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

Deutscher Sparkassen- und Giroverband e. V. |
Charlottenstraße 47 | 10117 Berlin

Bundesanstalt für Finanzdienstleistungsaufsicht
Referat BA 57
Herr Martin
Graurheindorfer Straße 108
53117 Bonn
Deutschland

Kontakt: Martin Stein
Telefon: +49 30 20225- 5515
E-Mail: martin.stein@dsgv.de

Kontakt: Dr. Kai Zahrte
Telefon: +49 30 20225- 5367
Fax: +49 30 20225- 5345
E-Mail: kai.zahrte@dsgv.de

AZ DK: OB

Konsultation 02/2015 – Entwurf eines Rundschreibens zu Mindestanforderungen an die Sicherheit von Internetzahlungen

19. März 2015

Sehr geehrter Herr Martin,
sehr geehrter Herr Dr. Lutz,
sehr geehrter Herr Dr. Kokert,

Anlagen

zunächst dürfen wir uns verbindlich für die Möglichkeit bedanken, zu Ihrem Entwurf eines Rundschreibens Stellung nehmen zu können, welcher der Umsetzung der Leitlinien der European Banking Authority (EBA) zur Sicherheit von Internetzahlungen von Dezember 2014 dienen soll.

Die Wahrung der Sicherheit und des Schutzes von Daten bei Internetzahlungen liegen im ureigenen Interesse der Kreditinstitute. In Deutschland erfüllen Banken und Sparkassen bereits heute höchste Sicherheitsanforderungen. Deswegen begrüßen wir es ausdrücklich, dass es zu einer Klarstellung von kreditaufsichtsrechtlichen Anforderungen bei der stetig zunehmenden Zahl von Internetzahlungen kommt.

Wir haben allerdings einige Punkte identifiziert, die aus unserer Sicht präzisiert oder modifiziert werden sollten. Diese werden im Folgenden allgemein dargestellt. In dem als **Anlage** beigefügten Dokument finden Sie zudem unsere Anmerkungen zu einzelnen Textziffern Ihres Entwurfs.

1. Europäisch einheitliche Wettbewerbsbedingungen: Keine über die Anforderungen der EBA hinausgehenden Belastungen für deutsche Kreditinstitute

Um den Wettbewerb der deutschen Kreditinstitute sowohl mit Anbietern, die keine Zahlungsdienstleister sind, als auch mit Kreditinstituten im EU-Ausland nicht zu behindern, ist es von besonderer Wichtigkeit, dass die Anforderungen der BaFin nicht über den von der EBA gesetzten Rahmen hinausgehen. Konkrete Beispiele sind u.a. zusätzliche Meldepflichten, die

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

über die Störungen in der Abwicklung von Internetzahlungen hinausgehen, neue Anforderungen an die TAN-Absicherung und die Erfassung des Telefonbanking.

Bereits heute weist der kreditwirtschaftliche Sektor im Zahlungsverkehrsbereich eine Regulierungsintensität auf, die es den deutschen Kreditinstituten schwer macht, sich mit innovativen Lösungen etwa gegen Zahlungsdienstleister aus Luxemburg oder gegen IT-Dienstleister ohne ZAG-Lizenz zu behaupten.

Eine weitere Verschärfung dieses Ungleichgewichts hätte nicht zuletzt zur Folge, dass die Kunden verstärkt die Verfahren von Nicht-Kreditinstituten nutzen würden, da aus deren Sicht diese einfacher zu bedienen oder preiswerter wären. Da diese Verfahren bislang weitgehend dem Einflussbereich der BaFin entzogen sind, würde das – neben den wirtschaftlichen Auswirkungen für die Kreditinstitute in Deutschland – insgesamt eine Absenkung des Verbraucherschutzniveaus im Internetzahlungsverkehr zur Folge haben. Gerade dies soll aber mit den Vorschlägen der EBA bzw. der Umsetzung durch die BaFin verhindert werden.

2. Beschränkung der Anforderungen auf die jeweilige Sphäre des Zahlungsdienstleisters

Bei den aufsichtsrechtlichen Anforderungen sollte stärker berücksichtigt werden, dass sich die Einflussnahme einzelner Zahlungsdienstleister im Rahmen eines Zahlungssystems (Schemes) auf die jeweilige Sphäre bzw. Rolle beschränkt. Eine durchgängige Abbildung und wirtschaftlich tragbare Umsetzung ist nur unter Berücksichtigung aller Parteien – Zahlungsdienstleister, Systembetreiber, Händler - und deren jeweiligen Rollen möglich. Dies gilt insbesondere für Kartenzahlungen, die maßgeblich den Regeln der internationalen Kreditkartenorganisationen unterworfen sind.

3. Keine Ausweitung des Anwendungsbereiches gegenüber den Anforderungen der EBA

Ein besonders gravierender Punkt, in dem der Rundschreibenentwurf teilweise über die EBA-Leitlinien hinausgeht, ist der sachliche Anwendungsbereich.

Die EBA-Leitlinien erfassen ausschließlich browser-basierte Verfahren. Das Telefonbanking und Verfahren für Kundenprodukte, wie EBICS und FinTS, sind von den EBA-Guidelines ausdrücklich ausgenommen. Diesem Ansatz sollte das Rundschreiben folgen.

Des Weiteren gehen wir davon aus, dass die Anforderungen im Lastschriftgeschäft allein für die Ausgabe und Änderung von E-Mandaten gelten, wie sie beispielsweise in Annex VII des Regelwerks des European Payments Council zur SEPA-Lastschrift beschrieben werden und bei dem die Autorisierung der Zahlstelle direkt über eine Online-Banking-ähnliche Infrastruktur stattfindet.

4. Keine Vorwegnahme zukünftiger gesetzlicher Regelungen

Der Rundschreibenentwurf enthält Regelungen, die erst mit der derzeit laufenden Novelle der EU-Zahlungsdiensterichtlinie (PSD II) sowie mit dem gerade in nationaler Abstimmung befindlichen IT-Sicherheitsgesetz (IT-SiG) zukünftig auf eine gesetzliche Grundlage gestellt werden sollen.

Anpassungen von IT-gestützten Prozessen sind in der Kreditwirtschaft regelmäßig mit erheblichem Aufwand und einer längeren Vorlaufzeit verbunden. Vor diesem Hintergrund wäre es eine unverhältnismäßige

Belastung für die Institute, wenn das Bankaufsichtsrecht sie zum jetzigen Zeitpunkt zu einer Anpassung von Prozessen zwingen würde, die möglicherweise in kürzester Zeit durch neue gesetzliche Regelungen nochmals aufwändig zu modifizieren wären. Deswegen sollte unbedingt der Ausgang der Beratungen zur PSD II und zum IT-SiG abgewartet werden, um Doppelaufwand oder Pflichtenkollisionen zu vermeiden.

5. Verweise nur auf geltendes nationales Recht

Im Entwurf wird mehrfach – in wortgetreuer Umsetzung der EBA-Grundlage – die Zahlungsdiensterichtlinie (RL 2007/64/EG – PSD I) referenziert. Diese gilt aber in Deutschland als europäische Richtlinie nicht unmittelbar, sondern wurde in zahlreichen Vorschriften des Bürgerlichen Gesetzbuchs (BGB), des Zahlungsdiensteaufsichtsgesetzes (ZAG) und des Einführungsgesetzes zum Bürgerlichen Gesetzbuche (EGBGB) umgesetzt. Dabei hat der nationale Umsetzungsgesetzgeber teilweise die in der PSD I angelegten Optionen für nationale Sonderregeln genutzt. Deswegen sollten Verweise nicht auf die PSD I, sondern stets auf die hierzulande geltende gesetzliche Grundlage, also die Vorschrift aus BGB, ZAG oder EGBGB erfolgen.

6. Referenzierung anerkannter europäischer Technikstandards

Aufgrund der europäischen Auslegung der EBA-Richtlinien sollte in dem Rundschreiben keine Referenzierung auf nationale technische Richtlinien erfolgen. Sofern internationale (technische) Standards existieren, wie etwa der ISO 27001, sollten diese referenziert werden und als Nachweis der Regelkonformität im jeweiligen Bereich genutzt werden können. Darüber hinaus würde dies europäisch einheitliche Wettbewerbsbedingungen schaffen, weil die ISO-Standards internationale Geltung haben.

7. Begriff der sensiblen Zahlungsdaten

Die Deutsche Kreditwirtschaft begrüßt die Intention, den Kundendatenschutz im Internetzahlungsverkehr in Europa weiter zu stärken. Dies deckt sich mit den Bestrebungen der Kreditinstitute.

Allerdings wird der Begriff der „sensiblen Zahlungsdaten“ im Rundschreiben inkonsistent genutzt. Wir verstehen unter diesem Begriff gemäß der EBA-Leitlinien solche Daten, die zur Authentisierung einer Zahlungstransaktion im Internet dienen. Wir gehen davon aus, dass Sie unserem Verständnis folgen können und keine Doppelregulierung oder sogar Kollision mit den geltenden Datenschutzvorschriften des Telemediengesetzes und des Bundesdatenschutzgesetzes sowie mit den zivilrechtlichen Rahmenbedingungen im Zahlungsdiensterecht (§§ 675c ff. BGB) beabsichtigen.

Wir schlagen deshalb in der Anlage eine Präzisierung des Begriffs vor. Damit soll einerseits eine Abgrenzung zwischen den aufsichtsrechtlichen Anforderungen, dem Zahlungsdiensterecht im BGB und den Datenschutzvorschriften (BDSG und Telemediengesetz) erfolgen und andererseits eine Beibehaltung etablierter Prozesse und Verfahrensabläufe sicher gestellt werden, die sich in der Vergangenheit vor dem Hintergrund des Datenschutzrechts als unproblematisch erwiesen haben.

8. Comply-or-Explain-Prinzip

Aufgrund der Entstehungsgeschichte und der Ziele der EBA-Leitlinien gehen wir davon aus, dass die Erfüllung einer aufsichtsrechtlichen Anforderung auch mit anderen als den genannten Mitteln den aufsichts-

rechtlichen Vorgaben genügt werden kann, wenn die Gleichwertig vom Zahlungsdienstleister überzeugend erklärt werden kann („Comply-or-Explain-Prinzip“).

Wir bitten Sie unsere Anmerkungen im Rahmen des finalen Rundschreibens zu berücksichtigen. Gegen eine Veröffentlichung unserer Stellungnahme auf der Homepage der BaFin haben wir keine Einwände. Darüber hinaus würden wir Ihnen unsere Anliegen gerne in einem persönlichen Gespräch erläutern.

Mit freundlichen Grüßen
für Die Deutsche Kreditwirtschaft
Deutscher Sparkassen- und Giroverband e.V.

i. A.

Dr. Kai Zahrte

i. A.

Martin Stein

Anlage

Anmerkungen zu einzelnen Textziffern des Entwurfs eines Rundschreibens zu Mindestanforderungen an die Sicherheit von Internetzahlungen

Begriffe:

Folgende im Rundschreibenentwurf verwendete Begriffe sind für das Verständnis der Adressaten von besonderer Bedeutung. Deshalb sollten die Termini wie folgt durchgehend einheitlich definiert und verwendet werden:

- „Autorisierung“ wird von § 675j Abs. 1 BGB legal definiert als „Einwilligung oder Genehmigung eines Zahlungsvorgangs“. Es handelt sich dabei also um eine Willenserklärung.
- „Authentisierung“ bezeichnet den Nachweis der Echtheit von Zahlungsdaten im Sinne von Integrität und Nichtabstreitbarkeit.
- „Identifikation“ bezeichnet die Feststellung einer Person. Diese Identifikation kann dann im Wege der Authentisierung verifiziert werden.
- “Sensible Zahlungsdaten“ sind Daten, die zur Authentisierung einer Zahlungstransaktion im Internet dienen. Daten, die zur Zuordnung eines Kunden zu seinem gewählten Zahlverfahren genutzt werden können, wie z.B. Benutzerkennung, Kreditkartennummer und Kontonummer bzw. IBAN, gehören nicht dazu. Auch Kontoauszugsinformationen fallen hier nicht unter den Begriff sensible Zahlungsdaten, da sie bereits durch die allgemeinen Datenschutzvorschriften ausreichend geschützt sind.
- Der Begriff „Acquirer“ bezeichnet gemäß ZAG einen Zahlungsdienstleister der Dienste nach § 1 Abs. 2 Nr. 4 Alt. 2 anbietet.
- Die „Datenminimierung“ ist in §3a BDSG beschrieben.

Zu Tz 2:

Die Erweiterung des Geltungsbereiches auf das Telefon-Banking ist nicht nachvollziehbar. Beim Telefon-Banking handelt es sich der Natur nach nicht um einen „Internet-Zahlungsdienst“. Auch sind die meisten Anforderungen schon rein technisch nicht auf das Telefon-Banking übertragbar. Daher ist das Telefon-Banking auch bewusst nicht Bestandteil der EBA-Leitlinien: „*Excluded from the scope of the guidelines are:-…- payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology-…*” (Seite 10, Punkt 11).

Ähnliches gilt für Zahlungen per Kundensoftware (sog. „Online-Banking-Client“) auf Basis der in Deutschland üblichen Kommunikationsstandards FinTS und EBICS. Auch diese sind keine rein Internet-basierten Bezahlverfahren und daher nicht Gegenstand der zugrunde liegenden EBA-Leitlinien. In den meisten Fällen werden diese Softwareprodukte von Drittanbietern zur Verfügung gestellt, d.h. die Verantwortungs- und Haftungssphäre des Zahlungsdienstleisters kann nicht die einzelne Software umfassen.

Des Weiteren gehen wir davon aus, dass im Lastschriftgeschäft die Anforderungen gemäß den EBA-Leitlinien nur die Ausgabe und Änderung von E-Mandaten erfassen, wie sie beispielsweise in Annex VII des Regelwerks des European Payments Council zur SEPA-Lastschrift beschrieben werden. In diesem Verfahren findet die Autorisierung der Zahlstelle direkt über eine Online-Banking-ähnliche Infrastruktur statt. Im Falle der heute vielfach praktizierten Erteilung von SEPA-Lastschriftmandaten im elektronischen Geschäftsverkehr ist zu berücksichtigen, dass dabei noch keine E-Mandate eingesetzt werden, sondern der Zahler das konventionelle Mandat direkt gegenüber dem Händler erteilt, d.h. einem nicht der Bankaufsicht unterliegenden Unternehmen. Im Zeitpunkt des elektronischen Geschäftsabschlusses und der Auswahl des Zahlverfahrens ist der Zahlungsdienstleister des Zahlers nicht eingebunden. Eine Ausweitung des Anwendungsbereiches von Tz 42 über das in Annex VII definierte Verfahren hinaus würde somit einen Eingriff in die Vertragsgestaltung von unzähligen Internetunternehmen mit ihren Kunden bedeuten, deren finanzielle und tatsächliche Auswirkungen die aktuelle Erfüllungsaufwandsschätzung durch die BaFin bei Weitem übersteigen würde.

Grundsätzlich wird empfohlen, dass entsprechend der Ziffer 7 auf Seite 9 der EBA-Guidelines eine enumerative Auflistung der betroffenen Geschäftsvorfälle erfolgen sollte. Analog zu Ziffer 11 sollte ebenfalls aufgelistet werden, welche Verfahren nicht von den Anforderungen betroffen sind.

Zu Tz 6:

Der Begriff der „sensiblen Zahlungsdaten“ sollte nicht das Ergebnis der Beratungen zur PSD II vorwegnehmen. Hier ist auf kohärente Belegung der Begriffe zu achten (vgl. den Formulierungsvorschlag oben).

Zu Tz 7:

Im Rahmen der Erläuterungen wird auf nationale Sicherheitsstandards und -rahmenwerke referenziert. Im Interesse europäisch einheitlicher Wettbewerbsbedingungen sollte stattdessen nur auf international anerkannte Normen wie bspw. ISO 27001 abgestellt werden.

Zu Tz 15:

Es ist zu beachten, dass derzeit der Regierungsentwurf eines IT-Sicherheitsgesetzes im Deutschen Bundestag beraten wird, der ebenfalls die Meldung kritischer Sicherheitsvorfälle zum Inhalt hat. Hier muss eine zeitlich versetzte Doppelregulierung verhindert werden. Es wird daher empfohlen, die Aussagen unter dieser Teilziffer erst nach Verabschiedung des IT-Sicherheitsgesetzes zum Gegenstand eines separaten Rundschreibens zu machen.

In jedem Fall sollte vermieden werden, bereits bestehende Meldepflichten aus anderen Rechtsbereichen noch einmal über Verweistechniken in das Bankaufsichtsrecht hineinzuziehen.

Meldepflichten nach dem Rundschreiben sollten sich, wie in den EBA-Guidelines definiert, ausschließlich auf IT-Sicherheitsvorfälle bei Internet-Zahlungen beziehen. Ansonsten würden sich weitere Fragestellungen anschließen, z.B.:

- Reicht die Meldung an das BSI aus? Die Weiterleitung an die Aufsicht ist im IT-SiG vorgesehen.
- Wird das Meldeformular der BaFin vom BSI akzeptiert?
- Kann die Meldung eines Instituts analog IT-SiG über einen „Single Point of Contact“ (SPOC) erfolgen?

Ferner gehören die in der Erläuterung genannte Bargeldversorgung sowie der klassische Kartenzahlungsverkehr nicht in den anfangs definierten Anwendungsbereich des Rundschreibens (Internetzahlungen) und sollten daher nicht als Beispiele für Anwendungsfelder kritischer IT-Sicherheitsvorfälle aufgeführt werden. Auch die Konkretisierung von Ausfällen auf einen Zeitraum von mehr als einer Stunde halten wir für nicht sachgerecht, da die Wichtigkeit eines IT-Sicherheitsvorfalls nicht allein an dessen zeitlicher Dauer festgemacht werden kann. Wir empfehlen daher, den Instituten hier einen Ermessensspielraum einzuräumen.

Zu Tz 16:

Der Text in der Erläuterung bzgl. Unterstützung betroffener Kunden bei der Stellung eines Strafantrags sollte entfallen. Denn ein Einzelbetrugsfall bei einem Endkunden ist kein kritischer IT-Sicherheitsvorfall im Sinne der Tz 15 und 16 und geht auch über die Definition 3.3 der EBA-Guidelines hinaus.

Zu Tz 19:

Das Prinzip der Verteidigung in der Tiefe sollte genau wie in der Originalformulierung der EBA wie folgt verwendet werden:

„Das Prinzip der Verteidigung in der Tiefe bedeutet, dass das Versagen einer Verteidigungslinie durch andere Verteidigungslinien kompensiert wird.“

Zu Tz 23:

Die allgemeine Anforderung “Die Websicherheit ist zu gewährleisten“ sollte im Sinne der konkreteren Beschreibung in Ziffer 4.2 der EBA-Guidelines ersetzt werden durch: „Die Websicherheit ist durch Extended Validation Zertifikate oder durch andere ähnliche *Authentifizierungsmethoden zu schützen.“*

zu TZ 24

Um datenschutzrechtliche Rahmenbedingungen angemessen zu berücksichtigen wird folgende Formulierung vorgeschlagen:

„Der Zugang zu

a) sensiblen Daten

b) logischen und physisch kritischen Ressourcen

ist zu überwachen, nachzuverfolgen und zu beschränken. Es sind geeignete Logdaten und Prüfprotokolle zu erstellen, zu speichern und zu analysieren*, soweit dies nach den auf die Speicherung und Auswertung von Daten anzuwendenden gesetzlichen Vorschriften zulässig ist.“*

Zu Tz 25:

Es sollte klargestellt werden, dass mit „Datenminimierung“ eine Umsetzung des Prinzips der Datenvermeidung und Datensparsamkeit gem. § 3 a BDSG gemeint ist.

Das Sammeln, Weiterleiten, Verarbeiten, Speichern und/oder Archivieren sowie die Visualisierung sensibler Zahlungsdaten *ist im Rahmen der hierfür geltenden Gesetze* auf ein Minimum zu begrenzen.

Zu Tz 26:

Im Sinne einer einheitlichen Terminologie sollte durchgehend der Begriff „Internet-Zahlungsdienst“ Anwendung finden.

Zu Tz 36:

Bislang regeln Kreditkartenverträge (Vertrag zwischen Kartenausgeber und Karteninhaber) die unterschiedlichen Einsatzszenarien der Karte nicht immer explizit. Die Möglichkeit des Karteneinsatzes im Internet ist aber eine allgemein bekannte Standardfunktion der Karte und damit auch ohne wörtliche Erwähnung im Rahmen einer Vertragsauslegung als vereinbarte Funktion zu werten.

Sofern eine darüber hinausgehende explizite Darstellung im Vertrag erwartet wird, sollte klargestellt werden, dass dies nur für zukünftige Verträge gilt, damit nicht mit allen Bestandskunden, die heute bereits Kreditkarten im Internet nutzen, neue Verträge zu vereinbaren sind.

Die Einhaltung der geldwäscherechtlichen Vorschriften des GwG in der Erläuterung ist selbstverständlich und sollte nicht durch Erwähnung an dieser Stelle einen neuen bankaufsichtsrechtlichen Charakter erhalten.

Zu Tz 37:

Die Formulierung „ausgehändigt“ sollte durch „zur Verfügung gestellt“ ersetzt werden, da bei Online-Zahlungen die Informationserteilung regelmäßig auf anderen Kanälen als durch physische Übergabe erfolgt und auch eine Abrufmöglichkeit auf einer Internetseite des Zahlungsdienstleisters ausreichen sollte.

Ferner sollte in der Erläuterung auf die Vorschrift zu Informationspflichten in Art. 248 EGBGB referenziert werden, da die EU-Zahlungsdiensterichtlinie in Deutschland nicht unmittelbar gilt.

Zu Tz 41:

Diese Anforderung ist nicht Bestandteil der EBA-Guidelines und sollte daher gestrichen werden.

Zu Tz 42:

Die Ausführungen im zweiten Absatz der Erläuterung gehen deutlich über die Forderungen der EBA hinaus. Weder wird dort gefordert, dass wesentliche Transaktionsdaten in die Generierung der TAN eingehen und angezeigt werden müssen, noch wird gefordert, dass die Zwei-Faktor-Authentisierung unabhängig von der primären Verbindung zum Zahlungsdienstleister ausgestaltet sein muss. Es handelt sich somit nicht um eine Erläuterung der zugrunde liegenden Anforderung, sondern um eine Verschärfung, auf die im Sinne der einheitlichen europäischen Regulierung verzichtet werden sollte.

Zu Tz 43:

3. Aufzählungspunkt: Der Geltungsbereich dieser Regelung sollte nicht nur auf Transaktionen innerhalb desselben Zahlungsdienstleisters beschränkt werden, sondern auch für Transaktionen zwischen Zahlungsdienstleistern desselben IT-Dienstleisters einer Verbundgruppe oder eines Bankkonzerns gelten.

4. Aufzählungspunkt: Bzgl. Kleinbetragszahlungen sollten die Betragsgrenzen nicht aus der EU-Zahlungsdiensterichtlinie übernommen werden, sondern die Betragsgrenzen aus § 675i BGB verwendet werden.

Zu Tz 44:

Siehe einleitende Definitionen.

Zu Tz 45:

Um zu vermeiden, dass ausschließlich Zahlungsdienstleister, die kein weiteres Geschäft betreiben, von der Erleichterung profitierten, wird empfohlen, die Formulierung wie folgt zu ändern: *„Wenn ein Zahlungsdienstleister Dienste anbietet, bei denen keine Transaktionen ausgeführt werden…“*

Zu Tz 46:

Um die geschäftspolitische Diversifikation zu erhalten, muss es Zahlungsdienstleistern auch zukünftig gestattet sein, Zahlungskarten herauszugeben, die nicht für Internetzahlungen zugelassen sind.

Eine starke Authentisierung führt nur dann flächendeckend zu mehr Sicherheit, wenn diese Vorgabe für alle Zahlungssysteme gelten, explizit auch für diejenigen, die unter das „Closed Loop“- Prinzip fallen. Ansonsten wäre damit zu rechnen, dass Kunden auf bequemere Verfahren ausweichen. Somit ergäbe sich eine Situation, in der ein nicht regulierter Zahlungsdienstleister den europäischen Banken gegenüber gravierend bevorzugt würde.

Darüber hinaus kann bei Mehrparteien-Systemen (z.B. Kreditkarte) eine einseitige Verpflichtung zur starken Authentisierung in der Praxis nicht wirksam umgesetzt werden, da hierfür entscheidend ist, ob auch

der Händler die starke Authentisierung unterstützt. Insofern sollte die Vorgabe mit dem Zusatz versehen werden die „Authentisierung des Karteninhabers zu unterstützen *sobald auch der Händler ein entsprechendes Verfahren unterstützt*".

Zu Tz 47:

Die Forderung sollte auf neu ausgegebene Karten beschränkt werden. Ferner sollten die Anforderungen auf Karten beschränkt werden, die im Internet eingesetzt werden können.

Zu Tz 50 und 54:

In der Erläuterung sollte auf § 675i BGB anstatt auf die EU-Zahlungsdiensterichtlinie referenziert werden.

Zu Tz 50:

Es wird davon ausgegangen, dass ein alternatives Authentisierungsverfahren auch der Verzicht auf eine Authentisierung des Karteninhabers sein kann, wenn dadurch dem Kunden kein Haftungsnachteil entsteht.

Zu Tz 51:

Diese Anforderung sollte gestrichen werden, da diese im Widerspruch zur geltenden zivilrechtlichen Regelung der §§ 675u, v BGB stehen würde. Abgesehen davon ist sie auch in den EBA-Leitlinien vor dem Hintergrund der laufenden Beratung gestrichen worden. Damit nicht nach Verabschiedung der PSD II eine neuerliche Anpassung der Kundenbedingungen notwendig wird, sollte dem Ansatz der EBA gefolgt werden.

Zu Tz 53:

Eine starke Authentisierung sollte auch bei Wallet-Lösungen ausschließlich für die Durchführung von Zahlungen gefordert werden, nicht aber für das Login.

Ferner sollte eine einheitliche Begrifflichkeit gewählt werden („Wallet-Lösung", „Wallet-Zahlungsdienst").

Zu Tz 58:

Hierbei handelt es sich nicht um eine Anforderung. Die Tz sollte gestrichen oder mit Tz 59 verknüpft werden.

Zu Tz 61:

Der Passus „vom Zahlungsdienstleister" sollte gestrichen werden, da Kreditinstitute oftmals Software von Drittherstellern anbieten und somit die Software nicht selbst signieren können.

Zu Tz 69:

Die Systeme zur Erkennung und Verhinderung von Manipulationen unterliegen datenschutzrechtlichen Begrenzungen. Darauf ist hinzuweisen, damit deutlich wird, dass die bankaufsichtsrechtlichen Anforderungen nicht über das datenschutzrechtlich Mögliche hinausgehen.

Es wird empfohlen, das Wort „Systeme“ durch die flexiblere Formulierung „Mechanismen“ zu ersetzen. Kapitel 5 der EZB-Empfehlungen spricht in diesem Zusammenhang treffend von „Sicherheits-Mechanismen“.

Weiterhin sollte im zweiten Halbsatz das Wort „autorisiert“ durch „ausgeführt“ ersetzt werden. Denn die Autorisierung erfolgt meist zu einem Zeitpunkt, zu dem noch nicht alle Informationen vorliegen, um eine Manipulation zu erkennen bzw. zu verhindern.

Zu Tz 70:

Es ist zu präzisieren, dass sich die Anforderung nur auf diejenigen Teile der IT-Infrastruktur erstrecken kann, die sich in der Sphäre des Zahlungsdienstleisters befindet.

Analog zu TZ 69 wird empfohlen, das Wort „Systeme“ durch die flexiblere Formulierung „Mechanismen“ zu ersetzen.

Zu Tz 71:

Die Formulierung ist missverständlich, denn BDSG und TMG enthalten speziell in diesem Bereich keine „einschlägigen Vorschriften“.

Zu Tz 76:

Die Formulierung „zwischen Bank und Kunde“ sollte ersetzt werden durch „zwischen den kommunizierenden Teilnehmern“. Damit würde dem Wortlaut der EBA-Leitlinien gefolgt, welcher berücksichtigt, dass die kommunizierenden Teilnehmer (z. B. bei mehrstufigen Prozessen im Kartenzahlungsverkehr) nicht zwangsläufig Kunde und Zahlungsdienstleister sein müssen.

Zu Tz 77:

Statt einer Aufforderung durch die Acquirer sollte hier eine verbindliche Vorgabe an die Händler, keine sensiblen Zahlungsdaten zu speichern, zum Einsatz kommen. Für Kreditkarten ergibt sich dies beispielsweise bereits aus den PCI-Anforderungen.

Es wird darauf hingewiesen, dass der Online-Händler nach HGB, TMG und anderen Archivierungspflichten verpflichtet ist, Abrechnungsunterlagen und technische Protokolle zu erstellen, die je nach Definition (s.o.) ggf. sensible Zahlungsdaten enthalten können.

Zu Tz 78:

Diese Anforderung steht im Widerspruch zu Tz 77, in der gefordert wird, dass Online-Händler keine sensiblen Zahlungsdaten speichern dürfen.

Zu Tz 81 bis 84:

Die Anforderungen sollte dahingehend umformuliert werden, dass ein Zahlungsdienstleister auch mehrere gesicherte Kanäle anbieten kann und jeweils den bestgeeigneten Kanal für die Kundenkommunikation wählt bzw. mehrere Kanäle für die Kundenkommunikation kombiniert.

Zu Tz 87:

Die Anforderung sollte bspw. wie folgt umformuliert werden, da eine „Sicherstellung“ von Verständnis nicht möglich ist: „Es sind angemessene Maßnahmen zur Kundenschulung und Kundensensibilisierung durchzuführen, *um Kunden zu erklären,* …“.

Zu Tz 89 und 90:

Die Verantwortung des Zahlungsdienstleisters sollte sich darauf beschränken, die Möglichkeit der Limitsetzung anzubieten. Ob und in welcher Form der Kunde von diesem Angebot Gebrauch macht, liegt insbesondere in der Verantwortung des Kunden.

Vorgeschlagene Formulierung; *„Es sind Limite für die Zahlungsdienste zu setzen und bei Bedarf den Kunden Möglichkeiten für eine weitere Begrenzung dieser Limite bereitzustellen.“*

Zu Tz 91:

Es wird davon ausgegangen, dass die Deaktivierung der Internet-Zahlungsfunktion und nicht die Deaktivierung des Limits gemeint ist.

Zu Tz 92:

TZ 92 kann gestrichen werden, da die Anforderungen in Art. 248 §§ 7 ff. EGBGB einschlägig geregelt sind.

Zu Tz 93:

Die Formulierung “*in Echtzeit*“ sollte in „*unverzüglich, bei Kartentransaktionen spätestens zum Zeitpunkt der Abbuchung beim Zahler*“ geändert werden, da aufgrund buchungstechnischer Gegebenheiten eine Prüfung in „Echtzeit“ nicht immer möglich ist. Speziell bei Kreditkarten ist es in Deutschland allgemein üblich, dass der Karteninhaber durch die kartenausgebende Bank einmal im Monat eine Abrechnung erhält, üblicherweise kurz vor dem Zeitpunkt der Abbuchung am Bankkonto. Für Internetverfügungen sollten somit keine schärferen Anforderungen als für POS-Verfügungen gelten.