Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Stellungnahme der Deutschen Kreditwirtschaft zum Vorschlag der Europäischen Kommission zur Änderung der EU-Zahlungsdiensterichtlinie (PSD II)

Stand: 2. Dezember 2013

Registriernummer der Deutschen Kreditwirtschaft
im Transparenzregister der
Europäischen Union: **52646912360-95**

Federführer:
Deutscher Sparkassen- und Giroverband e. V.
Charlottenstraße 47 | 10117 Berlin
Telefon: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

Inhalt

I. Einleitung und Überblick

Am 24. Juli 2013 hat die Europäische Kommission ihren „Vorschlag 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) 547/3) vorgelegt. Die Deutsche Kreditwirtschaft begrüßt, dass die Europäische Kommission nur in einigen Punkten Änderungsbedarf in der EU-Zahlungsdiensterichtlinie sieht. Das Zahlungsrecht in der EU ist in den EU-Mitgliedstaaten erst seit November 2009 in Kraft und es sollten nur dort Änderungen vorgenommen werden, wo besonderer Verbesserungsbedarf besteht. Ansonsten sollte das Zahlungsrecht unverändert bleiben, um Rechtssicherheit zu gewährleisten, den Anpassungsaufwand für Zahlungsdiensteanbieter und –nutzer auf das Nötigste zu beschränken und die Funktionsfähigkeit des Einheitlichen Euro Zahlungsraums SEPA zu wahren.

Aus Sicht der Deutschen Kreditwirtschaft sind bei einigen der von der Europäischen Kommission vorgeschlagenen Änderungen in der EU-Zahlungsdiensterichtlinie noch erhebliche Verbesserungen erforderlich.

Besonders hoher Handlungsbedarf besteht bei

- den Änderungen beim Erstattungsrecht des Zahlers im Lastschriftverfahren (Artikel 67 Absatz 1, siehe II.1.),
- den zivilrechtlichen Vorschriften für Drittdiensteanbieter (Artikel 58, 59 und 87, siehe II.2., und Artikel 65 Absatz 2, siehe III.1.a.) sowie
- den Vorschriften zur sicheren Kundenauthentifikation (Artikel 87, siehe II.3.).

Des Weiteren besteht Verbesserungsbedarf bei den Änderungen im Bereich Informations- und Ausführungspflichten sowie im Haftungsregime (siehe III).

II. Besonders verbesserungsbedürftige Punkte

1. Artikel 67 Absatz 1 - Das SEPA-Basislastschriftverfahren muss in seinem Bestand geschützt werden. Eine Einschränkung des unbedingten Erstattungsrechts des Zahlers ist nicht im Interesse von Zahlungsdienstnutzern und -anbietern

Mit Artikel 67 Absatz 1 letzter Unterabsatz möchte die Europäische Kommission einerseits gemäß der Forderung von Verbraucherschutzverbänden ein unbedingtes Erstattungsrecht des Verbrauchers als Zahler von SEPA-Basislastschriften (no-question-asked-Prinzip) kodifizieren und andererseits gemäß der Forderung von einzelnen Unternehmen nach Rahmenbedingungen für ein „no-refund-scheme“ das Erstattungsrecht ausschließen, wenn der Zahlungsempfänger seine vertraglichen Leistungspflichten gegenüber dem Zahler erfüllt hat. Jedoch wird der Regelungsvorschlag beiden Anliegen nicht gerecht, sondern gefährdet den Fortbestand des SEPA-Basislastschriftverfahrens:

a. Gegen eine Kodifizierung eines unbedingten achtwöchigen Erstattungsrechts des Verbrauchers als Zahler einer SEPA-Basislastschrift ist nichts einzuwenden, da bislang schon im Regelwerk zum SEPA-Basislastschriftverfahren dieses „no-question-asked“-Prinzip verbindlich vereinbart ist. Der bisherige Artikel 62 EU-Zahlungsdiensterichtlinie liefert für solche vertragliche Gestaltungen eine stabile Rechtsgrundlage.

b. Jedoch ist die in Artikel 67 Absatz 1 letzter Unterabsatz des Richtlinienvorschlags vorgesehene Einschränkung des Erstattungsrechts auf die Fälle, in denen der Händler/Dienstleister seine Leistung noch nicht erbracht hat, nicht sachgerecht:

- Eine Verknüpfung von Zahlungsverkehr und Grundgeschäft beim Erstattungsrecht führt dazu, dass das heutige unbedingte Erstattungsrecht des Zahlers beim SEPA-Basislastschriftverfahren von acht Wochen faktisch auf wenige Tage verkürzt und in etlichen Fällen abgeschafft würde. Dieser Ansatz verschlechtert die Rechtslage für den Verbraucher deutlich und entspricht überhaupt nicht der Erwartungshaltung der Zahler bei Nutzung der Lastschrift. Das SEPA-Basislastschriftverfahren würde ganz erheblich an Attraktivität verlieren, was auch zu Lasten der Zahlungsempfängerseite ginge.
- Auch wäre es von den Zahlungsdienstleistern im Massenzahlungsverkehr (in Deutschland fast 9 Mrd. Lastschriften pro Jahr) nicht umsetzbar, gemäß der Regelung in Artikel 67 Absatz 1 letzter Unterabsatz bei jeder einzelnen Lastschriftrückgabe wegen Widerspruchs des Zahlers (in Deutschland derzeit etwa 130 Millionen Vorgänge) mögliche Leistungsstörungen und Streitigkeiten aus dem Grundgeschäft zu überprüfen. Das Lastschriftverfahren könnte mit seinen bisher sehr niedrigen Kosten nicht mehr weiter betrieben werden.
- Mit einer Veränderung der Erstattungsregeln im SEPA-Basislastschriftverfahren werden alle bislang eingeholten Lastschriftmandate ihre Gültigkeit verlieren, weil diese gemäß dem SEPA-Basislastschriftregelwerk ein unbedingtes achtwöchiges Rückerstattungsrecht des Zahlers als fundamentales Prinzip zum Inhalt haben. Dies ist vor allem für die Zahlungsempfänger ein großer Nachteil, da sie von ihren Zahlern neue Lastschriftmandate einholen müssten, um den Lastschriftverkehr mit ihnen fortsetzen zu können. In Deutschland würde das geschätzt etwa einen Bestand von über 800 Millionen Mandate betreffen.

Aus allem folgt, dass Artikel 67 Absatz 1 letzter Unterabsatz dahingehend geändert werden muss, dass dort ohne Einschränkungen ein unbedingtes Erstattungsrecht des Zahlers von 8 Wochen Länge nach der Belastungsbuchung kodifiziert werden sollte. Zur Vermeidung von etwaigen Missverständnissen sollte zudem in der Vorschrift oder in einem diesbezüglichen Erwägungsgrund der Richtlinie der heute geltende Grundsatz der Trennung von Zahlungsverkehr und Grundgeschäft verankert werden, wonach der Erstattungsanspruch des Zahlers gegenüber der Zahlstelle im Zahlungsverkehr zivilrechtliche Ansprüche des Zahlungsempfängers gegen den Zahler aus dem Grundgeschäft (z.B. Bezahlung des Kaufpreises einer gekauften und gelieferten Ware) unberührt lässt.

Um dem von der Kommission angenommenen Bedürfnis nach Rahmenbedingungen für ein „no-refund-scheme“ Rechnung zu tragen, könnte in der Vorschrift unter bestimmten Voraussetzungen den Vertragsparteien – Zahlungsdienstleister, Zahler und Zahlungsempfänger - das Recht für entsprechende vertragliche Vereinbarungen eingeräumt werden. Dabei muss aber darauf geachtet werden, dass eine solche Verfahrensweise im Interbankenverhältnis mit einem eigenen Regelwerk unterlegt werden muss, das vom EPC-Regelwerk für die SEPA-Basislastschrift zu trennen ist. Nur mit einer deutlichen Unterscheidung zwischen den Verfahren wird die SEPA-Basislastschrift in ihrem Bestand gesichert und der Verbraucher kann in diesem Verfahren weiter auf sein unbedingtes Erstattungsrecht vertrauen.

2. Artikel 58 – Es müssen angemessene Sicherheitsvorkehrungen für die Nutzung von „dritten Zahlungsdienstleistern“ getroffen werden.

Die EU-Kommission möchte mit Artikel 58 den Wettbewerb im Zahlungsverkehr durch Öffnung der bilateralen technischen Kunde-Bank-Schnittstelle für „Zahlungsauslösedienste“ gemäß Artikel 4 Num-

mer 32 und „Kontoinformationsdienste“ gemäß Artikel 4 Nummer 33 fördern. Dazu sollen solche „dritten Zahlungsdienstleister“ (vgl. Artikel 4 Nummer 11, im Folgenden: Drittdienste), beispielsweise via Online-Banking, Überweisungen für den Zahler initiieren und vollen Einblick in dessen Kontoinformationen (u.a. Saldo, Buchungen) nehmen können. Der Zahler soll hierfür seine personalisierten Sicherheitsmerkmale (z.B. seine Online-PIN und -TAN) dem Drittdienst aushändigen dürfen. Die dazu von der Kommission vorgeschlagenen Reglungen, insbesondere der Artikel 58, sind noch erheblich verbesserungsbedürftig, um nicht nur dem Drittdienst ein Geschäftsmodell zu eröffnen, sondern auch die Interessen der die technische Kunde-Bank-Schnittstelle betreibenden Zahlungsdienstleister und die Interessen der Kunden ausreichend zu berücksichtigen. Es gilt, in einem stimmigen Gesamtkonzept wirtschaftliche Interessenlagen und den Schutz der Integrität der technischen Infrastruktur zum Ausgleich zu bringen. Darüber hinaus gilt es, Eigentumsrechte, Verbraucherschutz, Datenschutz und Bankgeheimnis zu beachten.

a. Anspruch des Zahlers auf Nutzung von Drittdiensten (Artikel 58 Absatz 1) – Stärkung der Kontrolle über technische Kunde-Bank-Schnittstelle

(1) Schutz der Integrität der technischen Infrastruktur

Die im Richtlinienvorschlag bislang vorgesehene unkontrollierte Öffnung der technischen Kunde-Bank-Schnittstelle für Drittdienste würde zu einer enormen Gefährdung der Integrität der technischen Infrastruktur der Zahlungsdienstleister führen. Die elektronischen Kundenzugänge von Zahlungsdienstleistern genießen heute das nahezu uneingeschränkte Vertrauen der Kunden. Ohne die Möglichkeit des kontoführenden Zahlungsdienstleisters, den Zugriff auf seine technische Infrastruktur zu kontrollieren, und damit die Verlässlichkeit, Verfügbarkeit und Sicherheit der Systeme der Bank zu gewährleisten, bestünde das Risiko des totalen Reputationsverlustes für elektronische Kundenzugänge von Zahlungsdienstleistern mit kaum absehbaren Folgen für die Kundenbeziehungen der Zahlungsdienstleister (Online-Banking ist heutzutage unverzichtbarer Bestandteil der Kundenbeziehung) und die Volkwirtschaften.

Deshalb darf nur eine kontrollierte Öffnung der technischen Kunde-Bank-Schnittstelle vorgesehen werden. Diese müsste Vorgaben in Form von Sicherheitsanforderungen und für die technischen Schnittstellen, aber auch auf organisatorischen Vorgaben zum Beispiel in Form von Notfallplänen beinhalten. Die Einhaltung dieser Vorgaben wäre vom Drittdienst in einem Zertifizierungsverfahren nachzuweisen. Nur zertifizierte Drittdienste, die sich verpflichten, die technischen und organisatorischen Vorgaben einzuhalten und erforderliche technische Anpassungen in angemessener Zeit vorzunehmen, wären berechtigt, auf die elektronischen Kundenzugänge zuzugreifen. Geeignete technische Verfahren erlaubten es, berechtigte Zugriffe von unberechtigten zu unterscheiden. Von den Aufsichtsbehörden wird diese marktübliche Vorgehensweise für Akzeptanznetzwerke im kartengestützten Zahlungsverkehr gefordert und diese haben sich seit über zwanzig Jahren bewährt.

(2) Einbeziehung des kontoführenden Zahlungsdienstleisters

Die technische Kunde-Bank-Schnittstelle (z.B. Online-Banking) beruht auf einem Vertrag zwischen Kunde und Bank und gehört sowohl der Bank als auch dem Kunden. Genauso wie die Bank diese bilaterale Schnittstelle Dritten nicht zugänglich machen darf, hat der Kunde kein al-

leiniges Verfügungsrecht, die Schnittstelle gegenüber Dritten zu öffnen. Dies gilt erst recht, wenn der Drittdienst aus der Nutzung der Schnittstelle – wie im Markt zu beobachten – eigene wirtschaftliche Vorteile zieht, indem er den aus dem Zugang gezogenen Mehrwert als eigene Dienstleistung beispielweise an Online-Händler verkauft. Deshalb muss die Erweiterung der Nutzung der Schnittstelle auch von der Zustimmung der kontoführenden Stelle abhängig sein (double consent approach).

(3) Freischaltungsweisung des Zahlers

Sollte entgegen (2) der Zahler einen uneingeschränkten Anspruch auf Einschaltung von Drittdiensten erhalten, dann sollte zum Schutz der Sicherheit der technischen Kunde-Bank-Schnittstelle und dem Schutz des Zahlers Voraussetzung für die Öffnung der Schnittstelle sein, dass der Zahler zunächst unmittelbar seinem Zahlungsdienstleister eine – dem Zahlungsauftrag vorgelagerte – Freischaltungsweisung erteilt. Der kontoführende Zahlungsdienstleister sollte erst dann die Schnittstelle zugunsten des vom Zahler benannten Drittdienstes freischalten. Damit wird gewährleistet, dass die technische Kunde-Bank-Schnittstelle nicht von vornherein offen ist, sondern erst gemäß dem ausdrücklichen Kundenwunsch für bestimmte Drittdienste zugänglich wird. Dies ist eine wichtige Vorkehrung gegen betrügerische Angriffe auf die Kunde-Bank-Schnittstelle. Zugleich werden damit die verfahrenstechnischen Voraussetzungen geschaffen, dass der Zahler jederzeit bestimmten Drittdiensten den Zugang zu der Kunde-Bank-Schnittstelle wieder verwehren kann (siehe auch (3)). Ein vergleichbarer Steuerungs- und Schutzmechanismus für den Zahler besteht heute schon beim Lastschriftverfahren (vgl. Artikel 5 Absatz 3 d) i) und iii) EU-SEPA-Verordnung[1]), wonach der Zahler die Möglichkeit hat, sein Konto hinsichtlich des Einzugs von Lastschriften von bestimmten Zahlungsempfängern zu öffnen oder zu sperren.

(4) Sperrmöglichkeiten des Zahlers

Um die Kontrollrechte des Zahlers und der Bank über die Kunde-Bank-Schnittstelle zu wahren, sollte geregelt werden,

- ein Recht des Zahlers, sein Konto für „dritte Zahlungsdienstleister“ sperren zu können, und
- ein Recht des kontoführenden Zahlungsdienstleisters, die Schnittstelle bei Verlust der aufsichtsbehördlichen Befugnis des Drittdienstes oder zur Abwehr von akuten Gefahren für die technische Kunde-Bank-Schnittstelle (z.B. Hackerangriff) selber sperren zu können.

b. Zugriff des Drittdienstes auf die personalisierten Sicherheitsmerkmale des Zahlers (Art. 58 Absatz 2 a) – Wahrung der Geheimhaltungsbedürftigkeit

(1) Zugriff des Drittdienstes auf personalisierte Sicherheitsmerkmale des Zahlers ist zur Erbringung des Zahlungsauslösedienstes nicht erforderlich

Aus Sicherheitsgründen und zur Wahrung des Bankgeheimnisses sollte der Drittdienst keinen Zugriff auf die personalisierten Sicherheitsmerkmale des Zahlers (z.B. Online-PIN/TAN) haben. Denn damit erhält er den „Generalschlüssel“ zur Erteilung von Zahlungsaufträgen und zur Ein-

[1] VERORDNUNG (EU) Nr. 260/2012 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009.

sichtnahme in alle Kontoinformationen des Zahlers (z.B. kompletter Finanzstatus des Kunden der letzten 180 Tage). Dem Drittdienst wird damit eine zu weit gehende Verfügungsgewalt über das Konto des Zahlers eingeräumt, obwohl dies nicht erforderlich ist:

- Der Zahlungsauslösedienst braucht auf Grund der Kontodeckungsinformation des kontoführenden Zahlungsdienstleisters gemäß Artikel 58 Absatz 3 überhaupt keinen Zugriff auf alle Kontoinformationen des Kunden, um seine Dienstleistungen im Online-Handel zu erbringen. Schon die Kontodeckungsinformation reicht dafür aus, dass der Zahlungsauslösedienst den Online-Händler über die erfolgreich ausgelöste Zahlung unterrichten kann, damit der Händler wiederum die Auslieferung der Ware disponieren kann.

- Auch für die Weiterleitung des Zahlungsauftrags des Zahlers zugunsten des Online-Händlers an den kontoführenden Zahlungsdienstleister braucht der Drittdienst keinen unmittelbaren Zugriff auf die personalisierten Sicherheitsmerkmale des Zahlers. Es gibt technische Verfahren, bei denen der Zahler – ohne Zugriffsmöglichkeit des Drittdienstes – seine personalisierten Sicherheitsmerkmale unmittelbar seinem Zahlungdienstleister übermittelt, obwohl der eigentliche Zahlungsauftrag des Zahlers vom Drittdienst beim kontoführenden Zahlungsdienstleister eingereicht wird. Das heißt, erst beim kontoführenden Zahlungsdienstleister werden dem eingegangenen Zahlungsauftrag die vom Zahler unmittelbar zugeleiteten personalisierten Sicherheitsmerkmale zugeleitet. Beispielsweise wäre eine so genannte „Zentrale Onlinebanking-Seite“ (ZOB, vgl. Anlage) realisierbar, über die der dritte Zahlungsdienstleister Zahlungsaufträge beim kontoführenden Zahlungsdienstleister einreichen kann, gleichwohl aber stets sichergestellt wäre, dass vom Zahler seine Online-PIN und -TAN des Kunden unmittelbar in das System des kontoführenden Zahlungsdienstleisters (z.B. Onlinebanking-Seiten der kontoführenden Stelle) eingegeben werden können. Die Spezifikation der ZOB-Schnittstelle könnte durch relevante Marktteilnehmer erfolgen. Ggf. könnte das neu geschaffene European Retail Payments Board diese Standardisierungsaktivitäten überwachen. Die Zusicherung der Einhaltung der ZOB-Schnittstellenspezifikation durch den dritten Zahlungsdienstleister wäre im Artikel 5 als Voraussetzung für die aufsichtsrechtliche Genehmigung zu nennen.

(2) Begrenzung der Verwendung von personalisierten Sicherheitsmerkmalen

Sollte entgegen (1) dem Drittdienst der Zugriff auf die personalisierten Sicherheitsmerkmale des Zahlers (z.B. Online-PIN und -TAN) gestattet werden, dann müsste zur Vermeidung von Missbrauchsrisiken und zur Wahrung der Datenschutzrechte des Zahlers zweierlei festgelegt werden: Der Kunde muss zuvor bei seinem kontoführenden Zahlungsdienstleister das Konto explizit für den von ihm ausgewählten Drittdienst freischalten lassen. Auch im Fall einer solchen Freischaltung ist festzulegen, dass der dritte Zahlungsdienstleister diese personalisierten Sicherheitsmerkmale ausschließlich zum Zweck der Übermittlung an die kontoführende Stelle nutzen darf. Damit wird ihm zugleich u.a. eine Nutzung dieser Instrumente für eine Auswertung aller Kontoinformationen des Zahlers zur Bonitätsprüfung oder Erstellung eines Verhaltensprofils sowie eine Weiterleitung von Kontoinformationen an Dritte verboten. So würde eine – heute bei einigen Drittdiensten intensiv praktizierte – Durchleuchtung des kompletten Finanzstatus des Kunden mittels automatisierter und in Sekundenschnelle ablaufender Verfahren durch den Drittdienst ebenso verhindert wie eine als Drittdienst getarnte Schadsoftware-Attacke auf ein nicht freigeschaltetes Konto.

c. Authentifizierung durch den Drittdienst gegenüber kontoführenden Zahlungsdienstleistern (Artikel 58 Absatz 3 b und Artikel 87 Absätze 2 und 3)

Dritte Zahlungsdienstleister müssen sich beim Einschalten in die Kunde-Bank-Schnittstelle beim kontoführenden Zahlungsdienstleister mit eigenen Authentifizierungsinstrumenten ausweisen, die eine eindeutige Identifizierung des Drittdienstes erlauben. Dies ist die Voraussetzung dafür, dass die Kunde-Bank-Schnittstelle nur solchen Drittdiensten zugänglich ist, die über eine aufsichtsbehördliche Genehmigung gemäß der EU-Zahlungsdiensterichtlinie verfügen und die gemäß dem Willen des Zahlers Zugang zu der Schnittstelle haben sollen. Die Authentifizierungsverfahren sollten einschlägigen ISO-Standards folgen und die EBA unter Erweiterung des Artikel 87 Absatz 3 des Richtlinienvorschlags könnte hierfür verbindliche Mindestanforderungen aufstellen.

d. Speicherverbot bzgl. Zahlungsdaten und personalisierte Sicherheitsmerkmale (Artikel 58 Absatz 2 c)

Damit der Kunde weiter tatsächlich Herr seiner Kontendaten und personalisierten Sicherheitsmerkmale bleibt, darf der Drittdienst diese Daten ausschließlich zum Zweck der Erbringung des Zahlungsauslösedienstes nutzen und muss sie nach Abschluss des Vorgangs löschen. Des Weiteren muss zur Vermeidung der Erstellung von Kundenprofilen (s. o.) es dem Drittdienst untersagt werden, die ihm aufgrund der personalisierten Sicherheitsmerkmale des Zahlers faktisch zugänglichen Kontoinformationsdaten zu lesen und auszuwerten. Eine für den Zahler völlig intransparente Durchleuchtung seiner Kontoinformationen zum Zwecke der Bewertung seines Verhaltens muss zur Wahrung des Datenschutzes ausgeschlossen sein.

e. Kontodeckungsinformation an Drittdienst (Artikel 58 Absatz 3)

Mit der Pflicht des kontoführenden Zahlungsdienstleisters, dem Drittdienst eine Kontodeckungsinformation zur Verfügung zu stellen, wird vor allem das Geschäftsmodell von am Markt bereits agierenden Online-Bezahldiensten abgesichert, ohne Einkauf einer Zahlungsgarantie durch den kontoführenden Zahlungsdienstleister dem Online-Händler eine Information zum Bezahlvorgang zu geben, damit dieser die Lieferung von Waren bzw. die Erbringung von Dienstleistungen auslösen kann. Da der Drittdienst mit der von ihm abgerufenen „Bankauskunft“ selber einen wirtschaftlichen Vorteil generiert, also Gewinne aus dem Weiterverkauf nicht öffentlicher Informationen aus Datenbanken der Zahlungsdienstleister erzielt, müsste in der Vorschrift die Möglichkeit vorgesehen werden, dass der Auskunft gebende Zahlungsdienstleister vom Auskunftsnutznießer (= Drittdienst) ein angemessenes Entgelt erheben darf. Ansonsten würde die Regelung darauf hinaus laufen, dass einerseits eine Kostenlosigkeit der Information der Bank statuiert und anderseits dem Drittdienst der Verkauf dieser Information an Händler erlaubt wird. Ein solches Ergebnis ist weder mit marktwirtschaftlichen Grundsätzen noch mit dem Schutz von Eigentumsrechten kontoführender Zahlungsdienstleister vereinbar. Überdies würde auch unrechtmäßig in die von Artikel 7 der Richtlinie 96/9/EG (sog. „EG-Datenbankschutzrichtlinie“) – vgl. auch § 87b UrhG – geschützten Urheberrechte des Datenbankherstellers (hier des kontoführenden Zahlungsdienstleisters) eingegriffen, da der kontoführende Zahlungsdienstleister eine erhebliche Investition in den Aufbau der für das Onlinebanking notwendigen Datenbankinfrastruktur getätigt hat. Nach dem deutschen § 87e UrhG ist ein Zugriff Dritter auf eine fremde Datenbank nur auf Basis eines Nutzungsvertrags mit dem Datenbankhersteller möglich.

3. Artikel 59 – Erhaltung des hohen Sicherheitsniveaus im Kartenzahlungsverkehr

Die Ausführungen zu dritten Zahlungsdienstleistern, die die Onlinebanking-Infrastruktur kontoführender Kreditinstitute nutzen, gelten sinngemäß auch für dritte Kartenemittenten und die Infrastruktur der Kartenzahlungssysteme.

a. Unklare Vorschrift

Zunächst ist anzumerken, dass der Anwendungsbereich von Artikel 59 völlig unscharf ist. Dies liegt nicht zuletzt daran, dass die Begriffe „Drittemittent“, „Kartenzahlungsdienstleistungen“ und „Zahlungskarte“ keine Legaldefinition erfahren. Hinzu kommt, dass auch aus den Erwägungsgründen nicht ersichtlich wird, welches Geschäftsmodell hier überhaupt gefördert werden soll.

b. Keine Wettbewerbsverzerrung durch so genannte „Trittbrettfahrer“

Unabhängig von der konkreten Ausgestaltung des derzeit ersichtlich noch nicht praktizierten Geschäftsmodells dritter Kartenemittenten ist unter Wettbewerbsgesichtspunkten nicht nachvollziehbar, wieso der Anbieter eines technisch unvollkommenen – und deswegen möglicherweise preisgünstigeren – Produkts wie einer Zahlungskarte ohne die dazugehörige Zahlungsverkehrsinfrastruktur (so genannter „Trittbrettfahrer“) gefördert werden soll.

c. Keine Aufweichung des Sicherheitsstandards kontoführender Institute

Sofern kontoführende Zahlungsdienstleister zukünftig dennoch verpflichtet werden sollten, den Kontozugriff mit Karten von Drittemittenten zu gestatten, ist zumindest sicherzustellen, dass die ausgegebenen Karten denselben Sicherheitsstandards entsprechen, wie die Karten, die die kontoführenden Institute selbst emittieren. Denn heute geben Kreditinstitute in Deutschland Karten aus, die den höchsten technischen Sicherheitsstandards entsprechen. Dies tun sie, da sie stets bestrebt sind, Missbräuche gering zu halten, um Kunde und Bank vor Schäden zu bewahren sowie möglichst wenig Risikokosten in die Entgelte einkalkulieren zu müssen. Die Drittemittenten haben diese Motivation nicht, da nach der Konzeption des Richtlinienvorschlags bei ihnen kaum Haftungsrisiken liegen. Sie werden daher an einer möglichst günstigen Kartenproduktion interessiert sein, da sich hohe Sicherheitsstandards für Drittemittenten selber nicht auszahlen.

4. Artikel 87 – Wahrung der Verhältnismäßigkeit bei Anforderungen an Authentifikationsinstrumente

Für die Sicherheit des Zahlungsverkehrs kommt den Authentifikationsinstrumenten des Zahlers große Bedeutung zu. Insofern ist es nachvollziehbar, dass – in Anknüpfung an den vom SecuRePay-Forum der Bankaufsichtsbehörden in der EU beschrittenen Weg – mit Artikel 87 der „verstärkten Kundenauthentifizierung“ besondere bankaufsichtsrechtliche Bedeutung zugemessen wird. Allerdings besteht auch hier noch erheblicher Verbesserungsbedarf:

a. Verstärkte Kundenauthentifizierung (Absatz 1 Satz 1)

- Maßgeblich für die Vorgabe in Artikel 87 Absatz 1 einer „verstärkten Kundenauthentifizierung“ ist die Definition in Artikel 4 Nummer 22. Diese geht über die Definition in der Empfehlung zu Internetzahlungen des SecuRePay-Forums der Bankaufsichtsbehörden in der EU vom März 2013 hinaus,

indem über die Faktoren Besitz, Wissen und Sein hinaus noch weitere zusätzliche Anforderungen formuliert werden. Diese Bedingungen sind schon von der Formulierung her schwer verständlich und technisch kaum umsetzbar. Es sollte ausreichen, auf die Erfüllung von zwei Faktoren – Besitz, Wissen oder Sein – abzustellen.

- Der Anwendungsbereich von Artikel 87 Absatz 1 beschränkt sich auf „elektronische Zahlungen", die vom Zahler „ausgelöst" werden. Die gewählte Formulierung lässt aber nicht hinreichend deutlich die gemeinten Sachverhalte erkennen. Gemeint sein dürften Online-Banking-Überweisungen und kartengestützte Zahlungen unter Einsatz von Zahlungsinstrumenten (d.h. z.B. Online-Banking-PIN/-TAN oder Debitkarte und PIN), während Lastschriften gerade ausgenommen sein sollen, die vom Zahlungsempfänger ausgelöst werden. Eine solche Abgrenzung ist sachgerecht, aber müsste deutlich aus der Vorschrift hervorgehen.

- Nach Artikel 87 Absatz 1 Satz 1 muss generell eine „verstärkte Kundenauthentifizierung" vorgesehen sein, außer die EBA-Leitlinien lassen Ausnahmen zu. Ebenso wie in den vorhergehenden Kapiteln der Richtlinie sollte bereits in der Richtlinie selber nach Relevanz differenziert werden. So sollte bei Zahlungsvorgängen mit niedrigen Beträgen (bis 30 Euro je Transaktion) eine einfache Kundenauthentifizierung ausreichen können. Denn gerade bei diesen geringwertigen Zahlungen gilt es, Aufwand und Nutzen in ein vernünftiges Verhältnis zu bringen.

- Das aufsichtsrechtliche Regime fokussiert sich zu sehr auf die Kundenauthentifikation und berücksichtigt andere in der Praxis vorkommende technische Sicherheitsvorkehrungen nicht. So kann beispielsweise eine Ein-Faktor-Authentifikation durchaus ein vergleichbares Gesamtsicherheitsniveau erreichen, wenn bei den Zahlungen zusätzlich hochentwickelte Hintergrundsysteme zum Einsatz kommen, die helfen, etwaige betrügerische Angriffe auf das Kundenkonto festzustellen bzw. zu verhindern. Folglich muss der aufsichtsrechtliche Ansatz insgesamt flexibler gestaltet werden, um der Vielfalt technischer Lösungen Rechnung zu tragen.

b. Verstärkte Kundenauthentifizierung bei Drittdiensten (Absatz 1 Sätze 2 und 3)

- Soweit zwischen Anbieter und Nutzer für elektronische Zahlungen nicht multilaterale Authentifikationsverfahren vereinbart werden (z.B. qualifizierte elektronische Signatur einer Trusted Third Party nach EU-Signaturrichtlinie bzw. deutschem Signaturgesetz), sollte jeder Zahlungsdienstleister, d.h. auch ein Drittdienst, dem Kunden eigene Authentifizierungsverfahren bereitstellen. Es ist weder unter Sicherheitsaspekten, noch vor dem Hintergrund einheitlicher Wettbewerbsbedingungen ein Grund dafür ersichtlich, warum dritten Zahlungsdienstleitern hier eine Erleichterung zukommen sollte, indem sie auf vom Zahlungsdienstleister ausschließlich dessen Kunden bereitgestellte Instrumente zurückgreifen können.

- Des Weiteren muss berücksichtigt werden, dass eine Überlassung bestimmter Authentifizierungsinstrumente durch den kontoführenden Zahlungsdienstleister technisch gar nicht möglich ist. Haben Kunde und Bank für das Online-Banking das – seit über 10 Jahren bereits vorhandene – HBCI-Verfahren unter Einsatz einer fortgeschrittenen elektronischen Signatur im Sinne der EU-Signaturrichtlinie vereinbart, dann ist aufgrund der in diesem Verfahren vorgesehenen Ende-zu-Ende-Verschlüsselung ein Zugriff Dritter auf die Signatur des Kunden zur eigenen Verwendung ausgeschlossen. Haben Kunde und Bank sich auf die Nutzung der qualifizierten elektronischen Signatur einer Trusted Third Party nach der EU-Signaturrichtlinie und dem deutschen Signaturgesetz verständigt, dann verbieten schon heute die gesetzlichen Vorschriften eine Nutzung der elektroni-

schen Signatur des Dritten durch Dritte. Die Änderung der EU-Zahlungsdiensterichtlinie darf nicht dazu führen, dass solche sicheren Authentifikationsverfahren im Online-Banking verboten werden, nur um Drittdiensten einen flächendeckenden Zugriff auf Kundenkonten zu ermöglichen. Ein solches Verbot wäre nach heutigem Stand konträr zu anderen EU-Vorschriften, keineswegs sachgerecht und sicherheitspolitisch nicht vertretbar. Daher müsste die Regelung in Satz 3 ersatzlos entfallen.

- Sollte gleichwohl an dem Ansatz festgehalten werden, müsste geklärt werden, wie der dritte Zahlungsdienstleister gegenüber der kontoführenden Stelle die Nutzung von deren Authentifizierungsverfahren vergütet. Dies sollte dem Wettbewerb und einer vertraglichen Vereinbarung überlassen bleiben.

c. Authentifizierung von Drittdiensten gegenüber dem kontoführenden Zahlungsdienstleister (Absatz 2)

Damit der Zahlungsdienstleister seinen Pflichten nach Artikel 58 Absatz 2 b nachkommen kann, muss hier nicht nur geregelt werden, dass der dritte Zahlungsdienstleister sich selbst gegenüber dem kontoführenden Zahlungsdienstleister auszuweisen hat, sondern auch in welcher Weise. Eine zweifelsfreie Authentifizierung dient dabei dem Sicherheitsinteresse aller Beteiligten, auch dem Drittdienst, der ansonsten Gefahr liefe, dass sein Name missbraucht wird. Die Aufsichtsbehörde sollte dabei sicherstellen, dass diese Authentifizierung nicht schwächer ist als diejenige, mit der sich der Kunde gegenüber den Zahlungsdienstleistern authentifiziert. So wäre beispielsweise eine Authentifikation des Drittdienstes durch seine IP-Adresse sicherheitstechnisch völlig unzureichend.

d. Leitlinien der EBA (Absatz 3)

In der Richtlinie müsste deutlicher zum Ausdruck kommen, dass die EBA-Leitlinien zu Kundenauthentifizierungsverfahren nicht auf ein einziges Instrument oder einige wenige Instrumente hinauslaufen dürfen. Denn je mehr die Zahl der zulässigen Verfahren abnimmt, desto geringer wird die Zahl der Angriffsziele für Kriminelle und desto größer wird das Risiko einer flächendeckenden Wirkung von kriminellen Angriffen. Mit anderen Worten: Eine Pluralität von geeigneten Authentifikationsverfahren schützt vor systemischen Risiken.

In Absatz 3 sollte ergänzt werden, dass EBA und EZB auch für die Beschreibung bzw. Entwicklung des Authentifikationsinstruments zuständig sind, mit dem sich der dritte Zahlungsdienstleister gemäß Absatz 2 bei der kontoführenden Stelle ausweist.

III. Weitere verbesserungsbedürftige Punkte

1. Haftungsrecht – Die Verantwortungsbereiche von Zahler, Zahlungsdienstleister und Drittdienst sind im Haftungsrecht angemessen zu berücksichtigen (Artikel 65, 66, 80)

a. Artikel 65 Absatz 2: Keine Haftung des kontoführenden Zahlungsdienstleisters für von Drittdiensten verursachten Schäden

Mit Artikel 65 Absatz 2 wird geregelt, dass der kontoführende Zahlungsdienstleister für nicht autorisierte Zahlungsvorgänge auch dann haften soll, wenn die Ursache für den Vorgang beim vom Zahler eingesetzten Zahlungsdienstleister liegt. Eine solche Haftungsübernahme ist völlig ungerechtfertigt, da

der Drittdienst gemäß dem Ansatz des Kommissionsvorschlags gerade nicht im Lager des kontoführenden Zahlungsdienstleisters, sondern alleine im Lager des Zahlers steht. Hinzu kommt, dass es bislang ausschließlich der Zahler ist, der den Drittdienst auswählt und einsetzt. Der kontoführende Zahlungsdienstleister hat bislang keinerlei Steuerungsmöglichkeiten in Bezug auf den Drittdienst. Ihm gleichwohl eine Haftung für den Drittdienst aufzubürden, konterkariert alle haftungsrechtlichen Grundsätze im Zivilrecht und ist unverhältnismäßig. Stattdessen muss eine eigenständige Haftungsregelung für den Zahler gegen den Drittdienst geschaffen werden. Nur über einen solchen unmittelbaren Anspruch wird gewährleistet, dass der Drittdienst seine Fehler gegenüber seinen Kunden selber verantworten und hierfür auch haften muss. Ein solches Haftungsmodell ist auch zusätzliche Motivation für den Dienstleister, möglichst sichere technische Verfahren und Systeme einzusetzen. Der kontoführende Zahlungsdienstleister sollte nach Artikel 65 nicht gegenüber dem Zahler haften, wenn er nachweisen kann, dass die Ursache für den nicht autorisierten Zahlungsvorgang nicht bei ihm liegt.

Sollte der oben vorgeschlagenen Lösung nicht gefolgt werden, dann müsste der in Artikel 65 Absatz 2 Satz 2 vorgesehene Regressanspruch der Zahlstelle gegenüber dem Drittdienst als Anspruchsgrundlage ausformuliert werden. Da der Drittdienst nicht im Lager der Zahlstelle steht, müssten die oben beschriebenen Nachteile für die Zahlstelle zumindest teilweise durch eine Haftungsverschärfung und eine Beweislastregelung kompensiert werden. So sollte der Drittdienst der Zahlstelle verschuldensunabhängig haften, d.h. für die Haftung reicht alleine ein ursächlicher Fehler beim Drittdienst aus. Zudem darf die Beweislast nicht bei der Zahlstelle liegen, sondern ihr Erstattungsanspruch besteht, außer der Drittdienst kann binnen einer kurzen Frist von einer Woche den Nachweis führen, dass der nicht autorisierte Zahlungsvorgang nicht auf einem Fehler bei ihm beruht.

b. Artikel 66: Keine Modifikation geltender Haftungsmaßstäbe und -höhen, um Motivation des Zahlers zum sorgfältigen Umgang mit seinen Zahlungsinstrumenten zu erhalten

Im Massenzahlungsverkehr ist es unerlässlich, bei Haftungsfragen eine Balance zu wählen, bei der der Zahler einerseits in die aus seiner Sicht relative Risikofreiheit des Systems vertrauen kann, gleichzeitig aber auch durch eine adäquate Risikobeteiligung zu Wahrung eines Mindestmaßes an Sorgfalt bei seinen Zahlungsinstrumenten angehalten wird. Dies dient einerseits der Schaffung von Akzeptanz für das Zahlverfahren und verhindert andererseits, dass Verluste aufgrund hoher Missbrauchsquoten sozialisiert werden müssen.

(1) Bei Einsatz von Zahlungsinstrumenten Mithaftungsrisiko des Zahlers von 150 EUR erhalten (Absatz 1 Satz 1)

- Für die Reduzierung der Mithaftung eines Zahlers im Fall missbräuchlich genutzter Zahlungskarten auf 150 EUR besteht kein Anlass. Diese Haftungsgrenze war angesichts der tatsächlichen Verfügungsmöglichkeiten des Zahlers schon bisher relativ niedrig, mag aber hingereicht haben, um den Zahler zur sorgsamen Verwahrung seiner Karte zu motivieren. Die vorgeschlagene Herabsetzung auf 50 EUR fällt nun aber unter die psychologisch wichtige Grenze einer Haftungsbeteiligung im dreistelligen Bereich.

- Dabei ist zu bedenken, dass diese Haftung sich nur auf den Zeitraum zwischen Verlust der Karte und Sperranzeige beim Zahlungsdienstleister bezieht (vgl. Abs. 2). Es ist nicht ersichtlich, wieso ein Kartennutzer, der den Verlust seiner Karte bemerkt, aber nicht sofort meldet und somit einen Schaden durch missbräuchliche Verwendung billigend in Kauf nimmt, fortan nur noch in Bagatellhöhe an der Haftung beteiligt werden sollte.

- Insgesamt steht zu befürchten, dass mit der Absenkung der Haftungsgrenze die Motivation des Kunden zur Abgabe einer sofortigen Sperrnachricht bei Verlust oder Missbrauch seines Zahlungsinstruments erheblich eingeschränkt wird. Die aus verspäteten Sperrnachrichten resultierenden Schäden für den Zahlungsdienstleister müssen im Ergebnis dann von allen Kunden getragen werden, da eine Risikoerhöhung Einfluss auf die Entgeltgestaltung bei Zahlungsdienstleistungen haben kann.

(2) Zahlungen mittels eines Fernkommunikationsmittels, bei dem keine verstärkte Kundenauthentifizierung verlangt wird (Absatz 1 Satz 3)

- Zunächst ist festzustellen, dass die Haftung von Zahlungsempfänger und Zahlungsdienstleister aus der Vorschrift nicht klar zum Ausdruck kommt. Offenbar ist aber eine gesamtschuldnerische Haftung für den Fall vorgesehen, dass auf der Zahlungsempfängerseite keine verstärkte Kundenauthentifizierung verlangt wird.

- Diese Haftungsregel geht fehl, indem die Haftung des Zahlers auf Betrugsszenarien reduziert wird. Grundsätzlich geht das Zahlungsdiensterecht von einer Haftung des Zahlers für Vorsatz und grobe Fahrlässigkeit aus, wobei die Beweislast hierfür idR der Zahlungsdienstleister trägt. Hierin liegt bereits eine weitgehende Verlagerung des Haftungsregimes im Vergleich zu den gewöhnlichen zivilrechtlichen Prinzipien. Wieso nun auch die Haftung des Zahlers für Vorsatz und grobe Fahrlässigkeit ausgeschlossen werden soll, wenn kein Verfahren mit verstärkter Kundenauthentifizierung angeboten wird, ist nicht ersichtlich. Dabei ist zu berücksichtigen, dass ein solches Verfahren einer aufsichtsrechtlichen Genehmigung bedarf, also geprüft und zulässig sein muss. Wenn ein Zahler, der dieses zugelassene Verfahren nutzt, jedwede Sorgfalt außer Acht lässt oder gar wissentlich und willentlich einen Schaden hervorruft, ist er in keiner Weise schutzbedürftig. Etwas anderes kann sich auch nicht aus den Besonderheiten des Verfahrens ergeben, denn ein Verfahren, das so konzipiert wäre, ist nicht denkbar bzw. wäre dann niemals durch die Aufsicht zuzulassen.

- Wollte man den Zahler aus der Haftung auch für Vorsatz und grobe Fahrlässigkeit entlassen, wäre mit einem erheblichen Anstieg der Missbrauchszahlen zu rechnen. Die hieraus resultierenden Schäden wären auf alle Verfahrensteilnehmer umzulegen, denn die subjektiven Voraussetzungen für einen Betrugstatbestand werden dem Zahler in den seltensten Fällen nachzuweisen sein.

c. Artikel 80 Absatz 1 Unterabsatz 4: Nur Ersatz des Verspätungsschadens bei verspäteter Ausführung von Zahlungen

In der Zahlungsdiensterichtlinie war bislang nicht klar genug geregelt, dass bei verspätetem Eingang einer Zahlung beim Zahlungsdienstleister des Zahlungsempfängers der Zahlungsdienstleister des Zahlers dem Zahler den Verspätungsschaden und nicht etwa den Zahlbetrag zu ersetzen hat. Dieses Problem soll scheinbar mit Artikel 80 Absatz 1 Unterabsatz 4 behoben werden. Jedoch geht die Formulierung an der Sache vorbei. Stattdessen sollte der Verspätungsschadensersatz geregelt werden.

2. Erfüllung von Informationspflichten – Zulässigkeit moderner Kommunikationsformen als Alternative zum Postversand im vorvertraglichen Bereich und bei Änderungen von Zahlungsdiensterahmenverträgen (Artikel 44, 47)

Die mit der Zahlungdiensterichtlinie (PSD I) mit Wirkung zum November 2009 eingeführten Informationspflichten haben dazu geführt, dass Bankkunden bei Eröffnung eines Girokontos oder bei AGB-Änderungen bis zu 35 Seiten Vertragstext übermittelt werden müssen, welcher zu großen Teilen schlicht den Gesetzeswortlaut wiedergibt. Eine Anpassung der Lastschriftbedingungen durch Die Deutsche Kreditwirtschaft hat 2012 so den Versand von geschätzten 2000 Tonnen Papier erforderlich gemacht.

Zahlreiche Bankkunden haben sich in diesem Zusammenhang über die „Papierverschwendung“ beschwert und von ihren Instituten gefordert, ihnen fortan keine papierhaften AGB-Änderungsangebote mehr zu unterbreiten. Wegen des in Artikel 44 angelegten Zugangserfordernisses beim Kunden ist es den Zahlungsdienstleistern aber selbst bei explizitem Kundenwunsch nicht möglich, dieser Bitte nachzukommen

Dem erklärten Ziel der Überarbeitung der EU-Zahlungsdiensterichtlinie, neue internetbasierte Verfahren zu fördern, sollte deswegen auch dahingehend Rechnung getragen werden, dass vorvertragliche Informationen dem Kunden lediglich zur Verfügung gestellt werden müssen (z.B. als Internetdownload). Um dem Interesse des Kunden an einem manifestierten Vertragswerk Rechnung zu tragen reicht es aus, ihm zunächst in einfachen Worten den Inhalt des Vertrags bzw. der Vertragsänderungen zu schildern und ihn auf ein vorvertragliches sowie später jederzeitiges (vgl. Artikel 46) Recht hinzuweisen, den vollständigen Text auch unentgeltlich in Papierform zu verlangen.

Diese ökologisch wie ökonomisch sinnvolle Änderung würde zugleich den Zahlungsdienstnutzer vor Informationsüberfrachtung schützen.

3. Regelungsbedarf für die bessere Umsetzung der Wiederbeschaffung bei Fehlüberweisungen (Artikel 79 Absatz 1)

Artikel 79 regelt (wie bisher Artikel 74 a. F.) sachgerecht, dass ein Zahlungsauftrag in Übereinstimmung mit dem Kundenidentifikator ausgeführt werden kann und ein Abgleich mit dem Namen des Zahlungsempfängers nicht erforderlich ist. Dieser Vorrang des Kundenidentifikators ist für eine vollautomatisierte Verarbeitung von Zahlungsaufträgen und zur Erfüllung der recht kurzen Ausführungsfristen weiter erforderlich.

Allerdings ist festzustellen, dass der Zahler bei fehlgeleiteten Überweisungen aufgrund Verwendung eines falschen Kundenidentifikators Probleme haben kann, sein Geld zurück zu erhalten. Die auch jetzt in Artikel 79 Absatz 3 vorgesehene Regelung zur Problemminderung hat sich als unvollständig erwiesen. Danach hat sich der Zahlungsdienstleister des Zahlers zu bemühen, soweit ihm dies vernünftigerweise zugemutet werden kann, den Geldbetrag, der Gegenstand des Zahlungsvorgangs war, wiederzuerlangen. In der Praxis ergeben sich hier Schwierigkeiten, weil der Zahlungsdienstleister des Zahlungsempfängers bislang nicht ausdrücklich zur Mitwirkung verpflichtet ist und unter Berufung auf das Bankgeheimnis Probleme sieht, Namen und Anschrift des ungerechtfertigt bereicherten Zahlungsempfängers mitzuteilen. Diese Kenntnis ist für die Rechtsverfolgung durch Zahler aber unerlässlich. Deshalb sollte in Artikel 79 Absatz 3 ergänzt werden, dass der Zahlungsdienstleister des Zahlungsempfängers zur Mitwirkung verpflichtet ist. Verweigert der Zahlungsempfänger, der den Geldbetrag,

der Gegenstand des Zahlungsvorgangs war, zu Unrecht erhalten hat, die Erstattung, hat der Zahlungsdienstleister des Zahlungsempfängers Namen und Anschrift des Zahlungsempfängers mitzuteilen.

4. Zu Artikel 3 litt. k und l: Keine neuen Ausnahmen vom Anwendungsbereich der Richtlinie

Mit Artikel 3 lit. l sollen bestimmte von Telekommunikationsunternehmen erbrachte Dienstleistungen mit Zahlungscharakter vom Anwendungsbereich der Richtlinie ausgenommen werden. Dabei wird der heute schon bestehende Ausnahmebereich in sachlicher Hinsicht dadurch erweitert, dass die angebotenen Dienste nicht mehr im Zusammenhang mit dem zur Bestellung genutzten Endgerät stehen müssen. Hierdurch wird die Ausnahme zu unbestimmt. Dabei ist auch zu berücksichtigen, dass gerade im Bereich der Telekommunikationsdienste besonders hohe Risiken der Geldwäsche und der unseriösen Dienste bestehen (z.B. durch Nutzung von Sonderrufnummern usw.). Deswegen sollte die Ausnahmeregelung für elektronische Kommunikationsnetze/-dienste gänzlich gestrichen werden. Dies ist nicht unbillig, denn Kleinbetragszahlungen sind bereits privilegiert, sodass solche Dienste in diesem Rahmen nach wie vor in den Genuss von Erleichterungen kommen. Dasselbe gilt hinsichtlich der Ausnahme in Artikel 3 lit. k.

Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Anlage

Zahlungs-Online-Banking-Webseite

Im Online-Handel haben sich verschiedene Bezahlverfahren etabliert. In den letzten Jahren ist die sogenannte „Online-Überweisung“ hinzugekommen. Hierbei können Kunden den Kaufpreis per Online-Banking-Überweisung unter Einschaltung eines sogenannten Online-Bezahldienstes entrichten. Zur Wahrung der Online-Banking-Sicherheit im Interesse von Bank und Kunde wird mit vorliegendem Konzept eine verfahrenstechnische Lösung beschrieben, bei der der Kunde die zur Einreichung der „Online-Überweisung“ erforderlichen Online-Banking-Legitimationsdaten – wie Benutzerkennung und PIN – nicht dem Online-Bezahldienst zur Verfügung zu stellen braucht, sondern diese nur unmittelbar gegenüber seiner Bank verwendet.

Dieses Modell wird nachfolgend als „Zahlungs-Online-Banking-Webseite“ (ZOB-Seite) bezeichnet. Das Prinzip der ZOB-Seite wird bereits seit mehreren Jahren von Online-Bezahldiensten in Europa erfolgreich praktiziert.

1 Konzeptskizze

Die grundlegende Idee besteht darin, den für die unmittelbare Online-Banking-Kommunikation zwischen Bank und Kunde gewidmete Online-Banking-Schnittstelle dahin gehend zu erweitern, dass berechtigte Online-Bezahldienste zur Erbringung ihrer Dienstleistungen einen eigenen Zugang zur Online-Banking-Schnittstelle (ZOB-Seite) teilnehmender Kreditinstitute erhalten.

Die ZOB-Seite beruht in ihrer Funktion auf einer für einen Online-Zahlungsvorgang reduzierten Online-Banking-Webseite. Jedes Kreditinstitut, das an Online-Bezahldiensten teilnimmt, verpflichtet sich, eine solche Zugangsseite bzw. Schnittstelle zum Online-Banking im Internet anzubieten.

Dadurch haben registrierte Online-Bezahldienste die Möglichkeit, durch Aufruf der standardisierten Schnittstelle auf den ZOB-Service teilnehmender Kreditinstitute zuzugreifen, um auf diese Weise Online-Zahlungen einzureichen (s. Abbildung 1).

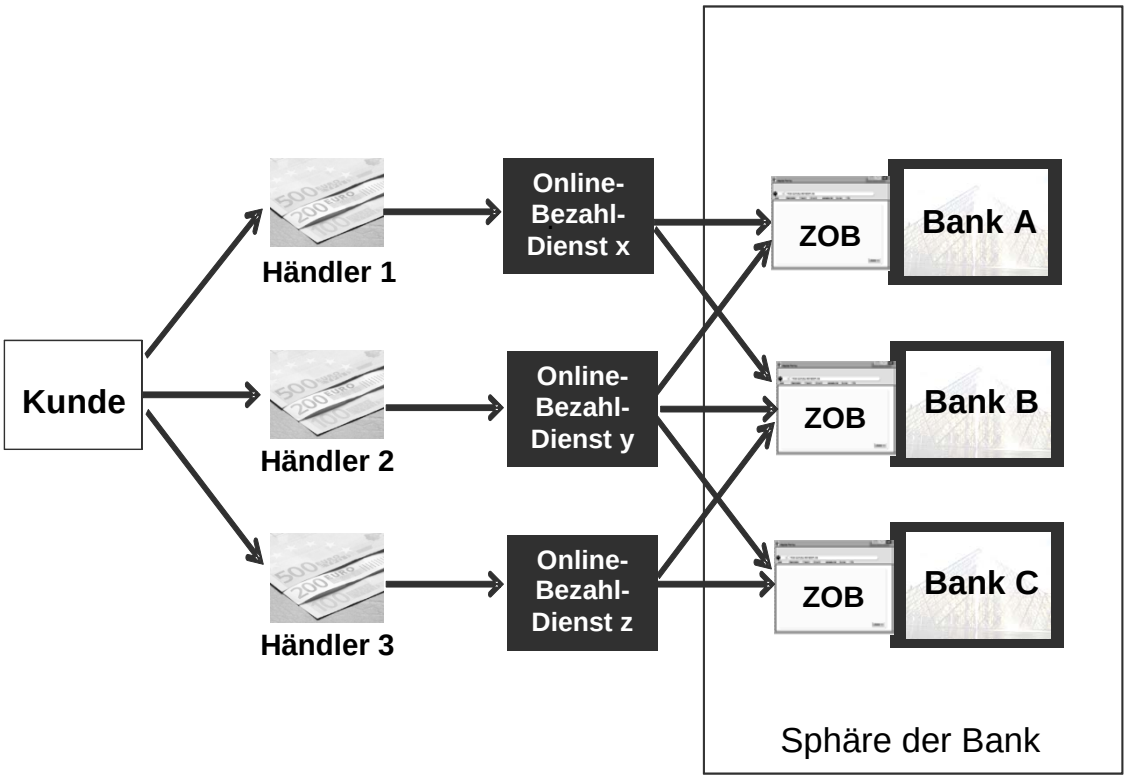

Abbildung 1: Schichtenmodell „Zahlungs-Online-Banking-Webseite“

Vorteile des Konzepts:

- Die Online-Banking-Anmeldedaten– wie Kundenkennung und PIN - werden nur in der sicheren Sphäre zwischen Kunde und Kreditinstitut ausgetauscht. Dritte erhalten keine Kenntnis dieser vertraulichen Kundendaten.
- Online-Bezahldienste erhalten keine Kenntnis über Konto- oder Umsatzdaten des Kunden, sondern lediglich die Information, ob der Zahlungs-

auftrag angenommen wurde. Im Regelfall ist diese Information für den Abschluss des Kaufvorgangs ausreichend. Abhängig von der jeweiligen Vereinbarung zwischen Online-Bezahldienst und Kreditinstitut kann das Kreditinstitut diese Bestätigung ggf. noch mit weiteren Informationen, wie bspw. einer Zahlungsgarantie, ergänzen.

- Online-Bezahldienste können auf den Aufbau aufwändiger Systeme zur Einschätzung der Ausführungswahrscheinlichkeit (Scoring-/Bonitäts-bewertungsverfahren) verzichten, sofern sie als Rückmeldung auf die Zahlungseinreichung eine Ausführungsbestätigung erhalten.

- Online-Bezahldienste müssen keine Kundendaten mehr auswerten. Sie ersparen sich so den sonst dafür erforderlichen Datenschutz. Dies erleichtert den Markeintritt insbesondere auch kleinerer Anbieter.

- Die Zugangsschnittstellen zu den ZOB-Services unterliegen einer einheitlichen von der Deutschen Kreditwirtschaft veröffentlichten Schnittstellenspezifikation (s. Kap. 3). Dadurch wird der Marktzugang für Online-Bezahldienst-Anbieter stark vereinfacht. Diese müssen nur eine einzige Schnittstelle implementieren und erhalten so in einheitlicher Weise Zugang zu den ZOB-Seiten aller teilnehmenden Kreditinstitute.

- Die Sensibilisierung der Kunden bezüglich Phishing- und Trojaner-Angriffen wird nicht beeinträchtigt, da Kunden weiterhin instruiert werden können, ihre Legitimationsdaten nur auf den ihnen bekannten Seiten ihrer Bank einzugeben (URL, Zertifikat).

- Da der Online-Bezahldienst nicht direkt an der Autorisierung der Zahlung durch den Kunden beteiligt ist, müssen nur zwischen Kunde und Institut Sorgfaltspflichten bzgl. des sicheren Umgangs mit den Legitimationsdaten vereinbart werden. Dies erleichtert auch haftungsrechtliche Fragen.

- Das Prinzip der ZOB-Seite ist unabhängig von den Sicherungsverfahren, die die Kreditinstitute anbieten, d.h. es können sowohl TAN-basierte als auch signaturbasierte Verfahren zum Einsatz kommen.

- Das Zertifizierungsverfahren, im Rahmen dessen der Bezahldienst nachweist, dass er die Anforderungen zur Verarbeitung sicherheits-relevanter Daten erfüllt, wird vereinfacht (s. Kap. 4).

- Durch die Verwendung standardisierter Schnittstellen ist die automatisierte Verarbeitung von Webseiten („Screenscraping“) überflüssig. Dadurch werden in der Vergangenheit bisweilen aufgetretene fehlerhafte Datenübermittlungen und Kundenreklamationen vermieden.

2 Technisches Modell

In der nachfolgenden Abbildung ist der Verfahrensablauf einer ZOB-Überweisung dargestellt:

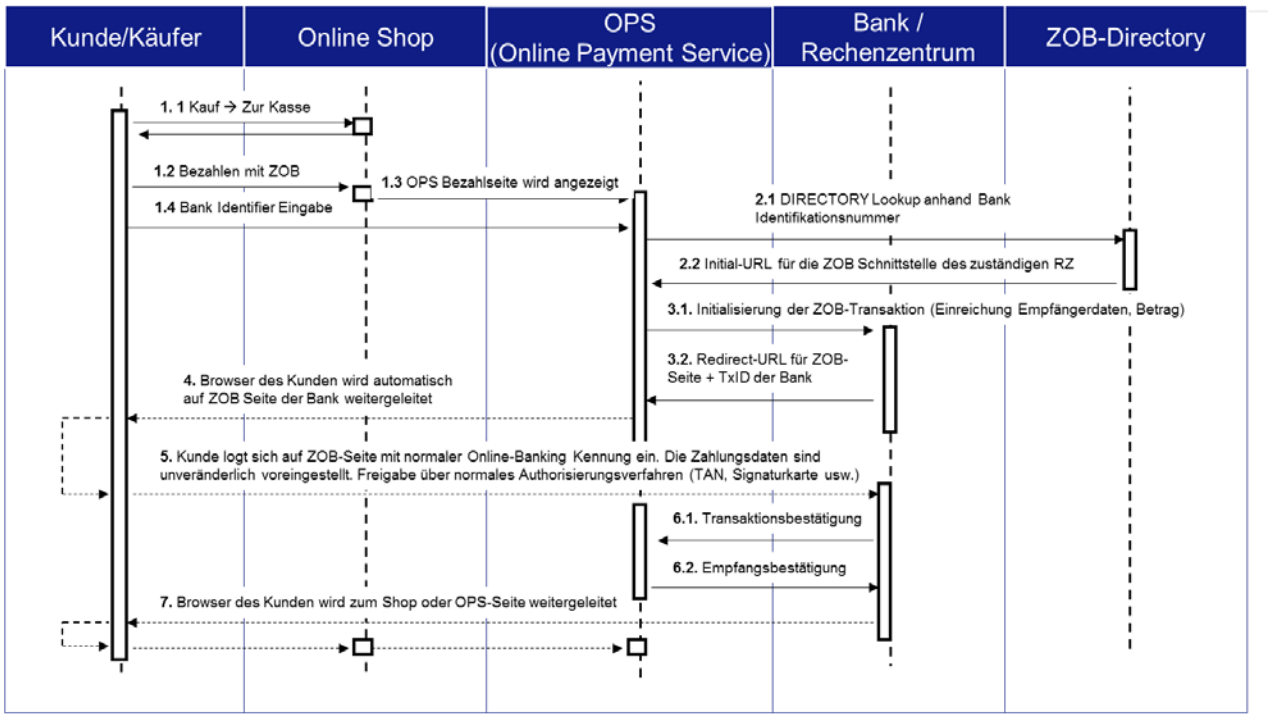

Abbildung 2: Prozessablauf einer ZOB-Transaktion

1. Der Kunde tätigt seinen Kauf auf der Seite des Online-Händlers. Der Online-Händler reicht die Rechnungsdaten aus dem Online-Kauf an den Online-Bezahldienst weiter. Der Kunde gibt auf der Seite des Bezahldienstes den Namen bzw. die Identifikation seines Kreditinstituts ein (Schritt 1).

2. Der Online-Bezahldienst ermittelt anhand eines ZOB-Verzeichnisdienstes („ZOB-Directory“) das zuständige Kreditinstitut (Schritt 2).

3. Der Online-Bezahldienst identifiziert sich gegenüber der Bank des Kunden mit der im Rahmen der DK-Zertifizierung erteilten Anbieterkennung und ggf. weiteren vereinbarten Legitimationsdaten und ruft von der Bank des Kunden deren ZOB-Service auf, übermittelt die Daten des Zahlungsauftrags und erhält die URL der ZOB-Seite (Schritt 3).

4. Der Kunde wird vom Bezahldienst auf die ZOB-Seite seiner Bank weiter geleitet. Aufgrund der bekannten Merkmale (Seitenlayout, Adresse (URL), Sicherheitszertifikat) kann der Kunde erkennen, dass er sich auf der ZOB-Seite seiner Bank befindet, also in der Sphäre seines Kreditinstituts (Schritt 4).

5. Der Kunde gibt auf der ZOB-Seite seine Zugangs- und Legitimationsdaten zum Online-Banking ein. Nach der Anmeldung wird dem Kunden der Zahlungsauftrag zur Prüfung angezeigt. Im nächsten Schritt gibt der Kunde die mit dem jeweiligen Sicherheitsverfahren generierten Legitimationsdaten ein bzw. signiert den Auftrag mit Hilfe seiner Signaturkarte und gibt damit die Ausführung des Zahlungsauftrags frei (Schritt 5).

6. Das Institut sendet eine Information über die Entgegennahme des Zahlungsauftrages über den ZOB-Service an den Online-Bezahldienst. Diese beinhaltet den Status des Zahlungsauftrags. Soweit mit dem Online-Bezahldienst weitere Nachrichteninhalte vereinbart sind, enthält die Nachricht der Bank eine Bestätigung der Ausführung des Überweisungsauftrags oder eine Zahlungsgarantie der Bank. Der Online-Banking-Vorgang ist damit abgeschlossen (Schritt 6).

7. Der Kunde wird nach dem Schließen der ZOB-Seite wieder auf die Seite des Online-Bezahldienstes oder des Händlers zurück geleitet. Der Online-Bezahldienst leitet ggf. die Zahlungsnachricht der Bank an den Online-Händler weiter (Schritt 7).

3 Schnittstellenspezifikation

Wie oben dargestellt werden die Zugangsschnittstellen zu den ZOB-Seiten der einzelnen Kreditinstitute von der Deutschen Kreditwirtschaft standardisiert. Ein Online-Bezahldienst muss daher diese Schnittstelle nur ein einziges Mal implementieren.

Die folgende XML-Schema-Datei enthält einen Vorschlag für die Schnittstellenbeschreibungen der einzelnen in Abbildung 2 dargestellten Kommunikationsschritte zwischen Online-Bezahldienst und dem ZOB-Service der Kreditinstitute. Die Strukturierung der hier aufgeführten Daten wird noch nach fachlichen und technischen Gesichtspunkten optimiert.

http://www.fints.org/spec/xmlschema/4.0/transactions/ZOB-2.xsd

Mit dem folgenden XML-Schema-Entwurf erhält ein Online-Bezahldienst eine vollständige Liste aller Banken und Sparkassen, die einen ZOB-Service anbieten. Die Liste enthält die benötigten Zugangsinformationen, wie insbesondere die URL des ZOB-Services.

http://www.fints.org/spec/xmlschema/4.0/transactions/ZOBBankList-3.xsd

4 Zertifizierungsanforderungen

Da der Online-Bezahldienst beim ZOB-Modell keine sicherheitsrelevanten Informationen, wie z.B. Bankzugangs- oder Legitimationsdaten entgegennimmt oder verarbeitet, hat er nur noch wenige Sicherheitsanforderungen zu erfüllen.

Dennoch ist eine Registrierung der Online-Bezahldienste zum ZOB-Verfahren erforderlich, da sichergestellt werden muss, dass der Online-Bezahldienst die ZOB-Seiten der Institute in korrekter Weise einbindet und sich manipulationssicher identifiziert. Mit nachgewiesener Registrierung erhält der Online-Bezahldienst eine Anbieterkennung und persönliche Identifikationsdaten, mit denen er sich gegenüber dem ZOB-Service legitimieren kann. Auf Basis dieser Registrierung kann dann eine Teilnahmevereinbarung zwischen Online-Bezahldienst und Kreditinstitut oder Konzentratoren geschlossen werden, im

Rahmen derer zusätzliche Services, wie bspw. eine Zahlungsgarantie, vereinbart werden.