Interessengemeinschaft Kreditkartengeschäft
c/o PaySys Consultancy GmbH
Im Uhrig 7
D-60433 Frankfurt a.M.

escher@gsk.de
hgodschalk@paysys.de
T: +49-89-288 174 31

Bundesanstalt für Finanzdienstleistungsaufsicht
Referat BA 57
Herrn Dr. Lutz
Graurheindorfer Str. 108
53117 Bonn

Per E-Mail : Konsultation-02-15@bafin.de

**19. März 2015**

**GZ: BA 57-K 3142-2013/0017**
**Konsultation 02/2015-Rundschreiben zu den Mindestanforderungen an die Sicherheit von Internetzahlungen**

Sehr geehrter Herr Dr. Lutz,

wir wenden uns im Auftrag der deutschen *Interessengemeinschaft Kreditkartengeschäft"* (nachfolgend „**IK**") an Sie und begrüßen nachdrücklich die Einladung zur öffentlichen Konsultation, an der wir uns gerne beteiligen.

Die IK ist eine rechtlich nicht verselbständigte, wettbewerbsneutrale Plattform für Unternehmen, die im Kredit- und Debitkartengeschäft in Deutschland Kartenissuer, -acquirer, -Netzbetreiber oder Prozessoren sowie Lizenzgeber informiert und Stellungnahmen zu Gesetzgebungs- und Regulierungsvorhaben mit Auswirkungen auf das Kartengeschäft abgibt.

Die folgenden Teilnehmer an der IK haben bei Erarbeitung dieser Stellungnahme mitgewirkt:

- Atos Worldline GmbH
- B+S Card Service GmbH
- Chase Paymentech
- Commerzbank AG
- ConCardis GmbH
- Deutsche Telekom AG
- DVB Logpay GmbH
- easycash GmbH
- Elavon Financial Services Limited, Germany
- EVO Payments International GmbH

- First Data Deutschland GmbH
- InterCard AG
- Lufthansa AirPlus Servicekarten GmbH
- Postbank P.O.S.
- TeleCash GmbH & Co. KG
- transact Elektronische Zahlungssysteme GmbH
- Verband der Sparda-Banken e.V.

Mit den folgenden Anmerkungen nehmen wir Stellung zur Konsultation 02/2015 zum Entwurf eines Rundschreibens zu Mindestanforderungen an die Sicherheit von Internetzahlungen (im Folgenden „**die Konsultation**“ bzw. bei Zitat von Textziffern ohne weitere Quellenangaben), die der Umsetzung der Empfehlungen des European Forum on the Security of Retail Payments vom 01.02.2013 (im Folgenden „**SecuRe Pay Empfehlungen**“) sowie den am 19.12.2014 veröffentlichten Guidelines on the Security of Internet Payments der EBA (im Folgenden „**EBA-Guidelines**“) dient.

Die Teilnehmer der IK sind selbstverständlich auch daran interessiert mitzuwirken, Zahlungen im Internet in angemessenem Rahmen sicherer zu machen und ihre interne IT-Sicherheitsorganisation fortlaufend an Marktentwicklungen und erkennbare Gefährdungssituationen anzupassen. Dies unternehmen Kartendienstleister bereits heute auf der Grundlage produkt- und geschäftsangemessener Risiko- und Sicherheitsbetrachtung.

Für aufsichtsrechtliche Vorgaben ist allerdings bedeutsam, dass für Marktteilnehmer mit funktional gleicher Leistungserbringung gleiche Regeln, gleiche Aufsicht und auch gleiche Sanktionen gelten („level-playing field“) und Wettbewerbsverzerrungen zwischen Anbietern in unterschiedlichen EU-Staaten, damit aber auch „Aufsichtsarbitrage“, verhindert wird. Schließlich betrachtet die IK das Bestreben mit Sorge, zahlreiche belastende Produkt-, Verhaltens- und Organisationspflichten ohne Gesetzgebungsverfahren im Wege einer einfachen Verwaltungsrichtlinie zu statuieren.

## I. Vorbehalt des Gesetzes

Abweichend zu anderen deutschen finanzaufsichtlichen Rundschreiben mit Mindestanforderungen an die Geschäftsorganisation von Instituten in Deutschland, wie die MaRisk (Rundschreiben 10/2012) bzw. die MaComp (Rundschreiben 4/2010) lassen die Mindestanforderungen an die Sicherheit von Internetzahlungen nach der Konsultation die zugrundeliegende Rechtsgrundlage im Unklaren. Dies erscheint insofern problematisch, da die BaFin unbestimmte gesetzliche Rechtsbegriffe durch Verwaltungspraxis präzisieren kann, selbst aber nicht über das Gesetz hinausgehend ori-

ginäre Handlungs- oder auch Gestaltungspflichten im Hinblick auf Finanzprodukte ohne gesetzliche Grundlage begründen darf.

So lassen sich sicherlich zahlreiche Anforderungen an das Sicherheitsmanagement als Präzisierung allgemeiner bankaufsichtlicher Organisationspflichten nach § 25a KWG bzw. für Zahlungsinstitute nach § 22 Abs. 1 ZAG einordnen.

Über diese finanzaufsichtlichen Generalklauseln hinaus wird es jedoch nicht zulässig sein, ohne gesetzliche Grundlage in bestehende oder praktizierte Finanzprodukte des Zahlungsverkehrs, insbesondere durch Anforderungen an starke Kundenauthentisierung, einzugreifen bzw. Gestaltungspflichten zu statuieren.

Ohne gesetzliche Grundlage ist die BaFin jedoch nicht befugt, abstrakte oder konkrete Verpflichtungen zu begründen oder die Rechte des Adressaten zu entziehen oder zu beschränken. Eingriffe in die Grundrechte der Normadressaten bedürfen hierbei einer Ermächtigung mittels eines allgemeinen Gesetzes (BVerfGE 8, 325). Entscheidend hierbei ist, dass Verlautbarungen und Rundschreiben der BaFin lediglich der Konkretisierung eines bestehenden Aufsichtsmaßstabs dienen und daher ihre Grundlage in diesem finden. Die Maßnahmen der BaFin interpretieren daher, können jedoch nicht modifizieren (*Thiele*, Finanzaufsicht: Der Staat und die Finanzmärkte, S. 207). Sie dienen damit nur dazu, die Auslegung von Normen durch die Behördenbediensteten zu standardisieren, und stellen somit nur Innenrecht der Verwaltung dar (*Schwintowski/Köhler*, Bankrecht, 4. Auflage, 2014, § 4 Rn. 91; *Höhns*, Die Aufsicht über Finanzdienstleister, 2002, S. 158). Die Begründung von allgemeinen Handlungspflichten oder Pflichten zu einer bestimmten Art der Ausgestaltung der Finanzprodukte des Normadressaten auf Grundlage einer Verwaltungsvorschrift in Form eines Rundschreibens ist daher nicht zulässig.

Auch die SecuRe Pay-Empfehlungen der EZB bzw. auch die EBA-Guidelines bieten nach deutschem Verfassungs- und Verwaltungsverständnis keine entsprechende Rechtsgrundlage um dem Vorbehalt des Gesetzes nach Art. 20 Abs. 3 GG zu genügen. Im Rahmen bereits bestehender gesetzlicher Organisationsanforderungen oder Generalklauseln können hierdurch zwar europaweit Harmonisierungen angestrebt werden, nicht jedoch neue, bislang nicht **gesetzlich** definierte Verhaltens- oder Produktgestaltungspflichten konstituiert werden.

Diese Hinweise sind auch nicht etwa rein universitärer-theoretischer Natur, sondern ausgesprochen praktisch mit erheblich belastender wirtschaftlicher Relevanz für die regulierten Institute und deren technische Dienstleister. So ist zum einen anzuerkennen, dass in den Entwurfsarbeiten auf europäischer Ebene zur zweiten Zahlungsdiensterichtlinie gerade an einem neuen

gesetzlichen Programm mit organisatorischen IT-Sicherheitsanforderungen und auch Anforderungen zu einer starken Kundenauthentisierung gearbeitet wird, die letztlich vermutlich im Jahre 2017 in eine Transformation mit Deutscher Gesetzgebung münden werden. Auf dieses Gesetzgebungsverfahren und auch die zeitlich zu erwartenden Umsetzungs- und Anwendungspflichten ist die Zahlungsverkehrsbranche vorbereitet. Ein zeitliches „Vorziehen“ entsprechender Verhaltens- und Gestaltungspflichten im Verwaltungswege – so letztlich die Empfehlung in den EBA-Guidelines – mag zwar aus europäischer Sicht pragmatisch wirken, ändert aber nichts an bestehenden verfassungsrechtlichen Schranken nach deutschem Recht.

Für eine ordnungsgemäße Umsetzung neu statuierter Pflichten würde auch den betroffenen Instituten – im Vergleich zur PSD-2 Umsetzung - nicht ausreichend Zeit verbleiben, insbesondere im Hinblick auf Erfordernisse von Vertragsänderungen mit Kunden, Austausch existierender Legitimationsmedien und Kreditkarten, vor allem aber Umstellung komplexer Datenverarbeitungsprozesse bei technischen Dienstleistern – aber auch von Online-Händlern – bei Umsetzung einer „starken Kundenauthentisierung“.

Gegebenenfalls war auch dies ein Motiv für die britische Finanzaufsicht FCA, dass diese sich entschlossen hat, die SecuRe Pay-Empfehlungen noch nicht im Rahmen ihrer Verwaltungspraxis umzusetzen, sondern auf die Implementierung der PSD-2 zu warten. Die FCA wird daher erst mit Inkrafttreten der britischen Richtlinienumsetzung die dann mit der PSD-2 statuierten Pflichten umsetzen und in ihrem Aufsichtsprogramm anwenden (vgl. http://www.fca.org.uk/firms/firm-types/payment-services-institutions).

Einer rein aufsichtspraktischen Begründung von Verhaltens- und Gestaltungspflichten, wie Ausgestaltung von Zahlungsprodukten und Begründung von Meldepflichten, ohne entsprechende gesetzliche Grundlagen ist daher entgegenzutreten.

## II. Erstreckung auf nicht-regulierte Marktteilnehmer

Es werden auch zahlreiche Pflichten für Kartenzahlungsdienstleister formuliert, die diese selbst nicht umsetzen können. Es wird vielmehr eine „Erstreckung auf nicht-regulierte Marktteilnehmer“ erwartet, indem Zahlungsdienstleister mit Hilfe zivilrechtlicher Verträge aufsichtspolitische Regelungsziele auf Online-Händler überwälzen sollen. Diese Verpflichtungen alleine mit verwaltungspraktischen Methoden der Finanzaufsicht durchzusetzen, halten wir ohne gesetzliche Grundlage für unzulässig.

Insbesondere gegenüber Online-Händlern liegen regelmäßig keine einseitig änderbaren AGB zu Grunde. Wegen des wechselseitigen Investitionsbedarfs und Implementierungsaufwands für IT-Abrechnungssystemen von Online-Händlern werden typischerweise längere Vertragslaufzeiten verein-

bart, ohne Möglichkeit eines Kreditkartenacquirers kurzfristig, innerhalb von wenigen Monaten einseitig wesentliche Aspekte der Leistungserbringung zu verändern.

Soweit in Verträgen mit Händlern Anpassungsklauseln enthalten sind, knüpfen diese typischerweise an Veränderungen des Aufsichtsrechts im Sinne **gesetzlicher Regelungen** an, nicht jedoch im Hinblick auf angestrebte Neuverpflichtungen im Wege einer Verwaltungsrichtlinie. Zivilrechtlich wäre es daher auf Händlerseite gar nicht möglich, eine aufsichtliche Erstreckung durch Neubegründung vertraglicher Pflichten von Online-Händlern durch einseitige Vertragsanpassungen kurzfristig zu erreichen.

Die Pflichten für Acquirer gegenüber Online-Händlern sollten daher beschränkt sein auf die Kommunikation der Inhalte der EBA-guidelines und EZB-recommendations und ggf. auf das Einholen von Erklärungen der Online-Händler, in welchem Umfang sie Bezahlverfahren mit starker Authentifizierung einsetzen, um aus diesem Datenmaterial etwaigen weiteren gesetzgeberischen Handlungsbedarf zu identifizieren.

## III. Europäisches Level-Playing-Field

Eine etwaige Statuierung von Verhaltenspflichten, einschließlich Pflichten zur Gestaltung von Zahlungsprodukten im Wege einer verpflichtenden starken Kundenauthentisierung vor nationalem Inkrafttreten der PSD-2 Umsetzung würde auch – gerade abweichend von den europäischen Zielsetzungen – zu einer Verzerrung eines europäischen „Level-Playing-Field“ führen, da beispielsweise britische Institute, einschließlich britischer Niederlassungen in Deutschland diesen Pflichten zur Gestaltung von Zahlungsprodukten nicht unterliegen würden. Deutsche Institute unter BaFin-Aufsicht wären hingegen im gleichen Markt verpflichtet, ihre Prozesse und Zahlungsprodukte entsprechend der Vorgaben der Konsultation anzupassen. Dies würde nicht nur zu erheblichen Wettbewerbsverzerrungen in Deutschland unter Zahlungsdienstleistern führen, sondern gerade auch in dem sehr erfreulich wachsenden Markt des elektronischen Handels im Internet, da sich dann vermutlich zahlreiche im Internet agierende Händler aus Kostengründen von deutschen Zahlungsdienstleistern abwenden und britischen Zahlungsdienstleistern zuwenden würden. Auch Sitzverlagerungen deutscher Online-Händler zur Vermeidung des auch nur mittelbaren Anwendungsbereichs der Mindestanforderungen wären mit dem Risiko von Arbeitsplatzverlusten in Deutschland nicht auszuschließen.

Die IK plädiert daher dafür, statt des Erlasses einer belastenden Verwaltungsrichtlinie erst in Umsetzung der PSD-2, wie auch von der britischen Finanzaufsicht FCA vorgesehen, den ordentlichen Gesetzgebungsweg zu beschreiten, um hierbei auch Marktverzerrungen zu vermeiden, bzw. neue Marktbelastungen in einem parlamentarischen Verfahren zu entscheiden.

## IV. Proportionalitätsgrundsatz

Abweichend von der bisherigen verwaltungspraktischen Setzung von Mindeststandards an eine ordnungsgemäße Geschäftsorganisation fehlt es in den zur Konsultation stehenden Mindestanforderungen an die Sicherheit von Internetzahlungen auch an einem grundsätzlich vorangestellten „Proportionalitätsgrundsatz“, wie er zur Wahrung des Verhältnismäßigkeitsgrundsatzes zu Recht von AT 3.2 der MaComp sowie den MaRisk zugrundeliegt, um der heterogenen Institutsstruktur und der Vielfalt der Geschäftsaktivitäten Rechnung zu tragen. Insofern regt die IK die Aufnahme eines diesbezüglichen Proportionalitätsgrundsatzes entsprechend den MaComp oder den MaRisk dringend an.

## V. Unterschiede Überweisungs-/Kartenzahlungsverkehr und unverhältnismäßige Belastung von Kartenanbietern

Es dürfen auch nicht evidente Schwächen der EZB-Empfehlungen und der EBA-Guidelines ungeprüft übernommen werden, um eine fehlende Differenzierung zwischen Überweisungsverkehr und Kartenverkehr zu vermeiden. Mit der unterschiedslosen Übertragung von Überweisungsregulierung auf Kreditkartenanbieter ginge eine unangemessene Belastung von Kartenzahlungsprodukten einher, welche nicht durch Verwaltungsrichtlinie der BaFin, sondern (erneut) nur mittels gesetzlicher Regelung zulässig wäre. Im Rahmen einer verhältnismäßigen Regulierung müssen die unterschiedlichen Rahmenbedingungen von Überweisungen und Kreditkartenzahlungen im Internet berücksichtigt werden:

a) Eine Bank, die Internet-Banking anbietet, entscheidet im **Überweisungsverkehr selbst** über ihre eigenen Sicherheitsstandards, einschließlich der Authentifizierungsmechanismen bei Überweisungen. Dort können die aufsichtlichen Anforderungen autonom umgesetzt werden.

b) **Anders** im **Kreditkartenverkehr, der sich** durch eine strenge Prozess- und Systemdefinition der jeweiligen Kreditkartensysteme/Lizenzgeber auszeichnet. Während sich die IT-Sicherheitsbetrachtung im Rahmen des Überweisungsverkehrs auf das Rechtsverhältnis zwischen der Bank und dem Kunden beschränkt, sind an einer Kreditkartentransaktion fünf Parteien in sechs Rechtsverhältnissen beteiligt. **Anders** als eine Bank im Überweisungsverkehr ist ein Zahlungsdienstleister gar nicht in der Lage, eigenständig gegenüber dem System abweichende organisatorische Voraussetzungen zu schaffen.

## VI. Anmerkung zu den Mindestanforderungen im Einzelnen

### 1. Zu 1. Anwendungsbereich

Das Rundschreiben soll für „Zahlungsgeschäfte im Sinne des § 1 Abs. 2 Nr. 2 ZAG im Massenzahlungsverkehr über das Internet“ eine Legaldefinition für Internetzahlungsdienste bereitstellen. Hier geht die BaFin aber bereits im Anwendungsbereich über die SecuRe Pay-Empfehlungen hinaus, da die gesamte Arbeit der SecuRe Pay-Beteiligten und der EZB – wie auch die BaFin in der Einladung zum Konsultationsverfahren betont – auf Verbraucherzahlungen ausgerichtet war, was die EZB in ihrer Verlautbarung der SecuRe Pay-Empfehlungen vom 31.01.2013 als Zielsetzung mehrfach betont. Gleiches gilt für die EBA-Guidelines und die zugrundeliegende Zusammenfassung der EBA-Konsultation vom 20.10.2014, in deren Annex 3 (S. 32) die EBA zur Problemdefinition betont:

- “***Consumers*** *are affected because inadequate security diminishes the overall confidence in the online retail and banking sector.”*

und

- “*Payment systems, in turn, are impacted because the perception of failing payment security affects the way in which* ***consumers*** *make payment choices. As* ***consumer*** *confidence and specific payment instruments is undermined, they may switch to alternative but less efficient forms of payment (...).*”

sowie auf S. 33 / Objective:

> *“The draft guidelines constitute harmonized, minimum security recommendations in the fight against payment fraud and aim to increase consumer trust in internet payments services.”*

Da die Vertrags-, Kommunikations-, Informations- und Produktgestaltungsumgebung bei Unternehmenskunden der regulierten Institute, so insbesondere im Kreditkartenbereich bei Firmenkreditkarten oder sonstigen speziell an Firmen herausgegebenen Zahlungsprodukte, z.B. zur Begleichung von Reisekosten oder sonstigen Betriebsausgaben, einen grundlegend anderen Hintergrund als Verbraucher-Kreditkartenzahlungen oder sonstige Zahlungen im Internet haben, sollte der Einsatz des Internets für Zahlungen im Unternehmensbereich explizit von den Mindestanforderungen ausgenommen sein, um zumindest auch in dieser Hinsicht nicht ein europäisches Level-Playing-Field im Vergleich zu anderen europäischen Umsetzungen zu verzerren.

## 2. Zu 2.2 Risikoanalyse

a) Besonders die Anforderungen an die Risikoanalyse und das Risikomanagement sollten einen Proportionalitätsgrundsatz im Hinblick auf konkret angebotene Geschäfte im Verbraucherzahlungsbereich sowie Komplexität der Unternehmensstruktur des Instituts berücksichtigen. So sind Kreditinstitute gesetzlich umfassenden Pflichten zur Vorhaltung von Risikomanagementsystemen nach § 25a Abs. 1 KWG iVm Rundschreiben 10/2012 (MaRisk) unterworfen. Zahlungsinstitute hingegen unterliegen nach § 22 Abs. 1 ZAG nur einer allgemein gehaltenen Pflicht zur ordnungsgemäßen Geschäftsorganisation und insbesondere nicht den für KWG-Institute geltenden MaRisk. Diese, sich aus dem KWG und ZAG ableitende aufsichtliche Differenzierung zwischen Kredit- und Zahlungsinstituten muss sich auch unter Anwendung des Proportionalitätsgrundsatzes bei Risikomanagementanforderungen im Rundschreiben wiederfinden.

b) Darüber hinaus sollte bei Tz.7 bezüglich der kundenseitigen Risikoanalyse klargestellt werden, dass kein Institut Kenntnisse von der jeweils vom Kunden eingesetzten Hardware, allgemeinen Softwareumgebung oder individuell gewählten Zugangsform im Internet hat. Kenntnisse bestehen auf Seiten der Institute nur dahingehend, welche technischen Grundvoraussetzungen ein Kunde allgemein erfüllen muss, um mit dem Institut für Zahlungstransaktionen zu kommunizieren und welche Identifikations- und Authentifizierungsmechanismen der Kunde einsetzen muss. Die Kenntnis dieser Umstände „auf Kundenseite“ ist verständlicherweise Teil der Risikoanalyse. Andere Fragen der „technischen Umgebung der Kunden“ können jedoch in der Risikoanalyse ohne Kenntnis der Institute nicht berücksichtigt werden.

Im Kreditkartenbereich werden bislang von den Kartensystemen keine technischen Anforderungen an Kreditkartennutzer im Internet gestellt– und damit in der Folge auch nicht von den Kreditkarten-Issuern. Anders als im Überweisungsverkehr definiert ausschließlich der Online-Händler die zu ihm führenden technischen Kommunikationskanäle sowie die vom Kunden bei ihm einzusetzenden Sicherheitsmerkmale. Diese Anforderungen liegen jedoch außerhalb von Kenntnis und Beherrschbarkeit eines Kreditkartenissuers oder -acquirers.

Dieser Abschnitt im Rundschreiben kann daher nur auf diejenigen „abstrakt-generellen Anforderungen“ abstellen, die vom Zahlungsdienstleister selbst, nicht aber von anderen Beteiligten gefordert werden.

c) Des Weiteren erscheint bei Tz.7 die Begründung der BaFin mit Formulierung einer erwarteten Schutzbedarfsanalyse nach Vorgaben des BSI problematisch, welches im Rahmen der Risikoidentifikation und –analyse zwar eine denkbare, nicht aber eine zwingende Methode einer Risikoanalyse ist. Auch hier ist zur Anwendung von angemessenen und unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit geeigneten Analysemethoden offener zu formulieren, dass auch andere marktgängige Standards unter Berücksichtigung des Proportionalitätsgrundsatzes zur Anwendung kommen können, dass es aber nicht zwingend einer BSI-Schutzbedarfsanalyse bedarf. Hier ist schließlich zu beachten, dass selbst Kreditinstitute unter den MaRisk auch nur nach Maßgabe des Proportionalitätsgrundsatzes zu einer Anwendung von BSI-Schutzbedarfsanalysen verpflichtet sind.

Übersehen wird hierbei, dass im Kartenzahlungsverkehr der vom Payment Card Industry Council definierte Sicherheitsstandard („Payment Card Industry Data Security Standard“ oder kurz „PCI DSS“) existiert, der in den weltweit tätigen Kreditkartensystemen VISA, MasterCard, American Express und JCB International weltweit zur Anwendung kommt. Dieser Sicherheitsstandard ist für alle Issuer und Acquirer als Teilnehmer dieser Kartensysteme verpflichtend. Da das Kartenzahlungsgeschäft im Internet auch nicht an den europäischen, geschweige denn den deutschen Grenzen halt macht, sollten bereits existierende und international harmonisierte Sicherheitsstandards wie PCI DSS gerade vorzugsweise als Standards anerkannt werden.

Zum anderen wäre es unverhältnismäßig auch andere marktgängige Risikoidentifikationsstandards, z.B. nach ISO 27000, generell für unzulässig zu erklären.

Richtigerweise sollten abstrakt-generelle Anforderungen aufgestellt werden, zu deren Umsetzung dann die regulierten Institute unter Anwendung des Proportionalitätsgrundsatzes nach ihrer Institutsgröße, aber auch nach den praktizierten Geschäftstätigkeiten selbst entscheiden können, welcher Risikoidentifikations- und Analysestandard verwendet wird. Eine Verengung auf einen einzigen Standard, der zurzeit nicht einmal für Kreditinstitute unter Anwendung der MaRisk verbindliche Geltung hat, wäre eine unverhältnismäßige, an Differenzierung mangelnde Regelung.

## 3. Zu 2.3 Überwachung und Berichtswesen zu IT-Sicherheitsvorfällen

a) Die in Tz. 14 niedergelegte Anforderung „*zur zentralen Registrierung, Beobachtung und Weiterverfolgung von (…..) sicherheitsbezogenen*

*Kundenbeschwerden*“ ist erneut ohne gesetzliche Grundlage problematisch. Dem liegt nicht nur ein rechtliches, sondern auch ein organisatorisches Argument zugrunde, da in wenigen Monaten eine entsprechende Kundendatenbank ohne gebotene Vorbereitungszeit – wie in einem ordentlichen Gesetzgebungsverfahren – für Institute nicht zumutbar umsetzbar ist.

b) Die Definition eines **kritischen IT-Sicherheitsvorfalls** in Tz. 15 geht zu weit. Nicht alleine die „Beeinträchtigung“ der Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität von Systemen oder Anwendungen darf zu einer Meldepflicht führen, sondern allenfalls dann, wenn sich hierdurch ein Risiko realisiert, welches nicht durch entgegenlaufende Schutzmaßnahmen und entgegen der vorher aufgestellten Risikoplanung beherrschbar ist. Im Übrigen gilt auch hier, dass eine solche Meldepflicht nicht alleine durch eine Verwaltungsrichtlinie begründet werden kann, sondern allenfalls durch eine gesetzliche Regelung, sinnvollerweise mit Umsetzung der PSD-2, die ohnehin vergleichbare Meldepflichten enthalten wird.

Dies wird auch aus einem Vergleich mit der kommenden Meldepflicht nach § 8b Abs. 4 BSI-Gesetz-E (BT-Drs. 18/4096) deutlich, in dem eine Meldepflicht sogar für Betreiber Kritischer Infrastrukturen nur unter bestimmten qualifizierten Voraussetzungen begründet wird und auch nur dann, wenn das Funktionieren dieser Kritischen Infrastrukturen von „hoher Bedeutung für das Gemeinwesen“ ist (§ 2 Abs. 10 BSI-Gesetz-E), was bei IT-Systemen einzelner Zahlungsinstitute sicher wohl kaum der Fall sein wird.

Gleichwohl ist noch nicht absehbar, ob und in welchem Umfang der Verordnungsgeber nach § 10 BSI-Gesetz-E auch Anlagen einzelner Zahlungsdienstleister in diesem Sinne für gemeinwesenrelevant hält, so dass auch dies dafür spricht, etwaige Meldepflichten zu kritischen Störfällen bei Internetzahlungen frühestens in einem Gesetzgebungsverfahren zu begründen, um hierbei auch die Gefahr von doppelten Meldeverfahren mit unverhältnismäßigen Belastungen zu vermeiden.

c) Auch die in der Begründung genannten Beispiele für kritische IT-Sicherheitsvorfälle gehen weit über Praxiserfahrungen und risikoorientierte Regelungsansätze hinaus. Zum einen darf nicht ein Teilausfall „*jeglichen Zahlungsverkehrs einschließlich Kartenzahlung*“ bei Ausfall von mehr als einer Stunde als entsprechend kritisch gewürdigt werden, da es einen grundlegenden Unterschied macht, ob der Überweisungs-/Zahlungsverkehr mit zeitkritischen Komponenten für Kunden und Institute ausfällt, oder ob im Einzelhandel zu Bezahlzwecken ein Zahlungsinstrument gegebenenfalls kurzfristig nicht ein-

setzbar, aber jederzeit durch andere Zahlungsalternativen ersetzbar ist.

Schließlich ist auch eine Meldeanforderung bei Vorfällen, „.. *die zu signifikanten Reputationsschäden führen können*“ problematisch. Natürlich ist die Verhinderung von Reputationsschäden grundlegende Anforderung an eine ordnungsgemäße Geschäftsorganisation eines jeden Instituts. Es ist aber auch anzuerkennen, dass selbst in Risikomanagementanforderungen an Kreditinstitute nach den MaRisk bei Risiken für Reputationsschäden keine Meldepflicht an die Bankaufsicht besteht.

d) Die Anknüpfungspunkte im Rundschreiben an kritische IT-Sicherheitsfälle gehen auch weit über die EZB-Empfehlungen hinaus, die sich in recommendation 3 sowie dem Glossar auf zahlungsbezogene Sicherheitsvorfälle („major payment security event“) beziehen und hiermit – anders als die BaFin – Vorfälle definieren, die sich auf die zahlungsbezogenen Systeme und die hierbei verarbeiteten Zahlungsdaten von Zahlungsdienstleistern beziehen. Der im Rundschreiben verwendete Begriff der kritischen IT-Sicherheitsvorfälle kann sich daher allenfalls auf die in den SecuRe Pay Recommendations beschriebenen Fälle beschränken.

e) Wie bereits ausgeführt, können mit Verwaltungsrichtlinie auch nicht Anforderungen aufgestellt werden (Tz. 17) auf Online-Händler einzuwirken, bzw. diesen vertragliche Pflichten zur Einhaltung eines Rundschreibens aufzuerlegen. Auch diese Auferlegung von Pflichten gegenüber Instituten ist ohne gesetzliche Grundlage nicht möglich und lässt es konsequenterweise auch zivilrechtlich nicht zu, von Händlern eine entsprechende Vertragsanpassung zu verlangen. Im Ergebnis ist daher auch die Aufstellung dieser Handlungspflichten dem Gesetzgebungsverfahren zur Umsetzung der PSD-2 vorzubehalten.

**4. Zu 2.4 Risikokontrolle und –vermeidung**

a) Die Anforderungen in Tz. 23 „die Websicherheit ist zu gewährleisten“ ist so nicht umsetzbar. Genauso wenig wie die Fälschungssicherheit des Banknotenverkehrs „gewährleistet“ werden kann, ist dies den Instituten bezüglich der Websicherheit möglich. Im Rahmen von Kundeninformationen können selbstverständlich Pflichten zur Information von Kunden über gefälschte oder sonst manipulierte Webseiten – bei bestehender Kenntnis hiervon - bestehen. Die Fälschung oder Imitierung von Webseiten kann aber nicht bzw. im Hinblick auf erforderlichen Rechtsschutz nicht kurzfristig verhindert oder vermieden werden. Hier würde den Instituten eine nicht umsetzbare Pflicht auferlegt werden.

Auch hier fehlt es an einer Differenzierung zwischen Überweisungs- und Kartenverkehr. Im Überweisungsverkehr im Internet kann es in der Tat geboten sein, dass die Online-Bank auf die Vermeidung von Manipulationen **ihrer eigenen** Webseite zu achten hat, da genau über diese bilaterale Browser-Verbindung zwischen Bankkunde und Bank entsprechende „Phishing-Risiken" wenngleich nicht vermieden, so zumindest reduziert werden können.

Anders ist es im Kartenzahlungsverkehr, bei dem weder der Karteninhaber dem Issuer, noch der Online-Händler dem Acquirer „web-browserbasiert" unmittelbar einen Zahlungsauftrag über deren website erteilt. Die Erteilung des Zahlungsauftrags erfolgt vielmehr mehrgliedrig über die übrigen beteiligten Händler/Acquirer/Kartensystem und erst dann zum Issuer. Die Manipulationsfreiheit von Webseiten anderer Marktteilnehmer kann daher nicht von einem Kreditkartenissuer oder –acquirer verlangt werden. In verhältnismäßiger Weise kann daher nur auf Webseiten, die vom Zahlungsdienstleister selbst betrieben werden, abgestellt werden, worauf auch der dritte Satz der Begründung zu Tz. 23 hindeutet.

b) Zu den Anforderungen aus Tz. 30 zur Übernahme von Sicherheitsfunktionen durch Externe ist erneut unter Berücksichtigung des Anwendungsbereichs der Mindestanforderung sowie eines gebotenen Proportionalitätsgrundsatzes eine Klarstellung vorzunehmen, dass das Institut „durch geeignete vertragliche Regelung" sicherzustellen hat, dass der Externe die Anforderungen dieses Rundschreibens einhält, **soweit sich die Leistungen des Externen auf Geschäfte beziehen, die bei einer Leistungserbringung durch den Zahlungsdienstleister selbst von den Mindestanforderungen erfasst wären**.

**5. Zu 2.5 Nachvollziehbarkeit von Transaktion und e-Mandaten**

a) „e-Mandate" sind im Rundschreiben nicht definiert, so dass der Anwendungsbereich dieser Vorgaben im Unklaren bleibt. Es wird angeregt, auf die Definition der EZB in den SecuRe Pay-Empfehlungen zurückzugreifen, wonach die Herausgabe und Änderung elektronischer Lastschriftmandate gemeint war.

b) Zu Tz.37 sollte klargestellt werden, dass die vorvertraglichen Informationspflichten nach § 675d Abs. 1 Satz 1 BGB i.V.m. Art. 248 §§ 1 bis 16 EGBGB nicht verändert werden sollen und dass insbesondere gegenüber Unternehmen abweichende Vereinbarungen nach § 675e Abs. 4 BGB unberührt bleiben.

## 6. Zu 3.2 starke Kundenauthentisierung

a) Grundsätzlich unterstützt die IK den Regelungsgedanken, Zahlungen im Internet sicherer zu machen und Kunden (Karteninhaber), aber auch die Institute in eigenem Interesse vor Betrug zu schützen. Dazu gehören insbesondere auch Maßnahmen einer risikoangemessenen Anpassung des Sicherheitsniveaus im Bereich der Kundenauthentifizierung. Eine hoheitlich vorgegebene Definition eines Sicherheitsstandards darf jedoch nicht auf produkt-, geschäfts- und unternehmensbezogene Risikodifferenzierungen verzichten. In gleicher Weise kann von den Anbietern auf dem Kartenzahlungsmarkt nicht ohne angemessene betriebliche und technische Vorbereitungszeit ein radikaler Eingriff in bestehende Prozess-, Transaktions- und Vertragsstrukturen erwartet werden, da die starke Kundenauthentisierung massive Eingriffe für etablierte Zahlungsprozesse im Internet, insbesondere im Online-Handel bedeutet. Übersehen wird hierbei, dass zahlreiche Internet-Handelsaktivitäten, die breitflächig für Arbeitsplatzwachstum gesorgt haben, auf einfache Authentisierungsmethoden risikoorientiert zurückgreifen. Nahezu jeder Online-Händler müsste künftig für die Annahme von Internet-Zahlungen erhebliche Investitionen in seine technische Ausstattung tätigen. Aus einer Händlerperspektive betrachtet müssen somit erhebliche Kostensteigerungen bei der Zahlungsabwicklung in Kauf genommen werden, soweit für weitgehend jede Form von Internetzahlungen starke Kundenauthentisierung gefordert werden sollte. Da sich die aufsichtlichen Anforderungen damit erheblich belastend auf Händler erstrecken, die selbst nicht der Finanzregulierung unterliegen, kann eine starke Kundenauthentisierung gegenüber Zahlungsdienstleistern im **Einzelhandel** nicht mittels einer belastenden Verwaltungsmaßnahme, sondern nur unter Beteiligung der berufenen parlamentarischen Gremien gefordert werden. Die besondere Relevanz dieses Aspekts wird auch deutlich in der hohen Strittigkeit dieses Punkts im noch laufenden Gesetzgebungsverfahren der PSD-2.

b) Besonders bei der Pflicht starke Kundenauthentisierung einzusetzen stellt sich die eingangs erörterte Frage nach dem Vorbehalt des Gesetzes, da diese Authentifizierungsmethode den Instituten nach Auffassung der IK nicht durch einfache Verwaltungsrichtlinie auferlegt werden kann. Schließlich wären die Institute hieraus verpflichtet ihre eigenen Zahlungsprodukte und die bisher verwendeten Authentisierungsmechanismen komplett umzugestalten, soweit nicht heute bereits im Internet-Zahlungsverkehr „Besitzmedien“ eingesetzt werden. Bei Kreditkartenzahlungen im Internet entscheiden sich jedoch zahlreiche Händler aus Kosten- und Risikogesichtspunkten dafür, alleine auf der Grundlage der Kreditkartendaten Zahlungen zu akzeptieren und Betrugsrisiken mit transaktionsbasierten Kontrollmechanismen

zu bewältigen. Eine etwaige flächendeckende Pflicht zur Vorhaltung von Kartenlesegeräten oder Einsatz sonstiger Besitzmechanismen würde die Erfolgsgeschichte des online-Handels europaweit erheblich zurückwerfen. Darüber hinaus ist anzumerken, dass eine stark wachsende Anzahl von Einkäufen im online-Handel nicht mehr am heimischen PC erfolgt, sondern – aus dem heutigen, veränderten Lebensstil resultierend, mit Hilfe von mobilen Endgeräten, wie Smartphones oder Tablets erfolgt. Gerade bei der steigenden Verwendung von mobilen Endgeräten für die Einkäufe im online-Handel erscheint eine vorgeschriebene Verwendung von Besitzmechanismen als nicht verbraucherfreundlich und würde als Hemmschuh für die weitere Entwicklung des online-Handels wirken.

Die IK hält die volkswirtschaftlichen Nachteile und Belastungen des elektronischen Handels im Internet durch eine flächendeckende Forderung von starker Kundenauthentisierung für so bedeutsam, dass es alleine dieser Aspekt verdient, vertieft in einer branchenübergreifenden Diskussion des Gesetzgebers auch mit Vertretern des Handels und der Finanzbranche behandelt zu werden. Die IK sieht mit Sorge, dass die denkbaren Konsequenzen aus dieser Umsetzung bei weitem mehr gesamtwirtschaftliche Nachteile als Vorteile bringen und dass dies ggf. auf politischer Ebene noch nicht ausreichend erkannt wird.

c) Erneut sind die Differenzen zwischen dem Kartenzahlungs- und dem Überweisungsverkehr auch bei diesem Aspekt einzubeziehen: Bei letzterem hat die Online-Bank selbst die technologische Hoheit über das dem Kunden angebotene Authentisierungsverfahren und bestimmt daher autonom über die Umsetzung der entsprechenden Sicherheitsanforderungen. Die Kreditkartenissuer oder-acquirer haben diese Autonomie gerade nicht, da sie vollständig vom Angebot der Kreditkartensysteme abhängig sind und nicht einseitig / isoliert für eine mehrgliedrige Kreditkartentransaktion einen eigenen Standard verlangen können.

d) Die Frage der im Einzelfall einzusetzenden Authentisierungsmedien war bislang eine, dem Gesetz und der Regulierung nicht unterliegende geschäftspolitische Entscheidung eines Zahlungsdienstleisters unter Abwägung allgemeiner Risiko- und Kosten-Nutzen-Gesichtspunkten und darf nicht ohne gesetzliche Grundlage breitflächig von allen Instituten im Sinne einer Aufsichtspraxis verpflichtend vorgegeben werden.

e) Gegen eine Regulierungsvorgabe zur Authentisierungsmethode ist auch vorzubringen, dass hiermit ohne Not hoheitlich technologischer Fortschritt gehemmt wird. So werden insbesondere im Bereich der Kartenzahlungen große Investitionen und Anstrengungen unternom-

men, Kartenzahlungen im online Handel zukünftig mit sog. Tokens abzuwickeln. Tokens sind Einmal-Zahlungsdaten. Die Verwendung von Tokens macht die Zahlungen für Verbraucher und Händler einfacher und sicherer, da Tokens – selbst wenn es zu Datenabgriffen käme – nicht verwendet werden können, um damit betrügerische Transaktionen auszuführen. Regulierungsvorgaben zur Authentifizierungsmethode bei Zahlungen, die auf Basis von Tokens ausgeführt wurden, würde alle Anstrengungen und Investitionen in den neuen Tokenisierungsstandard hemmen.

f) Erneut ist darauf hinzuweisen, dass britische Zahlungsdienstleister unter Berücksichtigung der FCA-Implementierungspraxis diesen staatlich vorgegebenen Authentisierungspflichten zunächst nicht unterliegen werden und damit vorerst nicht gezwungen sind, ihre Zahlungsprodukte entsprechend kostenbelastend gegenüber dem Markt anzubieten. Auf die eingangs dargestellte Wettbewerbsverzerrung im „Level-Playing-Field“ des paneuropäischen Internetzahlungsverkehrs weisen wir erneut hin.

   Die IK plädiert daher dafür, die den Zahlungsverkehrsmarkt belastende generelle Pflicht zur Verwendung starker Kundenauthentisierung der gesetzlichen Regelung in Umsetzung der PSD-2 vorzubehalten und dies nicht im Rahmen einer Verwaltungsrichtlinie „vorzuziehen“.

g) Will die BaFin gleichwohl an Vorgaben zur starken Kundenauthentisierung ohne gesetzliche Grundlage festhalten, sollte auch hier betont werden, dass sich dies ausschließlich auf Retailzahlungen erstreckt und nicht auf den strukturell hiervon sehr unterschiedlichen Bereich des unternehmerischen Zahlungsverkehrs (Firmenkunden), die Zahlungsprodukte im Reisekostenmanagement oder in betrieblichen Beschaffungsprozessen einsetzen.

h) Entsprechend ist auch bei Tz.47 klarzustellen, dass nicht „alle ausgegebenen Karten“ in der Lage sein müssen mit starker Authentisierung genutzt zu werden, sondern allenfalls diejenigen, die dem Anwendungsbereich dieser Pflicht unterliegen, einschließlich risikoproportionaler Bewertung von Einzelinstrumenten nach Maßgabe von Tz.43 und Tz.45.

i) Haftungsregelungen (Tz. 51) zu starker Kundenauthentisierung wird erst die PSD-2 festlegen. Bis zu deren Inkrafttreten ist eine „Berücksichtigung“ starker Kundenauthentisierung nach geltender Rechtslage unter PSD-1/BGB gar nicht gegenüber Verbrauchern in Abweichung von § 675 u ff. BGB möglich.

j) Eine Begründung von Pflichten gegenüber Anbietern von Wallet-Lösungen (Tz. 52, 53) ist nicht möglich, soweit diese als Nicht-Institute aufsichtsfrei Wallet-Lösungen in Kooperation mit Zahlungsdienstleistern anbieten und damit dem Rundschreiben gar nicht unterfallen. Insofern sind die entsprechenden Ausführungen zu streichen.

k) Der Dialogprozess zwischen Online-Händler und Zahlungsdienstleister (Tz. 57) darf nicht mit dem Authentisierungsprozess des Zahlers verwechselt werden, die Anforderung in Tz. 57 ist schlicht nicht umsetzbar. Im Dialogprozess zwischen Online-Händler und dessen Zahlungsdienstleister (=Kreditkartenacquirer oder Acquiring-Prozessor) werden zwar heute schon zur Erzielung gebotener IT-Sicherheit Verschlüsselungsmechanismen eingesetzt, nicht aber eine transaktionsbasierende Authentisierung, bei der ggf. der Online-Händler selbst (zusätzlich zum Zahler) ein weiteres Besitzmedium einsetzen müsste. Dies könnte zu einem weitgehenden Erliegen des Zahlungsverkehrs im Internet-Handel führen, wenn auch der Dialog mit dem Händler einer starken Kundenauthentisierung unterworfen werden sollte.

l) In Tz 58 kann wohl statt „an Kunden“ nur gemeint sein „…an Zahlungsdienstenutzer zur Erteilung von Zahlungsaufträgen“. Anderenfalls würden auch Online-Händler (=Kunden von Acquirern) erfasst, einschließlich jeder Form von Software-Lieferung an Online-Händler, was nicht im Sinne der recommendations oder des BaFin-Rundschreibens ist.

m) Erneut kann über Tz. 69 oder 72 nicht für Kreditkartenissuer oder -acquirer im Status eines Zahlungsinstituts eine Pflicht zum Betrieb von Betrugserkennungs- und -verhinderungssystemen durch Rundschreiben begründet werden, sondern nach dem Grundsatz des Vorbehalts des Gesetzes nur kraft gesetzlicher Änderung. Nach geltender Rechtslage gilt die Pflicht zum Betrieb von Systemen zur Bekämpfung von Straftaten nach § 25h Abs. 1 S. 1 und 2 KWG sowie die Pflicht zur betrugsorientierten, fortlaufenden Transaktionsüberwachung nach § 25h Abs. 2 KWG nur für Kreditinstitute, nicht aber für Zahlungsinstitute, vgl. § 22 Abs. 2 ZAG.

## 7. Zu Ziff. 4.1 Schulungen der Kunden

Eine etwaige Pflicht zur „Kundenschulung“ (Tz. 87) ist im Verbraucher-Massenzahlungsverkehr nicht umsetzbar. Etwaige Inhalte einer Pflicht zur Kundeninformation (Tz. 82) sollten erst mit Umsetzung der PSD-2 gesetzlich definiert werden.

## 8. Zu Ziff. 4.2 Festlegung von Limiten

Die PSD-1 hat aus guten Gründen davon abgesehen, Pflichten zur Setzung von Kundenlimiten (Tz. 89, 90 zu statuieren. So sieht § 675k Abs. 1 BGB konsequenterweise nur die Möglichkeit, aber nicht die Pflicht vor, Nutzungsobergrenzen zu vereinbaren. Die Statuierung einer entsprechenden Pflicht in einer Verwaltungsrichtlinie ist nicht möglich.

## 9. Zu Ziff. 4.3 Status der Zahlungsvorgänge

Bei Informationen zum Status der Zahlungsvorgänge ist zwischen Überweisungs- und Kartenzahlungsvorgängen zu differenzieren. Während bei Überweisungen ein online-Dialog zwischen kontoführender Bank und Zahler besteht, ist dies bei der Kartenzahlung zwischen Issuer und Karteninhaber nicht der Fall. Soweit vereinbart, kann zwar nachträglich über eine autorisierte Transaktion informiert werden, jedoch ist es bedeutsam, dies nicht als Pflicht zu statuieren, da dies häufig nicht im Interesse des Karteninhabers ist und er häufig keine transaktionsbezogenen Geschäftsbestätigungen wünscht. Angestrebter Verbraucherschutz darf daher auch nicht zur Bevormundung führen, so dass – erneut – eine diesbezügliche Pflichtenbegründung in der Verwaltungsrichtlinie nicht vorgesehen werden sollte.

Gerne erläutern wir unsere Ausführungen auch im Rahmen eines persönlichen Gesprächs mit Ihnen.

Mit freundlichen Grüßen,

Dr. Markus Escher
- für die Interessengemeinschaft Kreditkartengeschäft -