Hans Rudolf Trüeb*/Barbara A. Keiser**

Regulierung und Marktzutritt dritter Zahlungsdienstleister

Inhaltsverzeichnis

* Dr. iur., LL.M., Rechtsanwalt bei Walder Wyss AG, Zürich, Titularprofessor an der Universität Zürich.
** lic. iur., Rechtsanwältin bei Walder Wyss AG, Zürich.

I. Markteintritt dritter Zahlungsdienstleister: Neue Bedürfnisse und Herausforderungen

1. Das Bedürfnis der Kunden und Anbieter nach Zahlungen im Internet

Die Anzahl Zahlungen, welche direkt im Internet abgewickelt werden, nimmt kontinuierlich zu, wobei bis anhin der elektronische Zahlungsverkehr primär durch die Banken abgewickelt wurde. Kreditkartenzahlungen über das Internet werden immer anspruchsvoller; es sind unzählige Eingaben, Passwörter und Checks erforderlich. Viele Kunden fühlen sich zunehmend unwohl, wenn sie die Daten ihrer Kreditkarte im Internet preisgeben müssen. Sie haben Angst vor Kreditkartenbetrug oder Sicherheitsbedenken wegen ihrer persönlichen Daten.[1] Alternative online Zahlungsdienste wie PayPal, paysafecard oder mywirecard bieten zwar vereinfachte Zahlungsabläufe, erfordern jedoch regelmässig ein separates Konto, das periodisch alimentiert werden muss. Das sogenannte Direct Operator Billing[2] steht nur für gewisse Dienste wie z.B. Apps zur Verfügung.

Die Kunden wünschen sich daher eine raschere und unkomplizierte Abwicklung von Zahlungen im Internet und nutzen online Zahlungsdienste nur noch, wenn die Zahlungsdienste schnell verfügbar und einfach zu bedienen sind. Drittparteien, die als Zahlungsdienstleister operieren, haben deshalb neue Geschäftsmodelle etabliert, um die Kundenbedürfnisse im online Zahlungsverkehr zu befriedigen. Die angebotenen Möglichkeiten sind nicht nur für jene Kunden interessant, die keine Kreditkarteninformationen online hinterlegen wollen, sondern auch für jene, die keine Kreditkarte besitzen.[3]

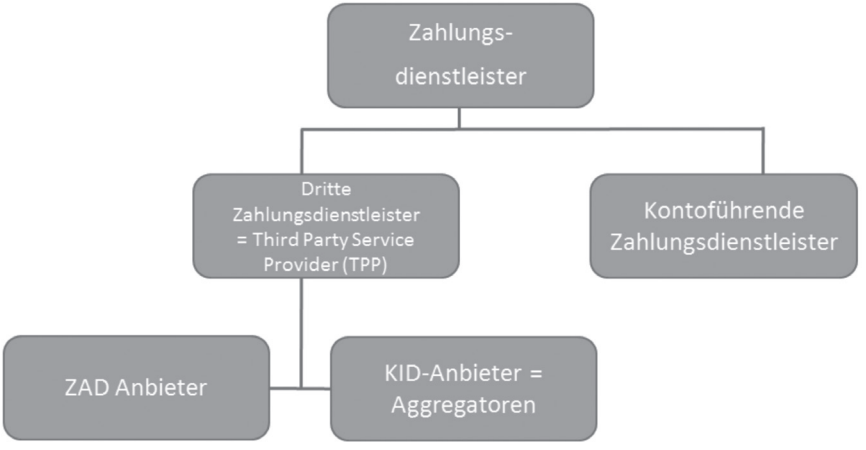
2. Begriffe und Erscheinungsformen

Den traditionellen kontoführenden Zahlungsdienstleistern, wie beispielsweise Banken oder anderen Kreditinstituten, welche für Kunden Zahlungskonten bereitstellen oder führen, stehen diese oben erwähnten dritten Zahlungsdienstleister oder Third Party Payment Service Provider (TPP) gegenüber.[4] Dritte Zahlungs-

1 http://ict.swisscom.ch/2013/09/direct-carrier-billing-apps/ (zuletzt besucht am 17.12.2014).
2 Auch «Direct Carrier Billing» genannt: Ein Zahlungsmechanismus über das Mobiltelefon mittels welchem Kunden Zahlungen, z.B. für Apps, Spiele und Musik direkt über ihr Mobiltelefonabonnement bzw. auf ihre Mobiltelefonabrechnung tätigen können.
3 http://ict.swisscom.ch/2013/09/direct-carrier-billing-apps/ (zuletzt besucht am 17.12.2014).
4 Art. 4 Abs. 1 lit. (ii) Nr. 10 Vorschlag für eine geänderte Richtlinie des Europäischen Par-

dienstleister bieten Dienste an, die im Zusammenhang mit dem Zugang zu Zahlungskonten stehen und die nicht vom kontoführenden Zahlungsdienstleister erbracht werden.[5]

Die Anbieterlandschaft präsentiert sich vereinfacht wie folgt:



2.1 Anbieter von Zahlungsauslösediensten

Dritte Zahlungsdienstleiser treten zum einen in der Form von Zahlungsauslösediensten (ZAD) auf. Die neuen Zahlungsdienstleister etablieren sich als Mittler im E-Banking, wobei die Kunden (d.h. die Zahler) die dritten Zahlungsdienstleister beauftragen können, Zahlungsaufträge in ihrem Namen direkt von ihrem Bankkonto gegenüber ihrem Kreditinstitut (d.h. ihrem kontoführenden Zahlungsdienstleister) auszulösen[6], ohne dass die Zahlungsdienstleister Besitz an den zu transferierenden Beträgen erlangen.[7] In der Sprache des europäischen Regulators ist ein Zahlungsauslösedienst ein «durch einen dritten Zahlungsdienstleister bereitgestellter Zahlungsdienst zur Ermöglichung des Zugangs zu einem Zahlungskonto, wobei der Zahler aktiv an der Auslösung der Zahlung beteiligt oder in die

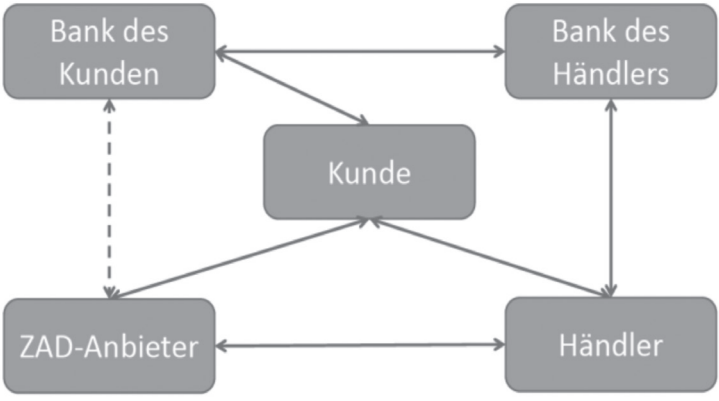
laments und des Rates über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinie 2002/65/EG, 2013/36/EU und 2009/110/EG sowie zur Aufhebung der Richtlinie 2007/64/EG (PSD 2).

5 Anhang 1 Nr. 7 PSD 2.

6 Swaantje Anneke Hass/Bernd Först, PSD beinhaltet viele neue Baustellen, diebank, FINANZMARKT, 2014, 27.

7 Grund (18) PSD 2.

Software des dritten Zahlungsdienstleisters einbezogen sein kann oder vom Zahler oder Zahlungsempfänger Zahlungsinstrumente verwendet werden können, um dem kontoführenden Zahlungsdienstleister die Daten des Zahlers zu übermitteln.»[8]



Beispiele für solche Anbieter sind giropay[9] (ein Joint Venture Deutscher Kreditinstitute) oder Sofortüberweisung.[10]

2.2 Anbieter von Kontoinformationsdiensten

Zum anderen treten dritte Zahlungsdienstleiser in der Form von Kontoinformationsdiensten (KID) auf. Die Anbieter, auch Aggregatoren genannt, holen dabei im Auftrag ihrer Kunden Kontoinformationen elektronisch beim kontoführenden Zahlungsdienstleister ab.[11] In der offiziellen Nomenklatur ist ein Kontoinformationsdienst ein «Zahlungsdienst» zur «Bereitstellung konsolidierter, benutzerfreundlicher Informationen über eines oder mehrere für einen Zahlungsdienstnutzer bei einem oder mehreren kontoführenden Zahlungsdienstleistern geführten Zahlungskonten an einen Zahlungsdienstnutzer».[12]

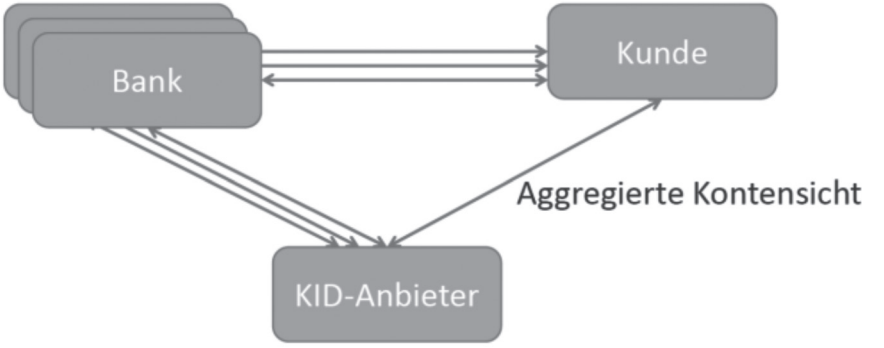
8 Art. 4 Abs. 1 lit. (ii) Nr. 32 PSD 2.

9 www.giropay.de/ (zuletzt besucht am 17.12.2014). Mit giropay kann der Kunde im Internet direkt aus einem Online-Shop heraus eine Überweisung tätigen.

10 Bei der Sofortüberweisung übermittelt der Kunde (Zahler) neben seinen Kontoinformationen seine persönliche Bank-PIN sowie eine gültige TAN über ein gesichertes Zahlformular an die Sofort AG, woraufhin diese bei der Bank die eigentliche Transaktion im Namen des Kunden ausführt. Dabei ruft die Sofort AG neben dem Kontostand noch weitere Daten zur Prüfung der Kontodeckung ab, https://www.sofort.de/ (zuletzt besucht am 17.12.2014).

11 Hass/Först (Fn 6), 28.

12 Art. 4 Abs. 1 lit. (ii) Nr. 33 PSD 2.



Beispiele dafür sind Steuerberater, die im Auftrag ihrer Kunden Kontodaten einholen und verarbeiten[13] oder Finanzplaner, wie z.B. die Qontis AG[14] welche eine bankübergreifende Übersicht über alle privaten Konten sowie Einnahmen und Ausgaben zur Verfügung stellen[15], die unter anderem Budgetierungstools, Liquiditätspläne oder Kostenoptimierungsvorschläge aufgezeigt.[16]

2.3 Neue Herausforderungen an der Kunde-Bank Schnittstelle

Um die oben beschriebenen neuen Geschäftsfelder zu erschliessen, benötigen die dritten Zahlungsdienstleister Zugang zu den Schnittstellen der Bank zu ihren Kunden. Heute besteht zwischen den Kreditinstituten, d.h. den kontoführenden Zahlungsdienstleistern, und den Kunden, d.h. den Zahlern, ein direktes Vertragsverhältnis, welches zu respektieren ist.[17] Die bilaterale Schnittstelle zwischen dem Kreditinstitut und Kunden genügt dabei sehr hohen, rechtlich geregelten Sicherheitsstandards, womit eine volle Kontrolle der Authentisierung, Autorisierung sowie Verschlüsselung des elektronischen Zahlungsverkehrs durch das Kreditinstitut gewährleistet werden kann.[18] Der Kunde muss sich stets mittels seiner

13 Hass/Först (Fn 6), 28.
14 Die Qontis AG bietet eine Personal Finance Management (PFM)-Online-Plattform, die es den Nutzern ermöglicht, ihre privaten Finanzen zu verwalten, www.qontis.ch/ (zuletzt besucht am 17.12.2014).
15 Hannes P. Lubich, Sicherer Umgang mit Kontoinformation und Zahlungsauslösung, COMPLIANCE/CLEARIT, 2014, 11; www.qontis.ch/ (zuletzt besucht am 17.12.2014).
16 http://www.nzz.ch/meinung/in-eigener-sache/nzz-gruendet-plattform-fuer-private-finanzverwaltung-1.18 130 158 (zuletzt besucht am 17.12.2014).
17 Hass/Först (Fn. 6), 28.
18 Lubich (Fn. 15), 11.

persönlichen Zugangsdaten direkt gegenüber dem Kreditinstitut legitimieren.[19] Dadurch wird der Schutz des Kunden, seiner Daten und seiner Legitimationsmittel gewährleistet. Zudem stellen die Kreditinstitute sicher, dass regulatorische Anforderungen eingehalten werden.

Die neuen Zahlungsdienstleister im elektronischen Zahlungsverkehr sind in der Schweiz nicht reguliert und unterliegen nicht den gleichen Standards wie die Kreditinstitute. Diese sind daher besorgt, dass eine unkontrollierte Öffnung der Kunde-Bank-Schnittstellen für dritte Zahlungsdienstleister zu vermehrten Unsicherheiten im Schutz der Kundendaten sowie Betrugsvorfällen führen könnte.[20]

Unter anderem bringt eine solche Öffnung die nachstehend beschriebenen Herausforderungen mit sich:

a Höchstpersönlichkeit der Legitimations- bzw. Authentisierungsmittel

Die Höchstpersönlichkeit der Legitimations- bzw. Authentisierungsmittel ist Dreh- und Angelpunkt des beidseitigen Vertrauens in die E-Banking Lösungen. Der Kunde ist gehalten, sich stets mittels seiner persönlichen Zugangsdaten direkt gegenüber dem Kreditinstitut zu legitimieren. Echte oder unechte Vertretung ist Sand im Getriebe des E-Banking. Die Bank muss sich unbedingt darauf verlassen können, dass auf der anderen Seite der Verbindung der Kunde sitzt und kein Dritter.

Die dritten Zahlungsdienstleister setzen ihre Geschäftsmodelle hingegen mittels sogenannter Impersonation um. Das bedeutet, dass der Kunde dem dritten Zahlungsdienstleister seine persönlichen Legitimationsmittel, welche im bilateralen Verhältnis mit dem Kreditinstitut bestehen, zur Verfügung stellt und der dritte Zahlungsdienstleister diese im Namen des Kunden bei der Interaktion mit dem Kreditinstitut verwendet. Dieser Vorgang vereinfacht zwar die Abwicklung der von den dritten Zahlungsdienstleister angebotenen Dienstleistungen, hat im Gegenzug aber die «Man in the Middle»-Problematik zur Folge; die Kreditinstitute können nicht mehr unterscheiden, ob sie mit ihrem Kunden oder einem Dritten agieren. Der «Man in the Middle» kann nicht nur ein legitimer Zahlungsdienstleister sein, sondern auch eine kriminelle Organisation, die ohne Wissen und Voll-

19 Hass/Först (Fn. 6), 28.
20 Hass/Först (Fn. 6), 28; Lubich (Fn. 15), 11.

macht des Kontoinhabers handelt. Damit würden kriminellen Machenschaften wie dem Phishing[21] oder Spoofing[22] Tür und Tor geöffnet.[23]

b Bankkundendaten und Cloud Computing

Ein weiteres Problem, welches sich durch den Markteintritt der dritten Zahlungsdienstleister stellt, ist der Schutz der Kundendaten. Die Kreditinstitute verfügen über streng geregelte sowie aufwendig gesicherte Systeme zur Speicherung und Bearbeitung der Kundendaten, bei welchen sämtliche Transaktionen überwacht werden können.[24] Zudem unterliegen die Kreditinstitute strengen Aufklärungspflichten gegenüber ihren Kunden bezüglich des Umgangs mit deren Daten.[25] Die dritten Zahlungsdienstleister hingegen bedienen sich häufig der Mittel des Cloud Computing, um Kundendaten günstig und jederzeit verfügbar bearbeiten zu können.[26] Dadurch wird ein schwer kontrollierbares Terrain geschaffen, welches sowohl den Diebstahl von sehr sensitiven Kundendaten als auch deren Missbrauch für Social-Engineering Angriffe begünstigt.[27] Schliesslich ist nicht geregelt, wer schlussendlich die Verantwortung für den Umgang mit den Kundendaten innerhalb solcher ubiquitärer Datenwolken tragen soll. Das Bankkundengeheimnis dürfte im Ausland nicht durchsetzbar sein.

21 Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen, Rolf H. Weber, E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, 2. Aufl., Zürich 2010, 540.

22 Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität, Weber (Fn. 21), 539.

23 Lubich (Fn. 15), 11.

24 Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2008/7, Auslagerung von Geschäftsbereichen bei Banken.

25 FINMA, Rundschreiben 2008/21, Operationelle Risiken Banken, Anhang 3.

26 Ins Internet ausgelagerte IT-Systeme, http://de.wikipedia.org/wiki/Cloud_Computing (zuletzt besucht am 17.12.2014).

27 Lubich (Fn. 15), 11.

II. Regulierung

1. Bestehende Regulierung im einheitlichen Euro-Zahlungsverkehrsraum

1.1 SEPA

a Definition von SEPA

Die Europäische Kommission und die Europäische Zentralbank (EZB) haben in den Jahren nach der Einführung des Euro am 1. Januar 2002 einen einheitlichen Euro-Zahlungsverkehrsraum (Single Euro Payments Area [SEPA[28]]) geschaffen. Ziel von SEPA ist die Standardisierung des bargeldlosen, grenzüberschreitenden Zahlungsverkehrs in Euro zwischen Staaten, deren Finanzinstitute an SEPA teilnehmen, so dass dieser ebenso einfach, effizient und sicher abgewickelt werden kann wie der nationale Zahlungsverkehr der einzelnen Staaten.[29]

b SEPA Scheme Rulebooks

Koordinations- und Entscheidungsgremium für den Zahlungsverkehr ist der European Payment Council (EPC); ein Zusammenschluss von Banken und Bankenverbänden aus ganz Europa. Zur Umsetzung des integrierten Euro-Zahlungsverkehrsmarkts hat der EPC die Verfahren für SEPA-Überweisungen und SEPA-Lastschriften entwickelt, welche durch mehrere EPC-Regelwerke, die sogenannten SEPA Scheme Rulebooks definiert wurden.[30] Konkret bestehen folgende SEPA-Zahlungsinstrumente sowie dazugehörende Regelwerke: Für die SEPA-Überweisungen (SEPA Credit Transfer) besteht das SEPA Credit Transfer Scheme Rulebook, welches im Januar 2008 eingeführt wurde. Für das SEPA-Lastschriftenverfahren (SEPA Direct Debit) wurden im November 2009 die SEPA Direct Debit Scheme Rulebooks eingeführt. Zudem hat der EPC mit dem SEPA Cards Framework die Rahmenbedingungen für den SEPA-konformen Karteneinsatz festgelegt.

28 Martin Hess/Barbara Keiser, Euro-Zahlungen gemäss den SEPA-Rulebooks durch Schweizer Finanzinstitute, SZW, 2009, 156.

29 Hess/Keiser (Fn. 28), 156.

30 http://www.sepa.ch/de/home/sepa.html (zuletzt besucht am 17.12.2014).

c Geltungsbereich

SEPA umfasst 28 EU-Länder sowie Island, Liechtenstein, Norwegen, Monaco, Republik San Marino und die Schweiz. Vertragspartei der SEPA Scheme Rulebooks sind aber nicht Staaten, sondern die unterzeichnenden Finanzinstitute. Die SEPA Scheme Rulebooks regeln auf vertraglicher Basis das Verhältnis zwischen den Finanzinstituten. Jedes Finanzinstitut, welches an den SEPA-Verfahren teilnehmen möchte, muss den SEPA Adherence Agreements beitreten. Dies sind multilaterale Verträge nach belgischem Recht, welche mit dem EPC und den an SEPA teilnehmenden Finanzinstituten abgeschlossen werden. Durch den Vertragsbeitritt werden die SEPA Scheme Rulebooks zum Vertragsinhalt und die Finanzinstitute sichern deren vorbehaltlose Einhaltung zu.[31]

1.2 PSD

a Definition der PSD

Am 1. November 2009 ist auf europäischer Ebene zudem die Zahlungsdienstrichtlinie (Directive on Payment Services oder PSD)[32] in Kraft getreten. Mit der PSD werden im Wesentlichen zwei Hauptziele verfolgt; zum einen die Liberalisierung (Marktöffnung) und zum anderen die Rechtsangleichung (Harmonisierung), so dass grenzüberschreitende Zahlungen innerhalb der Europäischen Union so einfach, effizient und sicher werden wie nationale Zahlungen innerhalb eines Mitgliedstaates. Die PSD bildet damit eine einheitliche rechtliche Grundlage für die Schaffung des EU-weiten Zahlungsverkehrs im Rahmen der SEPA-Verfahren sowie die rechtliche Basis für den einheitlichen Euro-Zahlungsverkehrsraum, sprich SEPA. Die detaillierten Regelungen der Zahlungsinstrumente finden sich dann wiederum sich in den SEPA Scheme Rulebooks.[33]

b Geltungsbereich

Die PSD gilt für sämtliche EU- und EWR-Länder. Sie findet auf die Schweiz indessen nicht direkt Anwendung, da die Schweiz weder Mitglied der EU noch des EWR ist und sich auch keine entsprechende Verpflichtung in den bilateralen Abkommen mit der Europäischen Gemeinschaft findet.[34]

31 Hess/Keiser (Fn. 28), 157.
32 Richtlinie 2007/64/EG vom 13. November 2007 über Zahlungsdienste im Binnenmarkt.
33 Europäische Kommission, Bank- und Finanzwesen, Richtlinie über Zahlungsdienste (PSD), http://ec.europa.eu/finance/payments/framework/index_de.htm (zuletzt besucht am 17.12.2014); Hess/Keiser (Fn. 28), 155.
34 Hess/Keiser (Fn. 28), 154.

2. Erweiterung der Regulierung auf der Ebene der EU

Der Markteintritt der dritten Zahlungsdienstleister sowie die sich daraus ergebenden neuen Herausforderungen werfen die Frage nach einer Regulierung dieser neuen Angebote auf. Es ist insbesondere zu regeln, wie sich solche TPP gegenüber den Banken authentisieren, ob und allenfalls auf welche Weise persönliche Legitimations- bzw. Authentisierungsmittel verwendet werden dürfen und wie der Umgang mit Kundendaten geregelt werden soll. Auch die EU hat den diesbezüglichen Handlungsbedarf erkannt (vgl. untenstehende Abschnitte zur PSD II: II.2.1 ff.).

2.1 PSD 2

Aufgrund der aktuellen technischen Entwicklungen im elektronischen Zahlungsverkehr sowie der stetigen Zunahme von Zahlungen im Internet hat die EU-Kommission die PSD umfangreich überarbeitet mit dem Ziel, elektronische Zahlungen für Einzelhändler und Verbraucher billiger und sicherer zu machen. Der Vorschlag für eine überarbeitete Richtlinie über Zahlungsdienste (PSD 2) wurde vom EU-Parlament am 3. April 2014 angenommen, und mit ihrer Verabschiedung wird Anfang 2015 gerechnet. Die Mitgliedstaaten sowie Unternehmen haben danach voraussichtlich zwei Jahre Zeit, um die PSD 2 umzusetzen. Die PSD 2 sieht eine Ausweitung ihres Anwendungsbereichs sowie eine Einschränkung bisheriger Ausnahmen vor.[35]

a Erweiterter Anwendungsbereich

Dritter Zahlungsdienstleister

Von massgeblicher Tragweite für Banken und andere Kreditinstitute ist die Aufnahme der dritten Zahlungsdienstleister, wie die Anbieter von Zahlungsauslösediensten oder Kontoinformationsdiensten[36] in den Anwendungsbereich der Richtlinie.[37] Die dritten Zahlungsdienstleister sollen gleichzeitig einen (regulierten) Zugang zur Schnittstelle zwischen Kunde und Kreditinstitut erhalten. Die hierfür notwendige Öffnung der Schnittstelle bildet Gegenstand anhaltender Diskussionen.[38]

35 CMS Hasche Sigle, Änderung der Zahlungsdienstrichtlinie (PSD 2) bringt weitere Regulierung im Bereich Zahlungsverkehr und E-Commerce, CMS Deutschland bloggt, 2014.
36 Vgl. Definitionen der Begriffe oben unter I.2.
37 Art. 2 i.V.m. Art. 4 Abs. 1 lit. (ii), Nr. 9–11 PSD 2.
38 Hass/Först (Fn. 6), 27.

Neuregelungen, insbesondere der Legitimation bzw. Authentisierung

Im Hinblick auf die Öffnung der Schnittstellen sieht die PSD 2 eine verstärkte Authentifizierung vor. Zum einen muss sich der dritte Zahlungsdienstleister gegenüber dem kontoführenden Zahlungsdienstleister, also dem Kreditinstitut des Kunden, auf unmissverständliche Weise authentisieren.[39] Zum anderen soll die Kundenauthentisierung auf zwei von drei der folgenden Ebenen geschehen: Wissen (beispielsweise Passwörter, Codes und persönliche Identifikationsmittel), Besitz (beispielsweise Token, Chipkarte oder Mobiltelefon) und Biometrie (beispielsweis Fingerabdrücke oder Gesichtserkennungsverfahren).[40] Zudem darf der dritte Zahlungsdienstleister keine sensiblen Zahlungsdaten oder personalisierte Sicherheitsdaten des Zahlungsdienstnutzers, also des Zahlers oder Zahlungsempfängers, speichern und muss gewährleisten, dass solche personalisierte Sicherheitsmerkmale keiner anderen Partei zugänglich sind.[41]

Nebst den Vorschriften zur verstärkten Kundenauthentifizierung, sieht die PSD 2 für die Zulassung von Zahlungsdienstleistern ein Eigenkapital von mindestens Euro 50 000.– vor. Der Betrag von Euro 50 000.– darf zu keinem Zeitpunkt unterschritten werden.[42] Diese Summe scheint sowohl aus Gründen des Kapitalschutzes als auch im Hinblick auf Haftungsrisiken als ungenügend.

Darüber hinaus unterstehen dritte Zahlungsdienstleister neu verschärften Informations- und Rechenschaftspflichten, welche mehr Transparenz bezüglich der Vertragsbedingungen schaffen sollen. Sie müssen beispielsweise dem Zahlungsdienstnutzer die Authentisierungsmittel sowie alle Entgelte, die der Zahlungsdienstnutzer an den dritten Zahlungsdienstleister zu entrichten hat und gegebenenfalls deren Aufschlüsselung mitteilen. Löst der dritte Zahlungsdienstleister auf Verlangen des Zahlers einen Zahlungsauftrag aus, muss er dem Zahler und allenfalls auch dem Zahlungsempfänger unmittelbar nach der Auslösung unter anderem eine Bestätigung der erfolgreichen Auslösung des Zahlungsauftrags, dessen Betrag sowie die Höhe eines dafür zu entrichtenden Entgelts zugänglich machen.[43]

Im weiteren sollen die dritten Zahlungsdienstleister den Bestimmungen der Richtlinie über die Netz- und Informationssicherheit der Europäischen Union NIS-Richtlinie[44], welche auf Cyber Security gewährleisten soll, unterliegen, ins-

39 Art. 58 Abs. 2 lit. (b) und Art. 87 PSD 2.

40 Auslegung gemäss den Mindestanforderungen für Sicherheit im Internetzahlungsverkehr der EZB; Hass/Först (Fn. 6), 29.

41 Art. 58 Abs. 2 lit. (a) und (c) PSD 2.

42 Art. 6 lit. (b) PSD 2.

43 Art. 38 und 39 PSD 2.

44 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in

besondere den Bestimmungen für das Risikomanagement und die Meldung von Vorfällen.[45]

Schliesslich wird mittels der PSD 2 auch die Haftung der dritten Zahlungsdienstleister geregelt und massgeblich verschärft. Ein dritter Zahlungsdienstleister kann unter anderem für vom Kunden nicht autorisierte Zahlungen wie auch für technische Störungen haftbar gemacht werden. Falls hingegen der kontoführende Zahlungsdienstleister, also das Kreditinstitut, keine verstärkte Kundenauthentisierung verlangt, trifft die Primärhaftung dieses Institut, selbst wenn der dritte Zahlungsdienstleister die Zahlung ausgelöst hat oder sonst für einen Schaden haftbar gemacht werden könnte.[46]

b Einschränkung von Ausnahmen

Neben dem oben beschriebenen erweiterten Anwendungsbereich[47] sieht die PSD 2 zudem eine Eingrenzung gewisser Ausnahmetatbestände vor.

E-Commerce Plattformen

Zukünftig sollen auch E-Commerce-Plattformen, wie Handelsvertreter, die den Verkauf oder Kauf von Waren oder Dienstleistungen in Namen des Zahlers oder Zahlungsempfängers aushandeln bzw. abschliessen, unter die PSD 2 fallen und somit zulassungspflichtig werden.[48]

Geldautomaten

Ebenso soll die Ausnahme für die Betreiber von Geldautomaten wegfallen.[49]

Telekommunikationsdienstleister

Das Zahlen von Waren oder Dienstleistungen über die Mobilfunkrechnung soll in Zukunft einer Genehmigung bedürfen. Davon ausgenommen wären nur Nebendienstleistungen wie etwa Klingeltöne und dies nur bis zu einer monatlichen Betragsgrenze von Euro 50.– für Einzelzahlungen und Euro 200.– bei mehreren Zahlungsvorgängen. Nicht mehr unter die Ausnahme fällt die Abwicklung von Zahlungen für Musik, Apps oder digitale Spiele.[50]

---

der Union vom 7. Februar 2013.

45 Art. 85 PSD 2.

46 Art. 80 PSD 2; CMS Hasche Sigle (Fn. 35); Hass/Först (Fn. 6), 29.

47 Vgl. oben II.2.1a.

48 5. Weitere Angaben, Einzelerläuterungen zum Vorschlag Art. 3 lit. (b) und Art. 3 lit. (b) PSD 2; CMS Hasche Sigle (Fn. 35).

49 Art. 3 lit. (o) PSD wurde gestrichen und ist in der PSD 2 nicht mehr vorhanden.

50 Art. 3 lit. (l) PSD 2; CMS Hasche Sigle (Fn. 35); Hass/Först (Fn. 6), 29.

Betreiber von Kundenkarten-, Geschenkgutscheine- oder Rabattsysteme

Schliesslich sollen z.B. die von grossen Netzen mehrerer Kaufhäuser des gleichen Konzerns angebotenen Rabattkarten, sogenannte Kaufhaus-Rabattkarten, nicht mehr als Ausnahme anerkannt werden. Zumindest nicht, wenn mit den Karten durchschnittlich mehr als Euro 1 Mio. monatlich umgesetzt wird. Bis anhing waren solche Systeme unter die Ausnahme der «beschränkten Netzes an Dienstleistern oder Waren» gefallen.[51]

2.2 Empfehlungen der Europäischen Zentralbank

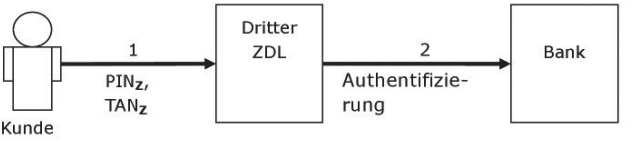
Die EZB hat im Mai 2014 Empfehlungen für die Sicherheit von Dienstleistungen, welche den Zugang zu Zahlungskonten von Kunden eines Kreditinstituts erfordern, publiziert.[52] Mit dem Ziel den Kontoinhaber zu schützen, empfiehlt die EZB unter anderem, dass die dritten Zahlungsdienstleister gleichwertige Sicherheiten und Kontrollmechanismen zum Schutz des Zahlungskonto des Kunden und den damit verbundenen Daten gewährleisten sollen wie kontoführende Zahlungsdienstleister, also Kreditinstitute. Überdies soll eine genügende Transparenz bezüglich der vom dritten Zahlungsdienstleister angebotenen Services hergestellt werden. Auch in Bezug auf die Legitimations- bzw. Authentisierungsmittel aus der Beziehung zwischen dem Kunden und dem Kreditinstitut, macht die EZB zwei Vorschläge:

(1) Entweder sollen das Kreditinstitut und der dritte Zahlungsdienstleister separate Authentisierungsmittel vereinbaren, welche den dritten Zahlungsdienstleister gegenüber dem Kreditinstitut eindeutig ausweisen. Der dritte Zahlungsdienstleiser authentifiziert sich also direkt gegenüber dem kontoführenden Zahlungsdienstleister mit seinen eigenen Credentials (d.h. ohne Impersonation) und erteilt den Zahlungsauftrag.

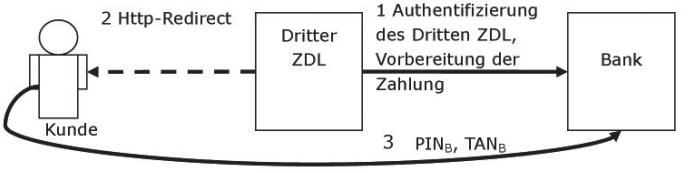
(2) Oder der dritte Zahlungsdienstleister authentifiziert sich ebenfalls gegenüber dem kontoführenden Zahlungsdienstleister, leitet dann aber den Kunden in sicherer Weise zur Webseite des kontoführenden Zahlungsdienstleister, wobei sich der Kunde gegenüber diesem authentisiert und den Zahlungsauftrag erteilt (sog. Redirect-Lösung).

51 Art. 3 lit. (k) PSD bzw. in der neuen Fassung Artikel 3 lit. (k) PSD 2; CMS Hasche Sigle (Fn. 35); Hass/Först (Fn. 6), 30.

52 European Central Bank, Final Recommendations for the Security of Payment Account Access Services following the Public Consultation, Mai 2014, https://www.ecb.europa.eu/pub/pdf/other/pubconsultationoutcome201405securitypaymentaccountaccessservicesen.pdf (zuletzt besucht am 17.12.2014).



EZB-Vorschlag 1: Der Kunde authentifiziert sich gegenüber dem Dritten ZDL und erteilt einen Zahlungsauftrag (1). Der Dritte ZDL authentifiziert sich gegenüber dem kontoführenden ZDL und erteilt den Zahlungsauftrag (2).



EZB-Vorschlag 2: Der Dritte ZDL authentifiziert sich gegenüber dem kontoführenden ZDL und sendet Informationen zur Vorbereitung einer Zahlung (1). Anschließend leitet der Dritte ZDL den Kunden in sicherer Weise zur Webseite des kontoführenden ZDL (2). Der Kunde authentifiziert sich gegenüber dem kontoführenden ZDL und erteilt den Zahlungsauftrag (3).

(Quelle: <http://www.bafin.de/SharedDocs/Bilder/DE/Grafik/bild_fa_bj_2014_06_zahlungsdienste_3.jpg;jsessionid=38FEB2E377A8765725F-B124A8A2B8B89.1_cid390?__blob=poster&v=1>, zuletzt besucht am 19.12.2014).

Schliesslich soll der Zugriff zum Zahlungskonto des Kunden durch den dritten Zahlungsdienstleister zeitlich minimiert und nur jene Kundendaten zur Verfügung gestellt werden, welche für die entsprechende Dienstleistung notwendig sind. Die Session soll nur solange offen bleiben, als die Abwicklung der Zahlungen dies erfordert. Zudem dürfen heikle Zahlungsdaten werden gespeichert noch für andere Zwecke als jene, welche ausdrücklich vom Kunden gewünscht wurden, verwendet werden.[53]

2.3 Regulierungsbedarf nach Schweizer Recht

Zurzeit besteht in der Schweiz keine Regulierung der dritten Zahlungsdienstleister. Sowohl durch die neuen technischen Herausforderungen als auch die Anpassung der PSD auf europäischer Ebene wird die Schweiz jedoch zur Einführung

53 European Central Bank (Fn. 53), 4 und 5.

einer Regulierung in geeigneter Form gehalten sein. Dies nicht zuletzt als Folge der fortgesetzten SEPA-Teilnahme.

Wie bereits oben erwähnt, gilt die PSD nicht für die Schweiz, und die Schweiz ist daher grundsätzlich nicht verpflichtet, ihr innerstaatliches Recht anzupassen.[54] Die SEPA Scheme Rulebooks sind jedoch im Hinblick auf die europäischen Rechtsvorschriften und insbesondere die Einführung der PSD entwickelt worden.[55] Die Schweizer Finanzinstitute können sich demzufolge nur vertraglich an die SEPA Scheme Rulebooks anbinden, wenn sie folgende Voraussetzungen erfüllen:

- Die SEPA Scheme Teilnehmer respektieren die wettbewerbsrechtliche Chancengleichheit *(level playing field)*.[56]
- Alle Teilnehmer müssen die SEPA Credit Transfer oder Direct Debit Scheme Rulebooks gleichermassen befolgen wie die anderen Teilnehmer.[57]
- Die Teilnehmer müssen den Nachweis erbringen, dass die Bestimmungen von Kapitel III und IV der PSD, welche für SEPA-Überweisungen resp. SEPA-Lastschriften relevant sind, in ihrem nationalen Recht vorhanden oder aufgrund einer im Wesentlichen gleichwertigen Praxis bindend sind (*are effectively represented in law or substantially equivalent binding practice)*.[58]

Zur Teilnahme an der SEPA nach Massgabe der Scheme Rulebooks mussten die Schweizer Finanzinstitute daher jeweils eine rechtsvergleichende Legal Opinion erstellen lassen, welche aufzeigte, dass sie die Anforderungen der SEPA-Verfahren erfüllen. Hinsichtlich der Vereinbarkeit mit dem EU-Recht wurden die entsprechenden Kapitel der PSD artikelweise rechtsvergleichend analysiert.[59] Basierend auf diesen Legal Opinions konnten die Schweizer Finanzinstitute ein Adherence Agreement des EPC unterschreiben bzw. an SEPA teilnehmen und haben sich damit verpflichtet, SEPA-konform zu arbeiten. Da sich die neuen Regelungen für die dritten Zahlungsdienstleister im Titel IV der PSD 2 befinden, werden Schweizer Finanzinstitute für eine fortgesetzte Teilnahme an den SEPA Scheme Rulebooks erneut aufzeigen müssen, dass im schweizerischen nationalen Recht gleichwertige Bestimmungen vorhanden sind oder eine im Wesentlichen

54 Vgl. oben II.1.2b.
55 Hess/Keiser (Fn. 28), 154 ff.
56 SEPA Credit Transfer Scheme Rulebook sowie SEPA Direct Debit Scheme Rulebook je Rule 5.1.
57 SEPA Credit Transfer Scheme Rulebook sowie SEPA Direct Debit Scheme Rulebook je Rule 5.1.
58 SEPA Credit Transfer Scheme Rulebook sowie SEPA Direct Debit Scheme Rulebook je Rule 5.1.
59 Hess/Keiser (Fn. 28), 160.

gleichwertige Praxis besteht. Nachfolgend sollen mögliche Regulierungsszenarien im Schweizer Recht aufgezeigt werden.

2.4 Bestehende Anforderungen und Regelungen nach Schweizer Recht

a Stufe Regulierung

Auf Stufe formeller Gesetze, Verordnungen und anderen Regulierungsinstrumenten lassen sich im Zusammenhang mit dem elektronischen Zahlungsverkehr vor allem Regelungen zur Sorgfaltspflicht der Banken finden. Die Banken unterstehen dem Auftragsrecht nach dem Schweizer Obligationenrecht und haften daher dem Auftraggeber, also dem Kunden, grundsätzlich für eine getreue und sorgfältige Ausführung der ihr übertragenen Geschäfte.[60] Durch das Datenschutzgesetz wird konkretisiert, dass Personendaten durch angemessene und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen.[61] Zudem müssen Banken gemäss dem Bankengesetz eine ihrer Geschäftstätigkeit entsprechende Verwaltungsorganisation vorsehen und Gewähr für eine einwandfreie Geschäftstätigkeit bieten.[62]

Zudem hat die Eidgenössische Finanzmarktaufsicht in ihrem Rundschreiben zu den operationellen Risiken der Banken bestimmt, dass die Geschäftsführung einer Bank Sicherheit, Integrität und Verfügbarkeit der Daten und Systeme zu gewährleisten sowie ein integriertes und umfassendes Risikomanagement für die Technologieinfrastruktur zu implementieren hat. Auch muss die Bank wissen, wo Kundenidentifikationsdaten gespeichert werden, von welchen Anwendungen und IT Systemen Kundenidentifikationsdaten verarbeitet werden und wo elektronisch auf sie zugegriffen werden kann.[63]

b Vertragliche Absicherungen

Mangels einschlägiger Regulierung der dritten Zahlungsdienstleister sind die Banken als Folge ihrer Sorgfaltspflicht gehalten, den Schutz der Kundendaten vertraglich zu sichern. Zu diesem Zweck sind die Institute dazu übergegangen, die Nutzung ihrer elektronischen Schnittstellen von der Einhaltung angemessener Vorkehrungen für die Datensicherheit und den Datenschutz abhängig zu machen.

60 Art. 398 Abs. 2 des Bundesgesetzes betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911.
61 Art. 7 Abs. 1 des Bundesgesetzes über den Datenschutz vom 19. Juni 1992.
62 Art. 3 Abs. 2 des Bundesgesetzes über die Banken und Sparkassen vom 8. November 1934.
63 FINMA (Fn. 25), Grundsatz 5 und Anhang 3 Grundsatz 3.

Diese Vorkehrungen stellen zum einen sicher, dass sich der dritte Zahlungsdienstleister eindeutig beim Institut authentisiert und autorisiert. Impersonation oder «Man in the Middle»- Lösungen können nicht toleriert werden. Ebenso ist vertraglich sicherzustellen, dass das Institut bei jedem Zugriff zweifelsfrei feststellen kann, von welchem ihrer Kunden die Instruktion ausgeht.

Sodann sind hinsichtlich Speicherung und Bearbeitung der Kundendaten verbindliche Abreden zu treffen. Aufgrund der territorialen Begrenzung des Bankkundengeheimnisses dürfen Daten durch die TPP ausschliesslich in der Schweiz gespeichert werden. Die Datencenter müssen den Anforderungen der Banken an die Datensicherheit genügen, und es sind Auditrechte zum Einhalten der Sicherheitsdispositive vorzusehen. Subunternehmer der TPP sind den Instituten zu melden und ebenfalls in die Sicherheitsdispositive einzubinden.

c Aktuelle Regulierungswelle

Am 27. Juni 2014 hat der Bundesrat die Vernehmlassung für ein neues Finanzdienstleistungsgesetz (FIDLEG) sowie ein neues Finanzinstitutsgesetz (FINIG) eröffnet, welche bis zum 17. Oktober 2014 dauerte. Das FIDLEG regelt die Voraussetzungen für das Erbringen von Finanzdienstleistungen und das Anbieten von Finanzinstrumenten in der Schweiz. Das FINIG unterstellt Finanzinstitute, welche die gewerbsmässige Vermögensverwaltung für Dritte betreiben, einer kohärenten Aufsichtsregelung, wobei sektorenübergreifend die Bewilligungsvoraussetzungen und weitere organisatorische Anforderungen für Finanzinstitute in der Schweiz neu geregelt werden sollen.[64] Gemäss den Erläuterungen zur Vernehmlassung der FIDLEG bezweckt diese den Schutz der Kundinnen und Kunden und die Schaffung vergleichbarer Bedingungen für das Erbringen von Finanzdienstleistungen durch die Finanzdienstleister.[65] Das neue Gesetz will sektorübergreifende Vorschriften für das Verhalten der Marktteilnehmer einführen, weshalb der Begriff der Finanzdienstleistung weit gefasst wird. Erfasst werden alle Tätigkeiten, die zum Erwerb eines Finanzinstruments durch eine Kundin oder einen Kunden führen können. Darunter fallen der Erwerb und die Veräusserung von Finanzinstrumenten auf Rechnung von Kundinnen und Kunden, unabhängig davon, ob die Finanzinstrumente von Dritten erworben werden oder vom Finanzdienstleister selbst geschaffen, platziert oder auf dem Sekundärmarkt veräussert werden (Ziff. 1). Ebenfalls als Finanzdienstleistungen gelten die reine Ver-

64 Vgl. Eidgenössisches Finanzdepartement (EFD), Erläuternder Bericht zur Vernehmlassungsvorlage, Übersicht, 25. Juni 2014.

65 Vgl. erläuternder Bericht des EFD (Fn. 64), 2 Erläuterungen zu den einzelnen Artikeln, 2.1 Finanzdienstleistungsgesetz, 1. Titel: Allgemeine Bestimmungen, Art. 1 Zweck und Gegenstand.

mittlung von Geschäften mit Finanzinstrumenten (Ziff. 2) sowie die Vermögensverwaltung und Anlageberatung. Als Finanzinstrumente gelten vor allem Beteiligungs- und Forderungspapiere.[66]

Die dritten Zahlungsdienstleister, welche Kontoinformationsdienste zur Erstellung von Budgetierungstools oder Kostenoptimierungsvorschläge anbieten, könnten je nach konkreter Tätigkeit unter die Kategorie der reinen Vermittlung von Geschäften oder der Anlageberatung fallen. Schliesslich sieht das neue FINIG auch eine Definition des Vermögensverwalters vor. Danach verwaltet dieser typischerweise gestützt auf individuelle Aufträge gewerbsmässig im Namen und für Rechnung der Kundinnen und Kunden Vermögenswerte. Im Gegensatz zum Anlageberater ist der Vermögensverwalter bevollmächtigt und auch faktisch in der Lage, selbständig über die Anlage des Kundenvermögens zu verfügen.[67] Diese Umschreibung kann auch auf dritte Zahlungsdienstleister in Form von ZAD zutreffen, soweit diese mit einer Verwaltungsvollmacht verbunden werden.

Trotzdem werden die dritten Zahlungsdienstleister von den aktuellen Gesetzesentwürfen nur peripher adressiert. Eine ausdrückliche Regulierung der TPP würde Rechtssicherheit schaffen und schwierige Abgrenzungsfragen vermeiden. Zudem wäre damit die fortgesetzte Teilnahme der Schweiz an der SEPA sichergestellt.

III. Ausblick und Handlungsbedarf

Eine Regulierung der dritten Zahlungsanbieter in der Schweiz scheint aufgrund mehrerer Gegebenheiten unausweichlich.

Zum einen wird mit der Verabschiedung der PSD 2 Anfang 2015 gerechnet. Deren Umsetzung im nationalen Recht muss innerhalb von zwei Jahren erfolgen. Die Schweizer Finanzinstitute müssen demnach für eine zukünftige Teilnahme an den SEPA Scheme Rulebooks innerhalb von zwei Jahren aufzeigen, dass im Schweizer Recht Bestimmungen vorhanden sind, welche jenen von Kapitel III und IV der PSD II entsprechen, oder aufgrund einer im Wesentlichen gleichwertigen Praxis in der Schweiz bindend sind. Um nicht unter Zeitdruck zu geraten,

66 Vgl. erläuternder Bericht des EFD (Fn. 64), 2 Erläuterungen zu den einzelnen Artikeln, 2.1 Finanzdienstleistungsgesetz, 1. Titel: Allgemeine Bestimmungen, Art. 3 Begriffe, Bst. b und d.

67 Vgl. erläuternder Bericht des EFD (Fn. 64), Art. 17 Abs. 1.

sollten sich die Schweizer Finanzinstitute schon jetzt mit den anstehenden Veränderungen auseinandersetzen.[68]

Zum anderen sollten die innerstaatlichen Regelungen aus eigenem Antrieb und unabhängig von den Entwicklungen auf europäischer Ebene die neuen technischen Möglichkeiten des elektronischen Zahlungsverkehrs sowie die Sicherheitsbedenken durch den Markteintritt der dritten Zahlungsdienstleister adressieren. Eine zukünftige Regulierung sollte zumindest folgende Minimalstandards beinhalten: Erstens dürfen die Legitimations- bzw. Authentisierungsmittel des Kunden mit seiner Bank einem dritten Zahlungsanbieter weder zugänglich gemacht noch von diesem genutzt werden. Entsprechend bedarf dieser separater Authentisierungsmittel, welche ihn der Bank gegenüber eindeutig ausweisen. Zweitens sollte auch die Autorisierung klar geregelt werden. Der Kunde soll den dritten Zahlungsdienstleister der Bank gegenüber explizit für den Zugriff auf seine Bankkundendaten und die individuellen Befugnisse (allenfalls mit Limiten) autorisieren müssen. Schliesslich sollen Verantwortlichkeiten und Haftungsfolgen der Bank, des dritten Zahlungsdienstleisters sowie des Kunden verbindlich geregelt werden.[69] Zu diesem Zweck ist eine angemessene Kapitalisierung des dritten Zahlungsdienstleisters sowie ein Gewährserfordernis für die leitenden Organe vorzusehen.

68 Hass/Först (Fn. 6), 30.
69 Lubich (Fn. 15), 11.