einen direkten Anspruch gegenüber dem Zahlungsauslösedienst hat.[59] Die praktische Bedeutung dürfte allerdings gering sein, da es einfacher sein dürfte, den Erstattungsanspruch gegen die kontoführende Hausbank durchzusetzen, die sich meist auch in geographischer Nähe der Kundin befindet.

2. Entlastung der Banken durch Abschottung?

a) Ausdrückliche Erlaubnis der Nutzung von Zahlungsauslösediensten

Angesichts der strengen Haftungsregelung für die Banken, die in einem ersten Zugriff sämtliche Risiken für unautorisierte Zahlungen tragen müssen, wäre es naheliegend, dass die Banken die Nutzung von Zahlungsauslösediensten möglichst zu verhindern suchen. Gerade dies lässt aber die Richtlinie nicht zu. Die PSD2 hält ausdrücklich fest, dass die Nutzung von Zahlungsauslösediensten unter Verwendung der personalisierten Sicher-

56 Art. 73 Abs. 2 Unterabs. 2 PSD2.
57 BÖGER, Neue Rechtsregeln, S. 277.
58 Art. 73 Abs. 3 PSD2.
59 BÖGER, Neue Rechtsregeln, S. 276.

heitsmerkmale zulässig ist.[60] Die AGB der EU-Banken enthielten bis anhin Sorgfaltspflichten und Weitergabeverbote, wie sie auch heute noch in den AGB der Schweizer Banken zu finden sind. Unter der PSD2 sind solche Weitergabeverbote im Hinblick auf die Dritten Zahlungsdienstleister nicht mehr zulässig.[61]

b) Ausdrückliche Kooperationspflicht der Banken

Angesichts der ablehenden Haltung der Kreditindustrie im Hinblick auf die Dritten Zahlungsdienstleister[62] sah sich der Richtliniengesetzgeber zudem zur ausdrücklichen Statuierung von Kooperationspflichten seitens der Banken gegenüber den Dritten Zahlungsdienstleistern veranlasst. Die Banken sind verpflichtet, Zahlungen, die über Zahlungsauslösedienste angestossen werden, gleich schnell und zu denselben Kosten («ohne Benachteiligung») auszuführen,[63] und dem Zahlungsauslösedienst alle Informationen zugänglich zu machen, über welche die Bank selbst verfügt.[64] Damit wird unter anderem gewährleistet, dass die Online-Händler auch bei Nutzung des Zahlungsauslösedienstes eine verlässliche Echtzeit-Bestätigung über den Zahlungsauftrag erhalten.[65] Die Verweigerung der Kooperationspflicht ist nur möglich bei betrügerischen oder nicht autorisierten Zugängen zum Bankkonto. Allerdings müssen dafür objektive und gebührend nachgewiesene Gründe bestehen; sodann ist der Zahler grundsätzlich unverzüglich nach der Verweigerung darüber in Kenntnis zu setzen.[66]

Die Kooperationspflichten der Bank sind zudem gemäss Richtlinie unabhängig vom Bestand einer vertraglichen Beziehung zum Zahlungsauslösedienst.[67] Das bedeutet gleichzeitig, dass die Kooperationspflicht nicht von der Zahlung eines Entgelts seitens des Zahlungsauslösedienstes abhängt.[68] Diesbezüglich hat also die Richtlinie eine Weichenstellung vorgenommen, die der Kritik der Banken an der Trittbrettfahrer-Rolle der Dritten Zahlungsdienstleister keine Rechnung trägt.

---

60 Art. 66 Abs. 1 und 3 lit. b PSD2; Erw. 69 und 96 PSD2.
61 LINARDATOS, WM Heft 7/2014, S. 301; BÖGER, Neue Rechtsregeln, S. 272.
62 Siehe etwa DEUTSCHE KREDITWIRTSCHAFT, Stellungnahme, S. 4 f.
63 Art. 66 Abs. 4 lit. c PSD2. Siehe auch Art. 66 Abs. 2 PSD2.
64 Art. 66 Abs. 4 lit. b PSD2.
65 BÖGER, Neue Rechtsregeln, S. 272.
66 Art. 68 Abs. 5 PSD2.
67 Art. 66 Abs. 5 PSD2.
68 BÖGER, Neue Rechtsregeln, S. 272.

Schliesslich ist in diesem Zusammenhang noch zu erwähnen, dass der Zahlungsauslösedienst die Authetifizierungsverfahren nutzen darf, welche die Bank für ihre Kunden verwendet.[69] Die Richtlinie stellt damit sicher, dass die Kundinnen und Kunden trotz Nutzung eines ZAD keine zusätzlichen Sicherheitsmerkmale eingeben müssen, was den Aufwand erhöht und als Marktzugangsbarriere gewirkt hätte.[70]

3. Marktzutritt zum Preis der Regulierung

Der forcierte Marktzugang der Dritten Zahlungsdienstleister und insbesondere der Zahlungsauslösedienste ist allerdings auch für diese Dienste nicht umsonst zu haben. Sie werden insgesamt in den Regelungsrahmen der PSD2 eingebunden und für sie gilt ein umfangreiches Pflichtenheft. Tatsächlich wird auch in den Erwägungen zur PSD2 als wesentliche Zielsetzung der Richtlinie die Schaffung von klaren Regelungen für Dritte Zahlungsdienstleister, insbesondere auch im Hinblick auf den Daten- und den Verbraucherschutz, definiert.[71]

a) Bewilligungspflicht und laufende Überwachung

Zunächst einmal führt die PSD2 für die Dritten Zahlungsauslösedienste eine Bewilligungspflicht ein und unterstellt sie einer laufenden Überwachung.[72] Kontoinformationsdienste unterstehen einer Registrierungspflicht.[73] Damit wird erstens einem Wildwuchs von zweifelhaften Anbietern mit zweifelhaften Geschäftsmodellen ein Riegel geschoben. Die Eckpunkte der Zulassungsbedingungen für die ZADs unterscheiden sich nicht stark von den Bewilligungsvoraussetzungen nach dem BankG/FINIG, allerdings sind sie auf die Geschäftstätigkeit der ZADs zugeschnitten. Es wird das Geschäftsmodell überprüft,[74] es müssen interne Kontrollmechanismen vorhanden sein,[75] es müssen Verfahren aufgesetzt sein für den Umgang mit sensiblen Zahlungs-

69 Art. 97 Abs. 5 PSD2.

70 BÖGER, Neue Rechtsregeln, S. 278.

71 Erw. 29 PSD2. Die finale Fassung der PSD2 enthält noch umfassendere Regelungen zum Daten- und zum Verbraucherschutz als der Kommissionsvorschlag, siehe dazu BÖGER, Neue Rechtsregeln, S. 263.

72 ZADs werden ausdrücklich als Zahlungsdienste erfasst: Anhang I Nr. 7 PSD2.

73 Art. 5, 11 Abs. 1 PSD2.

74 Art. 5 Abs. 1 lit. a PSD2.

75 Art. 5 Abs. 1 lit. e PSD2.

daten[76] und es müssen Sicherheitsprozesses bestehen für den Schutz der Zahlungsdienstnutzer.[77]

Weiter gehört zu den Bewilligungsvoraussetzungen, dass die Dritten Zahlungsdienstleister über eine Berufshaftpflichtversicherung verfügen müssen.[78] Damit wird vermieden, dass bei einer Risikoverwirklichung (betrügerische Belastungen des Kundenkontos, sonstiger Missbrauch von Kundendaten) die Anbieter ihre Zahlungsunfähigkeit anmelden und sich so aus der Verantwortung ziehen können.

b) Datenschutz

Die PSD2 enthält umfassende Regelungen hinsichtlich des Zugriffs und der Verwendung von Daten durch die Zahlungsauslösedienste und Kontoinformationsdienste. Sie müssen unter anderem sicherstellen, dass die personalisierten Sicherheitsmerkmale keiner andren Partei (ausser der Kundin und der kontoführenden Bank) zugänglich sind.[79] ZADs dürfen zudem keine sensiblen Zahlungsdaten der Kundin, namentlich ihre Bankzugangsdaten, speichern,[80] und sie dürfen nur die Daten verlangen, die für Zahlungsauslösedienstleistung notwendig sind.[81] ZADs und KIDs dürfen die erlangten Daten nicht zu anderen Zwecken als zu den ausdrücklich geforderten Dienstleistungen speichern oder verwenden.[82]

Die Datenschutzregelung ist also sehr restriktiv, denn damit wird die Verarbeitung dieser Daten zu kommerziellen Zwecken untersagt.[83] Für Kontoinformationsdienste dürfte dies aber den Kern des Geschäftsmodells bilden.

c) Identifikation des Zahlungsauslösedienstes

Zahlungsauslösedienste müssen sich gegenüber der Bank als solche identifizieren, wenn sie eine Zahlung in Auftrag geben.[84] Dies erlaubt es der

---

76 Art. 5 Abs. 1 lit. g PSD2.
77 Art. 5 Abs. 1 lit. j PSD2.
78 Art. 5 Abs. 2 PSD2 i.V.m. Anhang 1 Ziff. 7 und 8 PSD2. Siehe dazu auch Erw. 35 PSD2.
79 Art. 66 Abs. 3 lit. c, Art. 67 Abs. 2 lit. b PSD2.
80 Art. 66 Abs. 3 lit. e PSD2.
81 Art. 66 Abs. 3 lit. f.
82 Art. 66 Abs. 3 lit. g, Art. 67 Abs. 2 lit. f PSD2.
83 BÖGER, Neue Rechtsregeln, S. 274.
84 Art. 66 Abs. 3 lit. d PSD2.

Bank, den informationellen Zugriff des Zahlungsauslösedienstes auf das Konto zu beschränken, so dass nicht mehr die gesamte Zahlungshistorie eingesehen werden kann.

Ob dies über eine separate Schnittstelle erfolgt soll, oder – wie ursprünglich – ein Screen Scraping erlaubt sein soll, war lange Gegenstand von Diskussionen. Die EU-Kommission hat aber nun in ihren finalen technischen Regulierungsstandards (RTS) die Entscheidung zugunsten einer ausschliesslichen Schnittstellenlösung getroffen. Nach Ablauf der Umsetzungsfrist (14. September 2019) wird das Sreen Scraping nicht mehr erlaubt sein.[85]

d) Sicherheitspflichten

aa) Sichere Kommunikationskanäle

Sowohl die Dritten Zahlungsdienstleister als auch die Bank müssen sichere Kommunikationskanäle nutzen.[86] Die Kommission hat die Anforderungen in den RTS vom 27. November 2017 konkretisiert.[87]

bb) Qualifizierte starke Kundenauthetifizierung

Für eine erhöhte Sicherheit sorgt zudem die Pflicht, dass bei der Nutzung eines Zahlungsauslösedienstes eine starke Kundenauthetifizierung verlangt wird, die ein zusätzliches qualifizierendes Merkmal aufweist: Der Zahlungsvorgang wird dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpft.[88] Diese Pflicht ist aufsichtsrechtlicher Natur. Wie aber bereits dargelegt wurde, wirkt sie sich auch auf die Haftungslage aus.[89]

---

85 Siehe Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 (ABl Nr. L 69 v. 13.03.2018, S. 23), Art. 30, 31. Zum Verbot des Screen Scraping siehe den ausdrücklichen Hinweis im Kommissionsentwurf C(2017) 7782 final S. 3.

86 Art. 66 Abs. 3 lit. b und d PSD2.

87 Delegierte Verordnung (EU) 2018/389 der Kommission [...].

88 Art. 97 Abs. 3 PSD2. Zur starken Kundenauthentifizierung eingehend SCHMID, (Starke) Kundenauthentifizierung, S. 76.; HOFFMANN, VuR 2016, S. 243 ff.

89 Art. 74 Abs. 2 PSD2: Das Fehlen einer starken Kundenauthentifizierung führt dazu, dass die Bank den Schaden für eine unautorisierte Zahlung auch dann selbst trägt, wenn die Kundin grob fahrlässig gehandelt hat.

4. Technische Regulierungsstandards und Übergangsregelungen

In wesentlichen Punkten regelte die Richtlinie die Fragen der Dritten Zahlungdienstleister unter dem Vorbehalt dass die Einzelheiten noch durch technische Regulierungsstandards auszufüllen waren. Dies betraf insbesondere die Einzelheiten der starken Kundenauthetifizierung, die bei allen Fällen der Einschaltung von Zahlungsauslösediensten erfolgen muss.[90] Des Weiteren sollten auch die Einzelheiten der sicheren Kommunikation zwischen dem Zahlungsauslösedienst und der Bank noch durch technische Regulierungsstandards geregelt werden.[91]

Die EU-Kommission hat die RTS mittlerweile publiziert.[92] Sie gilt ab dem 14. September 2019. Für den Zugang zu den Kundenkonten über eine Schnittstelle gilt die Sonderfrist vom 14. März 2019.[93] Bis dahin gelten folgende Übergangsregelungen: Zahlungsauslösedienste, die bereits im Moment des Richtlinienerlasses tätig waren, geniessen Bestandesschutz und dürfen ihre Tätigkeit ohne besondere aufsichtsrechtliche Zulassung fortsetzen.[94] Ab dem Richtlinienerlass ist es den Banken untersagt, Zahlungsauslösedienste zu behindern oder zu blockieren.[95]

V. Schluss

Im Zahlungsverkehr hat die Digitalisierung zum Auftreten neuer Akteure auf dem Markt geführt. Unter diesen Akteuren sind solche, die für ihre Dienstleistung einen Zugang zum Bankkonto der Kundin benötigen. Das sind insbesondere die Kontoinformationsdienste und die Zahlungsauslösedienste. Das «Surfen auf der Bankinfrastruktur»[96] wirft Fragen im Hinblick auf den Wettbewerb, die Datensicherheit und den Datenschutz auf. Im Fokus des vorliegenden Beitrags standen die unautorisierten Transaktionen, die unter Nutzung eines Dritten Zahlungsdienstleisters erfolgten.

---

90 Art. 97 Abs. 3 PSD2.

91 Art. 98 Abs. 1 lit. d PSD2; Erw. 93 PSD2.

92 Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 (ABl Nr. L 69 v. 13.03.2018, S. 23).

93 Art. 38 RTS.

94 Art. 115 Abs. 5 PSD2.

95 Art. 115 Abs. 6 PSD2.

96 EMMENEGGER, Die Volkswirtschaft 6/2018, S. 48.

Dabei hat sich gezeigt, dass die Nutzung der neuen Angebote das Risiko von Phishing-Angriffen nicht exponentiell vergrössert. Würde es aber zu einem Angriff kommen, so wäre die Rechtslage in der Schweiz grundlegend anders als diejenige in der EU. In der Schweiz haben die Banken die Haftung für diese Fälle ausgeschlossen; die Nutzung eines Dritten Zahlungsdienstleisters unter Weitergabe der persönlichen Sicherheitsmerkmale ist eine Vertragsverletzung, die zur vollen Risikotragung der Kundin gegenüber der Bank führt. Anders verhält es sich in der EU. Diese hat mit der PSD2 den Markt für die Dritten Zahlungsdienste geöffnet und forciert in diesem Bereich den Wettbewerb nicht zuletzt auch durch die primäre Haftung der Banken im Falle unautorisierter Transaktionen, mit Regressmöglichkeiten auf die Dritten Zahlungsdienstleister. Gleichzeitig verlangt aber die EU hohe Sicherheitsstandards und bindet die Dritten Zahlungsdienstleister in die Regulierung ein.

Das schafft für die Nutzerinnen und Nutzer von solchen Dienstleistungen mehr Sicherheit. Im dynamischen Markt der Dienstleistungen im Zahlungsverkehr wird sich in der Schweiz mittelfristig die Diskussion um die Regulierung von neuen Akteuren nicht vermeiden lassen. Spätestens dann ist die Diskussion um die Frage, ob die Bankkundin autonom entscheiden kann, wem sie den Zugriff zu seinem Konto gewährt, wieder auf dem Tisch.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 1. Mai 2018.

BAFIN JOURNAL, Zahlungsdiensterichtlinie II: Risiken und schwerwiegende Folgen für Nutzer und Kreditinstitute, verfasst von Josef Kokert und Markus Held, Juni 2014, S. 1–47.

BAUMBACH/HOPT HGB-BEARBEITER, Handelsgesetzbuch mit GmbH & Co., Handelsklauseln, Bank- und Kapitalmarktrecht, Transportrecht (ohne Seerecht), hrsg. von Klaus J. Hopt u.a., 38. Aufl., München 2018.

BÖGER OLE, Neue Rechtsregeln für den Zahlungsverkehr, in: Volker Gross u.a. (Hrsg.), Bankrechtstag 2016, Berlin 2017, S. 193–300.

DEUTSCHE KREDITWIRTSCHAFT, Stellungnahme der Deutschen Kreditwirtschaft zum Vorschlag der Europäischen Kommission zur Änderung der EU-Zahlungsdiensterichtlinie (PSD II), S. 1–15.

EMMENEGGER SUSAN, Die EU öffnet den Markt für neue Zahlungsdienstleister, Die Volkswirtschat 6/2018, S. 48–49.

EMMENEGGER SUSAN, PSD2: Eckpunkte und Relevanz für Schweizer Finanzdienstleister, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018, S. 17–66.

GAUCH PETER/SCHLUEP WALTER R./SCHMID JÖRG/EMMENEGGER SUSAN, Schweizerisches Obligationenrecht, Allgemeiner Teil, Bd. I, 10. Aufl., Zürich 2014.

HOFFMANN JOCHEN, Kundenhaftung unter der Neufassung der Zahlungsdiensterichtlinie, VuR 2016, S. 243–254.

LINARDATOS DIMITRIOS, Der Kommisionsvorschlag für eine Zahlugsdiensterichtlinie II – Ein Überblick zu den haftungsrechtlichen Reformvorhaben, WM Heft 7/2014, S. 300–307.

OMLOR SEBASTIAN, Die zweite Zahlungsdiensterichtlinie: Revolution oder Evolution im Bankvertragsrecht?, ZIP 12/2016, S. 558–564.

SCHALLER JEAN MARC, Legitimationsmängel, in: Susan Emmenegger (Hrsg.), Bankvertragsrecht, Basel 2017, S. 45–70.

SCHMID FABIAN, (Starke) Kundenauthetifizierung: Aufsichtsrecht und Zivilrecht, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018, S. 67–85.

SCHOOR JULIUS S., «Sofortüberweisung». Sofort bezahlt. Sofort sicher?, S. 1–6.

SPINDLER GERALD/ZAHRTE KAI, Zum Entwurf für eine Überarbeitung der Zahlungsdiensterichtlinie (PSD II), BKR 2014, S. 265–271.

STENGEL CORNELIA, Unautorisierte Transaktionen in Zahlungssystemen: Am Beispiel von Twint, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018, S. 117–138.

TERLAU MATTHIAS, Die zweite Zahlungsdiensterichtlinie – zwischen technischer Innovation und Ausdehnung des Aufsichtsrechts, ZBB 2/2016, S. 122–137.

TERLAU MATTHIAS, SEPA Instant Payment – POS – und eCommerce-Abwicklung über Zahlungsauslösedienste und technische Dienstleister nach der Zweiten Zahlungsdiensterichtlinie (Payment Services Directive 2, PSD2), jurisPR-BKR 2/2016, Anm. 1, S. 1–18.

TRÜEB HANS RUDOLF/KEISER BARBARA A., Regulierung und Marktzutritt dritter Zahlungsdienstleister, S. 161–180.

Materialien

Hinweis: Zahlreiche der hier aufgeführten Dokumente sind über die gängigen Internetsuchmaschinen auffindbar. Auf die Angabe einer (häufig wechselnden) url wird daher verzichtet.

Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentizifierung und für sichere offene Standards für die Kommunikation (ABl Nr. L 69 v. 13.03.2018, S. 23).

Delegierten Verordnung (EU) …/… der Kommission vom XXX zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine stare Kundenauthentifizierung und für sichere offene Standards für die Kommunikation, C(2017) 7782 final S. 1–34.

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 (ABl Nr. L 337 v. 23.12.2015, S. 35).

Vorschlag (EU-Kommission) für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2013/36/EU und 2009/110/EG sowie zur Aufhebung der Richtlinie 2007/64/EG, COM(2013) 547 final vom 24.07.2013, S. 8.