

PSD II: Hauptproblem bleiben die TTPs

Von Kai Zahrtre und Roland Flommer

Noch im Frühsommer dieses Jahres sollen die Trilogverhandlungen zur PSD II abgeschlossen werden. Der bisherige Stand der Dinge erfüllt die Kreditwirtschaft nach wie vor mit Sorge. Denn es sieht nicht danach aus, als habe der europäische Gesetzgeber einen fairen Interessenausgleich zwischen allen Marktteilnehmern im Blick, bemängeln die Autoren. In dem Bestreben, den Wettbewerb im Zahlungsverkehr zu stärken, drohen die bisherigen Anbieter aus der Kreditwirtschaft gegenüber Drittanbietern von Zahlungsdienstleistungen benachteiligt zu werden, müssen sie doch die Infrastruktur stellen, die vom Wettbewerb mitgenutzt wird. Gleichzeitig werden durch den Kontozugang für die TTPs neue die Sicherheitsrisiken geschaffen und der Datenschutz geschwächt. Red.

Im Jahr 2000 wurde die Lissabon-Agenda formuliert, ein umfangreiches europäisches Reformprogramm, zu dem auch die Schaffung des einheitlichen Euro-Zahlungsverkehrsraums (Single Euro Payments Area, kurz Sepa) gehört. Seitdem sind eineinhalb Jahrzehnte vergangen, in denen die Europäische Kommission einen einzigartigen Marathon an Gesetzesvorhaben mit ungeahnter Komplexität in den Bereichen

Zahlungsverkehr, Girokonto, Karte und Preisregulierung gestartet hat.

Einige dieser Regulierungen waren notwendig und sinnvoll, um das Zahlungsverkehrsrecht in der Europäischen Union soweit zu harmonisieren, dass das Sepa-Projekt aufgesetzt werden konnte. Es ging dabei um die sogenannte „dritte Stufe der Euro-Einführung“. Von vornherein stand fest, dass dies enorme Anstrengungen bei allen Marktteilnehmern – vor allem aber bei der Kreditwirtschaft – zur Folge haben würde.

Neben diesen nachvollziehbaren und notwendigen Schritten enthalten die jüngsten Gesetzesvorhaben aber auch zahlreiche Anforderungen an die Kreditwirtschaft, die weit über das hinausgehen, was zur Harmonisierung des EU-Binnenmarktes und zur Sicherstellung eines effektiven Verbraucherschutzes erforderlich sind. Besonders kritisch sind hier zahlreiche Eingriffe in die Verfahrens- und Produkthoheit sowie die Preisbildung zu sehen. Sie sind aus

markt- und betriebswirtschaftlicher Sicht nicht zu rechtfertigen und stellen die Anbieter von Zahlungsverkehrsdienstleistungen vor erhebliche personelle, organisatorische und monetäre Herausforderungen. Gleichzeitig werden die Möglichkeiten der Preisgestaltung so eingeschränkt, dass ein nachhaltig ertragreiches Wirtschaften gefährdet wird.

Symptomatisch ist hier eine Konferenz in Brüssel im November 2014. Auf die Tagesordnung setzte die Kommission die Frage, ob Zahlungen in der Zukunft nicht kostenfrei sein sollten. Dort haben sich zwar die Anbietervertreter geschlossen gegen einen solchen Gedanken ausgesprochen. Aber unter dem Schlagwort eines vermeintlichen Verbraucherschutzes wird diese Forderung sicherlich nicht zum letzten Mal diskutiert worden sein.

Zielkonflikt zwischen Wettbewerb und Verbraucherschutz

Es bleibt also abzuwarten, ob die laufenden Regulierungspakete tatsächlich die Innovations- und Wettbewerbsfähigkeit im Euroraum stärken oder ob genau das Gegenteil eintritt, nämlich ein Rückzug wesentlicher Innovationstreiber aus einem zunehmend weniger lukrativen Wettbewerb.

Das umfassendste Gesetzgebungspaket im Zahlungsverkehr war die Zahlungsdiensterichtlinie (Payment Services Direc-

Zu den Autoren

Dr. Kai Zahrtre, Abteilungsdirektor, Recht des Zahlungsverkehrs und des Onlinebankings, **Roland Flommer**, Referent EU-Zahlungsverkehr, beide Deutscher Sparkassen- und Giroverband e.V., Berlin

tive, kurz PSD) aus dem Jahr 2007. Im Sommer 2013, nur vier Jahre nach der Umsetzung in Deutschland, hat die EU-Kommission bereits einen Vorschlag für die grundlegende Überarbeitung der Richtlinie vorgelegt. Dieser als PSD II bekannte Entwurf soll zukünftig Online-Bezahlverfahren umfassend regeln.

Erklärte Ziele auch dieser Novelle sind einerseits die Stärkung der Verbraucherrechte im Zahlungsverkehr und andererseits die Förderung des Zahlungsverkehrswettbewerbs im E-Commerce-Sektor. Hier liegt jedoch ein klassischer Zielkonflikt vor. Denn im Online-Zahlungsverkehr impliziert höherer Verbraucherschutz vor allen Dingen mehr Sicherheit und ein höheres Datenschutzniveau. Beides hat aber regelmäßig eine höhere technische und rechtliche Komplexität zur Folge. Und je detaillierter die Anforderungen an Sicherheit und Datenschutzvorschriften ausgestaltet sind, desto weniger Geschäftsmodelle dürften im Stande sein, diese Anforderungen zu erfüllen.

Verkürzt bedeutet dies: Je höher die Sicherheitsanforderungen, desto höher die Markteintrittsschranken. Oder umgekehrt:

je vielfältiger die Geschäftsmodelle sind, desto schwieriger wird es, hier allgemeingültige Antworten auf Fragen der Sicherheit und des Verbraucherschutzes zu finden. Einem technologieneutralen Regulierungsansatz müsste hier das Kunststück gelingen, einen goldenen Mittelweg zu finden. Blickt man aber auf die PSD II, so zeigt sich, dass das Modell, welches die Kommission im Blick hat, spürbar zulasten des Verbrauchers und deutlich zugunsten neuer Wettbewerber geht. Dieser Wettbewerb ist aber in weiten Teilen nur scheinbar. Dies wird am Beispiel der geplanten Regelung zum Kontozugriff durch dritte Zahlungsdienstleister deutlich.

Dritte Zahlungsdienstleister sollen Wettbewerb intensivieren

Dritte Zahlungsdienstleister (Third Party Payments Providers, kurz TPP) soll es nach Vorstellung des europäischen Gesetzgebers zukünftig in dreierlei Gestalt geben.

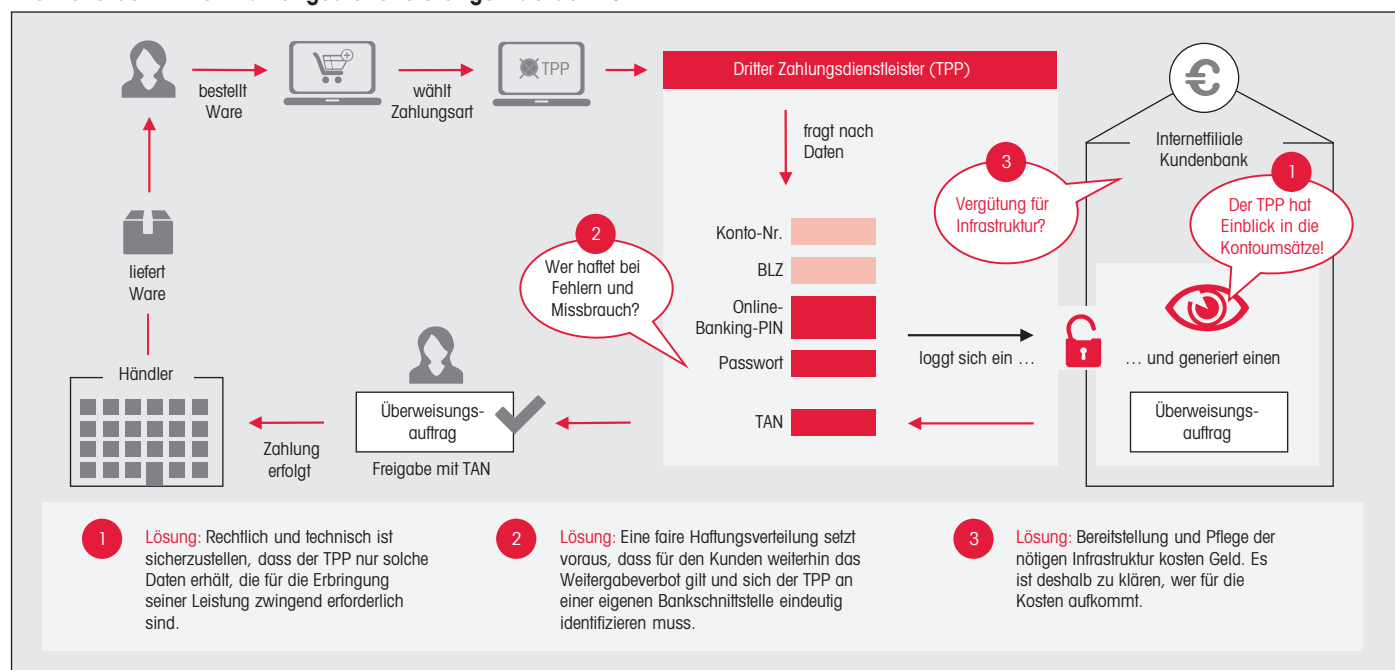
- Heute bereits am Markt aktiv sind die „Zahlungsauslösedienste“ (Payment Initiation Services, kurz PIS). Bei diesen Verfahren wählt der Bankkunde im Internet

auf einer Händlerseite als Bezahlmethode das Angebot des Drittdienstes aus. Auf Anfrage hin offenbart er zuerst seine Kontoverbindungsdaten, anhand derer der TPP prüft, ob das Konto online geführt wird. Wenn das der Fall ist, wird der Kunde nach seinen Zugangsdaten gefragt, mit denen sich der Drittdienst in die Online-Banking-Umgebung der Bank des Kunden einloggt und einen Überweisungsauftrag im Namen des Kunden initiiert.

- Neben den Zahlungsauslösediensten sollen auch sogenannte Kontoinformationsdienste (Account Information Services, kurz AIS) geregelt werden. Diese werten im Auftrag des Kunden dessen Vermögensverhältnisse aus, indem die bei (gegebenenfalls unterschiedlichen) Kreditinstituten geführten Kontoverbindungen in einer Übersicht zusammengeführt werden.

- Die letzte Kategorie bilden die Dritten Kartenemittenten (Third Party Payment Instrument Issuers, kurz TPPII). Hierbei handelt es sich um Dienstleister, die Zahlungskarten ausgeben, ohne ein dazugehöriges Konto zu führen. Die Karten sollen stattdessen an ein oder mehrere existierende Zahlungskonten bei Kreditinstituten

Die Rolle der Dritten Zahlungsdienstleister gemäß der PSD II



„andocken“ und so Kartenzahlungsvorgänge auslösen können.

Die EU-Kommission verspricht sich von allen drei Formen von Drittanbietern (TPP) eine Intensivierung des Wettbewerbs indem bestimmte relevante Zahlungsverkehrsfunktionen vom Girokonto entkoppelt werden.

Neue Angebote dürfen nicht zulasten des Datenschutzes gehen

Kunden ist oftmals nicht bewusst, was sie tun, wenn sie mit ihrer PIN den „General-schlüssel“ zu ihrem Konto aus der Hand gegeben haben. Solange nämlich, bis die PIN vom Kunden geändert wird, könnte sich derjenige, der sie einmal erhalten und – gegebenenfalls auch widerrechtlich – speichert, jederzeit ins Online-Banking des Kunden einloggen und Abfragen durchführen. Da im Online-Banking von Kreditinstituten oft die Umsätze von mehreren Monaten abrufbar sind, gewährt der Kunde, der einen Drittzahlungsdienst oder einen Kontoinformationsdienst nutzt, damit einen umfassenden Einblick in sein Zahlungsverhalten und seinen Vermögensstatus.

Diese hoch sensiblen Kontoumsatzdaten können für Dritte aus mehreren Gründen interessant sein.

■ Zum einen kann die Bonität des Kunden bewertet werden, indem Einkünfte und Ausgaben analysiert werden. Das Ergebnis wäre eine Bonitätsprognose, die vermutlich präziser und tiefergehend ist als eine Schufa-Abfrage. Die Empfänger solcher Daten könnten also nicht nur auf eigene Anfragen bei Auskunfteien verzichten, sondern sogar selbst eine Auskunftei betreiben. Ob ein Drittdienst, der so etwas tut, auch die Auskunfts- und Widerspruchsrechte des Verbrauchers in derselben Weise respektieren wird wie zum Beispiel die Schufa, müsste im Interesse der Verbraucher sichergestellt werden. Letztlich kann es der Durchsetzbarkeit aber schon entgegenstehen, wenn dieser Drittdienst nicht im Inland ansässig ist.

■ Daneben kann aus den Umsatzdaten auf Lebensgewohnheiten und persönliche Vorlieben des Kunden geschlossen werden, die für zielgerichtete Werbung interessant sind. Zwar ist im Entwurf der PSD II zu lesen, dass TPPs keine zweckfremden Auswertungen von sensiblen Kontoumsatzdaten vornehmen dürfen. Allerdings ist der Interpretationsspielraum hier hoch genug, um ein Geschäftsmodell auch für große soziale Netzwerke zu bilden. Diese haben inzwischen Lizenzen als Zahlungsdienstleister in Irland erworben, wo ein vergleichsweise niedriges Datenschutzniveau herrscht.

In anderen Regulierungen, zum Beispiel in der derzeit heftig diskutierten EU-Datenschutzgrundverordnung, wird das Prinzip der „privacy by design“ favorisiert. Damit ist gemeint, dass Datenschutz von vornherein schon technisch sichergestellt ist. So etwas wäre auch in Bezug auf die TPPs möglich. Die Europäische Zentralbank (EZB) hat vorgeschlagen, eine eigene Schnittstelle für Drittdienste einzurichten.¹⁾ Dort würden lizenzierten TPPs nur diejenigen Funktionen und Abfragen zur Verfügung stehen, die diese Dienste für ihr Angebot wirklich brauchen. Sensible Kontoumsatzdaten würden also nicht offen gelegt.

„Privacy by design“ vom Gesetzgeber bislang nicht aufgegriffen

Allerdings hat der europäische Gesetzgeber diese Idee bislang nicht aufgegriffen. Es mutet grotesk an, dass seit mehreren Jahren eine Verschärfung des Datenschutzniveaus in Europa angestrebt wird, im Zahlungsverkehrsbereich dagegen eine derart weite Flanke für Datenschutzverstöße geboten werden soll.

Das bemängelt auch Andrea Voßhoff, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit:²⁾ „Gegen die beabsichtigte Ausgestaltung bestehen datenschutzrechtlich erhebliche Bedenken, insbesondere weil ein Dritter – der Dienst-

leister – umfassenden Einblick in die Kunden-Kontoinformationen erhält. Hierbei handelt es sich um besonders sensible Finanzdaten, die auch zur Erstellung von Persönlichkeitsprofilen genutzt werden könnten. Daneben ist vorgesehen, dass der Kunde dem Zahlungsdienstleister seine personalisierten Sicherheitsmerkmale (zum Beispiel PIN und TAN) mitzuteilen hat. Dies birgt erhebliche Risiken für die Datensicherheit und eröffnet erhebliche Missbrauchsmöglichkeiten. Bei einer Datenspeicherung der Zahlungsdienste auf Servern in Staaten außerhalb der Europäischen Union könnten auch ausländische Geheimdienste einen Zugriff auf vertrauliche und sensible Kontoinformationen erhalten. Es muss daher sichergestellt werden, dass auch diesbezüglich hinreichende datenschutzrechtliche und datensicherheitsrechtliche Vorkehrungen getroffen werden.“

Wachsende Sorglosigkeit im Umgang mit Zugangsdaten

Die größten Risiken für die Verbraucher ergeben sich aber gar nicht aus möglichen Aktivitäten der Drittdienste selbst, sondern aus einer wachsenden Sorglosigkeit im Umgang mit Zugangsdaten. Dies lässt einen Anstieg der Cyber-Kriminalität befürchten.

Jeder, der eine gewisse Zeit täglich im Internet aktiv ist, braucht nur einen Blick in seinen Spamfilter oder die Abwehrprotokolle seiner Internetsicherheits-Software zu werfen, um zu sehen, dass er schon jetzt Angriffsziel zahlreicher Betrugsversuche ist. Gefälschte Mails von Banken fordern zum Beispiel zur Ausführung einer Testüberweisung auf, angeblich gesperrte Paypal-Konten sollen wieder freigeschaltet werden und Kreditkartendaten müssten angeblich aktualisiert werden. Hinzu kommt eine Flut von gefälschten Rechnungen. Trotzdem sind die Schadenszahlen infolge von Cyber-Betrug relativ gering. Das liegt daran, dass der Verbraucher heute vorsichtig ist. Kunden sind es gewohnt, ihre Zugangsdaten geheim zu halten, weil sie die Ri-

siken kennen: Die aktuelle EU-Studie zur Cyber-Sicherheit³⁾ ergibt, dass 59 Prozent der Deutschen Angst davor haben, dass ihre persönlichen Daten im Internet ausgespäht werden könnten. In keinem anderen Land wird diese Gefahr so hoch eingeschätzt. Die allerwenigsten Bank- und Sparkassenkunden geben deswegen heute PIN oder TAN an Dritte weiter.

Wettbewerb nicht auf Kosten der Sicherheit

Wenn es nun zukünftig so wäre, dass auch soziale Netzwerke, Internetshops oder Bezahldienste regelmäßig PINs von Kunden im Internet abfragen, ist es nur eine Frage der Zeit, bis der Kunde die dargestellte Sensibilität – oder schlicht den Überblick – verliert. Selbst dem technisch affinen Verbraucher ist es dann nämlich nicht mehr möglich festzustellen, ob derjenige, der ihn gerade nach seinen Bankdaten fragt, ein seriöser und mit Genehmigung der zuständigen Aufsicht arbeitender Anbieter oder aber eine der unzähligen Varianten von Schadsoftware ist. Entsprechend ist in einem Positionspapier der Verbraucherzentrale (Bundesverband) – vzbv – vom November 2013 zu lesen: „Die eigentliche Gefahr droht aus der Übung, nur für den Zugang zum eigenen Konto vorgesehene Zugangsdaten auch zum Bezahlen gegenüber Dritten zu nutzen. Den Vorteil dieser Dienste haben vor allem Webshop-Betreiber. [...] Wettbewerb darf aber nicht auf Kosten der Sicherheit durchgesetzt werden.“

Überraschenderweise hat sich die EU-Kommission bei ihrem Vorschlag für die PSD II, der den Erwägungsgründen nach vor allem auch dem Verbraucherschutz dienen sollte, gerade mit diesem Thema nicht auseinandergesetzt. In der zahlreiche Seiten umfassenden Rechtsfolgenabschätzung fehlt der Komplex Internetkriminalität vollständig. Die Europäische Zentralbank verfolgt in ihren „Empfehlungen für Kontozugriffsdienste“ einen anderen Ansatz: „Die Sicherheit des Zahlungskontos sollte nicht durch

die Dienstleistung von Kontozugriffsdiensten unterminiert werden.“⁴⁾

Wirklich ein fairer Wettbewerb?

Wenn die PSD II nun nicht in dem versprochenen Maße den Verbraucherschutz erhöht, so könnte man meinen, dass zumindest der Wettbewerbsaspekt adäquat geregelt wird. Auch hier hat der Entwurf jedoch eklatante Defizite: TPPs nutzen in nicht unerheblichem Maße die Schnittstellen und die dahinterliegende Infrastruktur des Online-Banking. Dies lassen sie sich von Internethändlern oder -käufern zu attraktiven Preisen bezahlen, ohne ihrerseits eine Nutzungsvergütung an die Kreditinstitute zu leisten. Hierdurch kommt es zu einer Verzerrung des Wettbewerbs, die schon in den fünfziger Jahren in der US-amerikanischen Wirtschaftsliteratur unter der Bezeichnung „free rider problem“ beschrieben wurde. Gemeint ist, dass Ressourcen übermäßig beansprucht und ineffizient genutzt werden, wenn der Nutzer nicht gleichzeitig Träger der Kosten ist. Dies führt in der Theorie stets zu einer Belastung der Allgemeinheit.

So etwas könnte auch hier passieren: Wenn das Gesetz die Kreditwirtschaft zwingen sollte, gratis und womöglich unter gleichzeitiger Übernahme zusätzlicher Haftungsrisiken Dritte auf Kundenkonten zugreifen zu lassen, ist aus den dargestellten Gründen ein Anstieg der Kosten und einer Zunahme von Haftungsfällen zu erwarten. Diese Mehrkosten müssen eigentlich vom Verursacher getragen werden. Sollte eine Bepreisung gegenüber dem TPP gesetzlich verboten werden, käme es folglich mittelfristig zu einer Verteuerung von online geführten Girokonten. Der Markt würde dadurch ineffizienter, und die Preissteigerung träge alle Teilnehmer – nicht nur diejenigen, die von der Existenz der TPP profitieren.

Blickt man auf den Vorschlag, dass Drittanbieter eine Zahlkarte an andere Konten „andocken“ können, so ist der Eingriff sogar noch tiefer: Bislang existiert nämlich gar nichts Vergleichbares am Markt. Dabei

gestattet es § 1 des Zahlungsdienstleistungsgesetzes (ZAG) bereits seit 2009 jedermann, eine Lizenz zu erwerben und Zahlungskarten auszugeben. Dass dies trotzdem bislang nicht ein einziger Anbieter tut, zeigt wie unattraktiv ein solches Geschäftsmodell auf einem funktionierenden Markt ist.

Bislang kein fairer Interessenausgleich

Auch diese grundsätzlichen marktwirtschaftlichen Überlegungen finden sich in der Rechtsfolgenabschätzung der EU-Kommission nicht. Die Kreditwirtschaft hat alle hier aufgeworfenen Aspekte mehrfach vorgetragen.⁵⁾ Es wird sich zeigen, ob und wie der europäische Gesetzgeber hierauf reagiert. Viel Zeit bleibt jedenfalls nicht mehr, denn die sogenannten Trilogverhandlungen zwischen EU-Kommission, Rat und Parlament sollen noch im Frühsommer zum Abschluss gebracht werden.

Als Fazit lässt sich festhalten: Im Regulierungsentwurf fehlt momentan der Versuch eines ernsthaften und fairen Interessenausgleichs zwischen Anbietern, Verbrauchern und Dritten. In einer Marktwirtschaft sollte der Gesetzgeber jedoch ein Auge darauf haben, dass alle Anbieter oder an der Leistungserbringung Beteiligten für ihren Leistungen marktgerechte Preise erzielen können, die nicht nur Kosten und Risiken abdecken, sondern vor allem auch einen Anreiz für Innovationen bieten. Entsprechend hat auch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) bereits deutlich gemacht, dass zu einer guten Leistung auch ein fairer Preis gehört. Damit wäre sowohl dem Wettbewerb als auch dem Verbraucher geholfen.

Fußnoten

¹⁾ Online abrufbar unter http://www.ecb.europa.eu/ecb/legal/pdf/en_con_2014_09_f_sign.pdf

²⁾ Vgl. Pressemitteilung vom 27. Februar 2015, online abrufbar unter http://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2015/08_NovellierungEUZahlungsdienstrichtlinie.html.

³⁾ Online abrufbar unter http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf, S. 26.

⁴⁾ Online abrufbar unter <http://www.ecb.europa.eu/pub/pdf/other/recommendationspaymentaccountaccessservicesdraft-201301en.pdf?1b2152ec95e7c86f5e55521081fda8a>

⁵⁾ DK-Papier.