Bundesverband der Zahlungsinstitute e.V. Im Uhrig 7 60433 Frankfurt a.M.

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

Bundesanstalt für Finanzdienstleistungsaufsicht
Referat BA 57
zu Händen Herrn Martin
Graurheindorfer Straße 108

53117 Bonn

bvzi Bundesverband der Zahlungsinstitute

Im Uhrig 7
60433 Frankfurt am Main

Telefon: (069) 95 11 77-15
Telefax: (069) 52 10 90
www.bvzi.de
info@bvzi.de

VR 14320
Amtsgericht Frankfurt am Main

Präsidium (Vorstand):
Nicolas Adolph (Sprecher)
Dr. Karsten von Diemar
Bernd Kierdorf
Christof Kohns

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

Geschäftszeichen: BA 57-K 3142-2013/0017

Frankfurt am Main, 18. März 2015

Sehr geehrter Herr Martin,
sehr geehrte Damen und Herren,

am 4. Februar 2015 hatten Sie den Entwurf eines Rundschreibens zu den Mindestanforderungen an die Sicherheit von Internetzahlungen veröffentlicht.

Der Bundesverband für Zahlungsinstitute (**BVZI**) bedankt sich für die Möglichkeit einer Stellungnahme im Rahmen des Konsultationsverfahrens 02/2015. Diese Stellungnahme wurde durch die Mitglieder des BVZI unter Mithilfe der Rechtsanwaltskanzlei Hogen Lovells International LLP (Dr. Richard Reimer und Olaf Bausch) erstellt. Aufgrund der erheblichen praktischen Auswirkungen möchten wir zugleich um einen Meinungsaustausch im Rahmen eines persönlichen Gesprächs mit Ihnen bitten.

Grundsätzliche Anmerkungen – Integrität des Finanzmarktes

1. Der BVZI begrüßt die Festlegung von Mindestanforderungen an die Sicherheit von Internetzahlungen, um hierdurch einen entscheidenden Beitrag zum Schutz sensibler Zahlungsdaten sowie dem Kundenschutz insgesamt zu leisten.

2. Der Entwurf des Rundschreibens basiert zum einen auf den von der European Banking Authority (**EBA**) am 19. Dezember 2014 veröffentlichten "Guidelines on the security of internet payments" (**Guidelines**). Zum anderen basiert der Entwurf des Rundschreibens auf den "Recommendations for the Security of Internet Payments" (**Recommendations**) des European Forum on the Security of Retail Payments (**SecuRe Pay**) vom 31. Januar 2013.

3. Die EBA, als eines der freiwilligen Mitglieder des SecuRe Pay, nimmt mit Hilfe der veröffentlichten Guidelines ihre Aufgaben wahr, Leitlinien im Sinne von Artikel 16 der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (EBA-Verordnung) zu schaffen, um eine gemeinsame, einheitliche und kohärente Anwendung des Unionsrechts sicherzustellen. Zielsetzung für die Veröffentlichung der Guidelines ist es, gemäß Artikel 16 Abs. 3 EBA-Verordnung den Recommendations eine unmittelbare Bindungswirkung für die zuständigen Behörden der Mitgliedsstaaten sowie der Finanzinstitute im Sinne der EBA-Verordnung herzustellen.

4. Die zuständigen Behörden, im Fall von Deutschland die Bundesanstalt für Finanzdienstleistungsaufsicht (**BaFin**), haben danach alle erforderlichen Anstrengungen zu unternehmen, um diesen Leitlinien nachzukommen. Bezogen auf die Guidelines müssen die zuständigen Behörden der Mitgliedsstaaten bis 5. Mai 2015 gegenüber der EBA mitteilen, wie sie diesen Leitlinien nachzukommen beabsichtigen oder alternativ die Gründe dafür offenzulegen, warum sie der Umsetzung der Leitlinien nicht nachkommen. Wir verstehen die Durchführung der Konsultation als einen Schritt der BaFin zur Umsetzung der Leitlinien und damit zur Erfüllung der ihr obliegenden Verpflichtung. Nach dem vorliegenden Entwurf des Rundschreibens zu den Mindestanforderungen an die Sicherheit von Internetzahlungen sollen konsequenterweise die in Deutschland ansässigen Zahlungsdienstleister im Sinne des § 1 Abs. 1 Zahlungsdiensteaufsichts-gesetz (**ZAG**) den Mindestanforderungen unterworfen werden.

5. Gleichwohl zeichnet sich jedoch ab, dass zuständige Behörden anderer Mitgliedsstaaten eine mit der Initiative der BaFin gleichlaufende Umsetzung dieser Guidelines aktuell nicht vorhaben. Die Idee einer europaweit einheitlichen Regelung ist es, im Rahmen des EU-Binnenmarktes ein "level playing field" zu schaffen, in dem ein Zahlungsdienstleister in einem Mitgliedsstaat der Europäischen Union (**EU**) die gleichen Rechte und Pflichten hat und in gleicher Weise beaufsichtigt wird, wie ein Zahlungsdienstleister in einem anderen Mitgliedsstaat. Der BVZI befürchtet, dass dieses "level playing field" in Deutschland durch die frühzeitige Verabschiedung des vorliegenden Entwurfs des Rundschreibens nicht erreicht wird, wenn die BaFin ihre Ermessensspielräume hinsichtlich Kontrollzeitpunkten, Kontrollschärfe und Sanktionen unterschiedlich anwendet als andere zuständige Behörden innerhalb der EU und es damit zu einer Wettbewerbsverzerrung innerhalb des EU-Binnenmarktes kommen könnte. Die divergierende Umsetzung in den Mitgliedsstaaten birgt das Risiko, dass die jeweiligen E-Händler, welche die Zahlungsmethoden auf ihrer Internetseite im Verhältnis zu den zu schützenden Kunden anbieten, gezielt solche grenzüberschreitend tätigen Zahlungsdienstleister nutzen, die diesen Mindestanforderungen nicht unterliegen und deshalb die Zahlungsdienste kostengünstiger anbieten können und dabei gleichzeitig in Kauf nehmen, dass das gewünschte Schutzinteresse aufgrund der eingesetzten schwächeren Sicherheitsverfahren nicht erreicht wird. Im Hinblick auf global operierende E-Händler birgt ein deutscher Alleingang das Risiko, dass die betroffenen

Zahlungsdienste von Deutschland in das europäische Ausland verlagert werden. Außerdem wird die Integrität des Deutschen Finanzmarktes in Bezug auf den Zahlungsverkehr dahingehend beeinträchtigt, dass die unter der Aufsicht der BaFin stehenden Zahlungsdienstleister nur im begrenzten Umfang am betreffenden Zahlungsverkehr beteiligt sind und die BaFin insoweit unter Beachtung der EU-Pass-Regelungen bezüglich der Wahrnehmung ihrer eigenen Aufgaben eingeschränkt wird.

6. Daneben sind die Verhandlungen über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2013/36/EU und 2009/110/EG sowie zur Aufhebung der Richtlinie 2007/64/EG (**2. Zahlungsdiensterichtlinie**) zu berücksichtigen, die noch im ersten Halbjahr 2015 abgeschlossen werden sollen und die eine weitergehende Harmonisierung von Zahlungsdiensten in Europa mit sich bringen wird. Wir haben durch entsprechenden Hinweis im Anschreiben der BaFin zur Konsultation 02/2015 verstanden, dass auch die BaFin diesen Gesetzgebungsprozess im Rahmen der Konsultation zum Entwurf des vorliegenden Rundschreibens beachten will. Vor diesem Hintergrund sind Regelungen auf nationaler Ebene, die nicht im vollen Umfang mit den Regelungen der 2. Zahlungsdiensterichtlinie im Gleichklang sind, zu vermeiden und konsequenterweise der Ausgang des Gesetzgebungsverfahrens zur 2. Zahlungsdiensterichtlinie abzuwarten. Es besteht anderenfalls die Gefahr, dass mit einer zu frühen Umsetzung der Guidelines auf nationaler Ebene Mindestanforderungen festgelegt werden, die gegebenenfalls im Widerspruch zu der 2. Zahlungsdiensterichtlinie und ihrer Umsetzung ins nationale Recht stehen könnten. Diese Bedenken wurden bereits von zahlreichen Interessengruppen (z.B. EPSM Stellungnahme vom 14. November 2014) im Rahmen der Stellungnahme zur Konsultation der Guidelines vorgetragen, weshalb inhaltlich hierauf verwiesen wird.

7. Ein weiterer Aspekt zum Thema "level playing field" ist, dass sowohl die Recommendations (Seite 2) als auch die Guidelines (Titel I – Tz 11) einen negativen Anwendungsbereich beinhalten, der sich im Entwurf des Rundschreibens nicht wiederfindet. Im Gegenteil soll der darin explizit ausgenommene Bereich von Zahlungen, über telefonische Bestellung, in Deutschland in die Regulierung über den Begriff des Telefonbanking aufgenommen werden. Diese Erweiterung des Anwendungsbereichs sowie die Nichtaufnahme des Negativ-Katalogs der Recommendations sowie der Guidelines führt gerade nicht zu einem "level playing field", der jedoch aus Sicht des BVZI anzustreben ist.

Vorschlag des BVZI

8. Deshalb schlagen wir vor, die Umsetzung der Guidelines im Wege eines Rundschreibens in jedem Fall bis zur gesetzgeberischen Umsetzung der 2. Zahlungsverkehrsrichtlinie in Deutschland auszusetzen. Für die Meldung nach § 16 Abs. 3 EBA schlagen wir vor, die vorstehenden Aspekte als wesentliche Gründe dafür anzugeben, warum die Guidelines, zumindest zum gegenwärtigen Zeitpunkt nicht wie gefordert bis zum 1. August 2015 und auch nicht vor Inkrafttreten einer nationalen Gesetzgebung zur Umsetzung der 2. Zahlungsdiensterichtlinie umgesetzt werden können. In diesem Kontext haben wir auch die Ausführungen der BaFin vom 2. Juni 2014 unter dem Titel "Zahlungsdiensterichtlinie II: Risiken und schwerwiegende Folgen für Nutzer und Kreditinstitute" verstanden.

9. Soweit dennoch ein Rundschreiben erlassen wird, schlägt der BVZI konkret vor, den Entwurf des Rundschreibens insoweit zu kürzen, als dass darin keine weitergehenden

oder anderslautenden Regelungen enthalten sind als in den Guidelines. Das kann redaktionell dadurch erreicht werden, dass lediglich auf den Wortlaut der Guidelines verwiesen wird und dieser für Zahlungsdienstleister, soweit sie davon vom sachlichen Anwendungsbereich betroffen wären, verbindlich einzuhalten sind, um ein "level playing field" sicherzustellen. Insoweit wird auf die von der EBA in deutscher Sprache veröffentlichten Guidelines hingewiesen:

https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_DE+Guidelines+on+Internet+Payments.pdf/eff847ff-f1ed-4589-8efc-900cd78e2707

10. Unabhängig davon nehmen wir als BVZI nachfolgend zu den einzelnen Aspekten des Entwurfs des Rundschreibens hilfsweise wie folgt Stellung.

Konkrete Anmerkungen zu den einzelnen Regelungen im Entwurf des Rundschreibens

Kapitel 1. Anwendungsbereich

11. In Tz 2 wird der sachliche und persönliche Anwendungsbereich des Rundschreibens festgelegt. Der Anwendungsbereich ist unseres Erachtens an die Vorgaben der Guidelines anzupassen.

Persönlicher Anwendungsbereich

12. Die Guidelines richten sich gemäß Titel I – Tz. 3 ausschließlich an die "Finanzinstitute", die in Artikel 4 Abs. 1 EBA-Verordnung definiert werden. Dabei handelt es sich um folgende Finanzinstitute:

    (a) Kreditinstitute im Sinne von Artikel 4 Abs. 1 der Richtlinie 2006/48/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 über die Aufnahme und die Ausübung der Tätigkeit der Kreditinstitute (**Bankenrichtlinie**) ;

    (b) Wertpapierfirmen im Sinne von Artikel 3 Abs. 1 Buchstabe b der Richtlinie 2006/49/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 über die angemessene Eigenkapitalausstattung von Wertpapierfirmen und Kreditinstituten (**Kapitaladäquanzrichtlinie**) und

    (c) Finanzkonglomerate im Sinne von Artikel 2 Abs. 14 der Richtlinie des Europäischen Parlaments und des Rates vom 16. Dezember 2002 über die zusätzliche Beaufsichtigung der Kreditinstitute, Versicherungsunternehmen und Wertpapierfirmen eines Finanzkonglomerats und zur Änderung der Richtlinien 73/239/EWG, 79/267/EWG, 92/49/EWG, 93/6/EWG und 93/22/EWG des Rates und der Richtlinien 98/78/EG und 2000/12/EG des Europäischen Parlaments und des Rates.

13. Artikel 4 Abs. 1 Bankenrichtlinie in der ursprünglichen Fassung vom 14. Juni 2006 enthält folgende Definition des Begriffs Kreditinstituts:

    (a) ein Unternehmen, dessen Tätigkeit darin besteht, Einlagen oder andere rückzahlbare Gelder des Publikums entgegenzunehmen und Kredite für eigene Rechnung zu gewähren, oder

    (b) ein E-Geld-Institut im Sinne der Richtlinie 2000/46/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über die Aufnahme,

Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (**1. E-Geld-Richtlinie**).

14. Zum Zeitpunkt der Verabschiedung der EBA-Verordnung am 24. November 2010 war die 1. E-Geld-Richtlinie bereits durch die Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Institute, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG (**2. E-Geld-Richtlinie**) ersetzt worden. Durch Artikel 20 der 2. E-Geld-Richtlinie wurde Artikel 4 Abs. 1 Bankenrichtlinie geändert. Deshalb wird in Artikel 4 Abs. 1 EBA-Verordnung lediglich auf Kreditinstitute verwiesen. Nicht Gegenstand des Verweises sind damit jedoch die E-Geld-Institute.

15. Der Verweis auf Wertpapierfirmen im Sinne von Artikel 3 Abs. 1 Buchstabe b) Kapitaladäquanzrichtlinie stellt ebenfalls auf Kreditinstitute ab. Außerdem sind weitere Unternehmen Gegenstand der Regelung, die jedoch keine Zahlungsdienste erbringen dürfen. Das Gleiche gilt für Finanzkonglomerate, so dass insoweit der Verweis keine praktischen Auswirkungen auf Institute im Sinne von § 1 Abs. 2a ZAG haben dürfte.

16. Im Ergebnis richten sich deshalb die Guidelines der EBA lediglich an Kreditinstitute und nicht an E-Geld-Institute oder Zahlungsinstitute. Dieses Ergebnis wird durch Titel I – Tz. 11 (negativer Anwendungsbereich) der Guidelines dadurch untermauert, dass die zentrale Aufgabe der Zahlungsinstitute in der Regel darin besteht, das Clearing und die Verrechnung von Zahlungsvorgängen sicherzustellen. Diese Dienstleistungen werden sowohl von den Recommendations (Seite 2) und den Guidelines (Titel I – Tz. 11) explizit von der Anwendung der Regelungen zur Sicherheit von Internetzahlungen ausgenommen. Selbst wenn man also hilfsweise auf die Fassung der Bankenrichtlinie in ihrer ursprünglichen Fassung abstellen wollte, beabsichtigt die EBA, durch die Aufnahme des negativen Anwendungsbereichs in Titel I – Tz. 11 der Guidelines keine Institute im Sinne von § 1 Abs. 2a ZAG zu erfassen, die lediglich das Clearing und die Verrechnung von Zahlungsvorgängen sicherstellen. Das muss aus Sicht des BVZI im Anwendungsbereich des Entwurfs des Rundschreibens konsequenterweise umgesetzt werden. Die Ausdehnung des Anwendungsbereiches des Rundscheibens auf alle Zahlungsdienstleister im Sinne von § 1 Abs. 1 ZAG, ohne solche Unternehmen auszunehmen, die lediglich das Clearing und die Verrechnung sicherstellen, würde den Anwendungsbereich in unzulässiger Weise erweitern und die ohnehin bereits im allgemeinen Teil dargestellte Wettbewerbsverzerrung zusätzlich verstärken und die betroffenen Zahlungsinstitute unverhältnismäßig belasten. Deshalb sollte klargestellt werden, dass sich der Entwurf des Rundschreibens lediglich an eine Teilmenge der Zahlungsdienstleister richtet und die Institute im Sinne von § 1 Abs. 2a ZAG nicht erfasst werden, soweit sie lediglich das Clearing und die Verrechnung sicherstellen oder keine Zahlungsdienste erbringen, also die Institute, die in den sachlichen Anwendungsbereich der Guidelines und des Entwurfs des Rundschreibens fallen (siehe hierzu die nachstehenden Ausführungen).

Sachlicher Anwendungsbereich

17. Der Entwurf des Rundschreibens hat ferner einen klaren Produktbezug und erstreckt sich sachlich lediglich auf Zahlungsgeschäfte im Sinne von § 1 Abs. 2 Nr. 2 ZAG. Das Zahlungsgeschäft erfolgt ohne Kreditgewährung und erfasst die in der Praxis des Zahlungsverkehrs gängigen Verfahren der Kreditinstitute. Grundlage, dass überhaupt ein Zahlungsgeschäft erbracht werden kann, ist die Führung von Konten, wobei der Anbieter

des Zahlungsdienstes personenidentisch mit dem kontoführenden Institut sein muss (vgl. Findeisen in Ellenberger/Findeisen/Nobbe (Hrsg.), Kommentar zum Zahlungsverkehrsrecht, 2. Auflage 2013, § 1 ZAG, Rdnr. 180). In diesem Zusammenhang werden Institute im Sinne von § 1 Abs. 2a ZAG regelmäßig im Rahmen des Clearing und der Verrechnung tätig, indem sie die erforderliche technische Infrastruktur bereitstellen. Sie führen insoweit gerade nicht zahlungsverkehrsfähige Konten und betreiben gerade keine Internet-Zahlungsdienste. Der sachliche Anwendungsbereich folgt demnach dem persönlichen Anwendungsbereich, der sich wie zuvor dargestellt, auf Kreditinstitute beschränkt.

18. Im Entwurf des Rundschreibens wird die Beschreibung "Massenzahlungsverkehr über das Internet" als Grundlage für die Definition des zentralen Begriffs "Internet-Zahlungsdienste" verwendet. Das Wort Massenzahlungsverkehr ist weder gesetzlich noch im Entwurf definiert und damit unbestimmt. Hilfsweise ist auch keine Bestimmung des Begriffs über die Heranziehung der Recommendations (Seite 1 f.) oder der Guidelines (Titel I – Tz. 7) möglich, die jeweils in ihrem Wortlaut identisch von Internetzahlungsdiensten sprechen. Ausgehend von der Absicht einer deckungsgleichen Umsetzung ist dementsprechend fraglich, mit welcher Absicht der Begriff "Massenzahlungsverkehr" verwendet wurde. Wir verstehen den Begriff dahingehend, dass damit lediglich solche Internet-Zahlungsdienste erfasst werden sollen, die Kunden auf der Grundlage von zahlungsverkehrsfähigen Konten die Beauftragung von SEPA Überweisungen und Lastschriften über entsprechende Internetplattformen mit Webbrowser ermöglichen. Ausgenommen sind deshalb insbesondere die Treuhandkonten der abrechnenden Zahlungsdienstleister, auf denen sie die Gelder ihrer Händler sammeln und periodisch auszahlen.

19. Wesentlich für die Bestimmung des sachlichen Anwendungsbereichs ist unseres Erachtens auch, dass nach Titel I – Tz. 7 Erster Spiegelstrich der Guidelines ausschließlich "die Ausführung von Kartenzahlungen im Internet einschließlich virtueller Kartenzahlungen sowie die Registrierung von Kartenzahlungsdaten zur Nutzung in "elektronischen Geldbörsen"" erfasst werden sollen. Die Ausgabe von einzelnen Kartenprodukten soll davon jedoch gerade nicht erfasst werden, was im Entwurf des Rundschreibens durch den Verweis auf § 1 Abs. 2 Nr. 2 Buchstabe c) ZAG richtigerweise umgesetzt wurde. Im Zusammenhang mit dem Begriff des Massenzahlungsverkehrs schlagen wir insoweit zur Klarstellung des Anwendungsbereichs vor, die Ausgabe von Karten ausdrücklich auszunehmen, weil solche Kartenausgaben in der Regel gerade nicht massenzahlungsverkehrsrelevant sind, sondern regelmäßig in den Genuss einer Ausnahme nach § 7a ZAG kommen würden. Deshalb bitten wir um entsprechende Klarstellung des Begriffs "Massenzahlungsverkehrs" wie nachstehend in Ziffer 26 vorgeschlagen.

Begriffsbestimmung

20. Der BVZI empfiehlt in Anlehnung an die Titel I – Tz. 12 der Guidelines sowie dem auf Seite 15 der Recommendations enthaltenen Glossar eine Regelung in den Entwurf des Rundschreibens aufzunehmen, in denen die im Rundschreiben verwendeten wesentlichen Begriffe definiert werden.

21. Ein solcher Abschnitt ist deshalb angezeigt, weil verwendete Begriffe im Entwurf des Rundschreibens zu Missverständnissen führen können. Das gilt vor allem für den Begriff des sogenannten "Acquirers", weil dieser ohne weitere Definition im Entwurf des Rundschreibens verwendet wird. Der gesetzlich nicht definierte Begriff wird nach dem

Verständnis des deutschen Gesetzgebers für die Unternehmen verwendet, die das Zahlungsauthentifizierungsgeschäft betreiben, die jedoch ausdrücklich von Tz 2 des Entwurfs ausgenommen werden. In der Gesetzesbegründung (BT-Drucks. 16/11613, S. 34) heißt es hierzu:

> *"Unter dieses Gesetz wird dagegen, zwar nicht unter Nummer 2 oder 3, aber unter Nummer 4 das Unternehmen fallen, […] dasjenige Unternehmen, welches die erforderlichen Verträge mit den die Karte als Zahlungsmittel annehmenden Unternehmen oder E-Händlern schließt (das sog. akquirierende Institut oder auch Acquirer), auch wenn es jeweils die tatsächliche Verarbeitung, was bislang in der Regel so ist, an einen sog. […] Acquiring Processor auslagert."*

22. Ausweislich des Anwendungsbereiches in Tz 2 des Entwurfs des Rundschreibens sowie nach Titel I – Tz. 7 Erster Spiegelstrich der Guidelines fallen die das Zahlungsauthentifizierungsgeschäft betreibenden Unternehmen jedoch gerade nicht in den Anwendungsbereich der Leitlinien zur Sicherheit von Internetzahlungen, sondern lediglich die Ausführungen von Zahlungsvorgängen mittels Karte. Die Verwendung des Begriffs "Acquirers" ist vor diesem Hintergrund irreführend. Im Übrigen wird sowohl in den Recommendations (Seite 2) als auch in den Guidelines (Titel I – Tz. 10) eine eigenständige Definition des "payment integrators" verwendet. Zu dieser Gruppe von "Anbietern von Integrationslösungen für Bezahlseiten" (Titel I – Tz. 10 der deutschen Fassung der Guidelines) gehören sowohl die abrechnenden Zahlungsdienstleister als auch die externen technischen Dienstleister der betreffenden Schemes oder Zahlungsdienstleister. Zur Vermeidung von Missverständnissen sollte deshalb der derzeitig verwendete Begriff "Acquirer" insgesamt durch den Begriff "abrechnende Zahlungsdienstleister" ersetzt werden. Dabei ist klarzustellen, dass unter diesen Begriff nicht auch die externen technischen Dienstleister fallen, da diese lediglich vertraglich von den sie einbeziehenden Zahlungsdienstleistern zur Einhaltung des Rundschreibens verpflichtet werden sollen.

23. Unter Berücksichtigung der angestrebten deckungsgleichen Umsetzung der Vorgaben aus den Recommendations und den Guidelines ergibt sich unserem Verständnis nach zweierlei für das Rundschreiben:

    (a) Zum einen würden über den in Tz 2 des Entwurfs des Rundschreibens definierten Anwendungsbereich hinaus weitere Personen durch das Rundschreiben verpflichtet, die im Anwendungsbereich jedoch nicht ausdrücklich erfasst werden.

    (b) Zum anderen kann nicht ausgeschlossen werden, dass auch Unternehmen verpflichtet werden, die nicht der Regulierung der BaFin (zum Beispiel technische Dienstleister, die nicht in den Besitz von Kundengeldern kommen) unterliegen. In Bezug auf diese Unternehmen fehlt es an einer gesetzlichen Grundlage für dieses Vorgehen.

24. Daneben werden im Entwurf des Rundschreibens weitere gesetzlich unbestimmte Begriffe verwendet, ohne dass nachvollziehbar definiert wird, wie diese Begriffe zu verstehen sind. Im Sinne der Rechtssicherheit bei der Anwendung sowie der Umsetzung des Rundschreibens und der Erzielung des oben dargestellten "level playing fields" auf europäischer Ebene erachten wir die Aufnahme von entsprechenden Begriffsdefinitionen als erforderlich. Diesbezüglich könnte auf die Begriffsdefinitionen der Recommendations (Seite 2, Glossar auf Seite 15) sowie der Guidelines (Titel I – Tz. 12) zurückgegriffen werden. Abgesehen davon ergeben sich aus einem unmittelbaren Vergleich des Rundschreibens im Verhältnis zu den zugrundeliegenden Dokumenten weitere Fragen

hinsichtlich einer unterschiedlichen Anwendung von Begriffen. Exemplarisch wird auf den wesentlichen Regelungsgegenstand "Starke Kundenauthentifizierung" im Sinne von Titel I – Tz. 12 der Guidelines im Verhältnis zu "Starke Kundenauthentisierung" im Sinne von Tz 42 des Entwurfs des Rundschreibens eingegangen.

25. In der englischen Sprache gibt es lediglich das Wort "authentication". In der deutschen Sprache hingegen gibt es sowohl die "Authentisierung" als auch die "Authentifizierung". Beide Begriffe unterliegen einer gemeinsamen Abhängigkeit jedoch sind sie nicht deckungsgleich, weshalb entscheidend auf den Betrachtungsstandpunkt abgestellt werden muss. Die Authentifizierung folgt der Authentisierung. Für die zu betrachtenden Zahlungsdienste bedeutet das:

    (a) Authentisierung: Der Kunde belegt seine Identität und welche Rechte er hat indem er sich authentisiert. Der Kunde handelt aktiv. Der Begriff erfasst die Sicht der Person die überprüft wird. Das heißt, der Kunde authentisiert sich zum Beispiel durch die Eingabe seiner Kartennummer (Besitz) und seiner PIN (Wissen).

    (b) Authentifizierung: Der Zahlungsdienstleister überprüft die vom Kunden erhaltenen Daten und authentifiziert den Kunden dadurch. Der Zahlungsdienstleister handelt passiv. Der Begriff erfasst die Sicht der Person, die die Überprüfung vornimmt. Das heißt, der Zahlungsdienstleister authentifiziert den Kunden zum Beispiel auf Basis der erhaltenden Kartennummer (Besitz) und der PIN (Wissen) als die berechtigte Person.

26. Unter Berücksichtigung der vorstehenden Ausführungen sollte die Verwendung der Begriffe im Entwurf des Rundschreibens an die Vorgaben der Recommendations und den Guidelines angepasst werden. Das Rundschreiben sollte den Empfängerhorizont als Maßstab anlegen und folglich aus Sicht der Personen verfasst werden, die in den Anwendungsbereich fallen. Dementsprechend sollte im gesamten Entwurf lediglich der Begriff der "Authentifizierung" verwendet werden. Die derzeitige Wortwahl hätte den Effekt, dass der Nutzer der jeweiligen Zahlungsdienste den Zahlungsdiensteanbieter authentifizieren muss, weil sich der Zahlungsdiensteanbieter ihm gegenüber authentisiert. Diese Vorgehensweise ist jedoch nicht gemeint und wäre in der Praxis auch nicht umsetzbar.

Vorschlag des BVZI

27. Unter der Annahme, dass E-Geld-Institute dennoch erfasst werden sollen, obgleich dies aus den vorgenannten Gründen im Hinblick auf die Anwendung des Artikels 4 Abs. 1 Bankenrichtlinie nach unserer Auffassung nicht der Fall ist, schlagen wir hilfsweise folgende alternative Formulierung vor:

> *"Das Rundschreiben ist auf alle Zahlungsdienstleister im Sinne des § 1 Abs. 1 Nr. 1 und 2 Zahlungsdiensteaufsichtsgesetz (ZAG) anwendbar, die Zahlungsgeschäfte i.S.d. § 1 Abs. 2 Nr. 2 ZAG im Massenzahlungsverkehr über* das Internet *tatsächlich im Rahmen ihres Geschäftsmodells anbieten (Internet-Zahlungsdienste). Soweit diese Zahlungsdienstleister lediglich das Clearing und die Verrechnung von Zahlungsvorgängen erbringen, fallen sie lediglich insoweit in den Anwendungsbereich des Rundschreibens, als dass sie explizit als "abrechnende Zahlungsdienstleister" in der jeweiligen Tz genannt und verpflichtet werden. Externe technische Dienstleister im Sinne von § 1 Abs. 10 Nr. 9 ZAG sind vom Anwendungsbereich des Rundschreibens ausgenommen.*

Das Kriterium des Massenzahlungsverkehrs liegt vor, wenn Kunden auf Internetplattformen zahlungsverkehrsfähige Konten zur Durchführung von SEPA Überweisungen und Lastschriften angeboten werden. Ausgenommen hiervon ist die Ausgabe von Kartenprodukten."

28. Unter Berücksichtigung dieses Vorschlags geht der BVZI lediglich hilfsweise davon aus, dass sich die Regelungen in ihrer Gesamtheit auf die Institute im Sinne von § 1 Abs. 2a ZAG erstrecken, weil der vorliegende Entwurf des Rundschreiben den Begriff des Zahlungsdienstleisters noch nicht in der von uns vorgeschlagenen Art und Weise einschränkt.

Kapitel 2.1 Regelungen und Verantwortlichkeiten

Tz 4 – "Verantwortliche Führungskräfte"

29. Das Rundschreiben legt die Verpflichtung fest, dass die Sicherheitsrichtlinien von den "verantwortlichen Führungskräften" abzunehmen sind. Der Begriff der "Führungskraft" ist gesetzlich nicht geregelt. Ausgehend von der Wortwahl gehen wir davon aus, dass es sich dabei um Mitarbeiter unterhalb der Ebene der Geschäftsleiter handelt und die Zuständigkeit innerhalb des Zahlungsdienstleisters entsprechend delegiert wurde. Wir bitten um Bestätigung dieser Interpretation insbesondere vor dem Hintergrund, dass sowohl die Recommendations als auch die Guidelines, die Abnahme durch die Geschäftsleitung ("senior management") fordern.

30. In gleicher Weise bitten wir um Klarstellung bezüglich folgender Begriffe:

    (a) Tz 13 – "zuständigen Führungskräften"

    (b) Tz 15 – "Management"

Tz 6 – "Risikomanagement-Funktion"

31. Zahlungsinstitute haben aktuell sehr unterschiedliche Maßnahmen zur Abwehr von betrügerischen Handlungen sowie der damit einhergehenden operativen Risiken getroffen. Damit kommen Institute im Sinne von § 1 Abs. 2a ZAG bereits heute ihren eigenen geschäftsstrategischen Interessen nach, die Sicherheit der eingesetzten Technologien für die Durchführung des Zahlungsverkehrs zum Schutz der vertraglich gebundenen Akzeptanzstellen (E-Händler) und ihrer Kunden zu gewährleisten.

32. Soweit das Rundschreiben auf Zahlungsdienstleister in Form von Kreditinstituten abstellt, verstehen wir das Erfordernis einer "zuständigen Risikomanagement-Funktion" in Übereinstimmung mit § 25a Abs. 1 Satz 3 Nr. 3 Buchstabe c) KWG, wonach eine "Risikocontrolling-Funktion" gesetzlich gefordert ist. Das gesetzliche Erfordernis für eine Risikocontrolling-Funktion wurde mit dem CRD IV-Umsetzungsgesetz in dieser Form erstmalig verbindlich zur Umsetzung der nach Artikel 76 Abs, 5 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (**CRD IV-Richtlinie**) geforderten "risk management function" im KWG aufgenommen (BT-Drucks. 17/10974, S. 85). Der Begriff der "risk management function" aus der CRD IV-Richtlinie wird zumindest vom Wortlaut her auch in den Recommendations und den Guidelines verwendet. Sollte dieses

Erfordernis in gleicher Form auf Zahlungsinstitute übertragen werden, würde es derzeit an einer gesetzlichen Ermächtigung fehlen.

33. Die Regelung des § 22 Abs. 1 Satz 3 Nr. 4 ZAG ist zwar einer früheren Fassung des § 25a KWG nachgebildet, jedoch ist der Fokus auf die Verhinderung von Geldwäsche und Terrorismusfinanzierung gelegt, weshalb die von Instituten im Sinne von § 1 Abs. 2a ZAG verlangten Kontrollmechanismen und Verfahren zur Einhaltung des Geldwäschegesetzes und der Beachtung der dafür einschlägigen Verordnung (EG) Nr. 1781/2006 vom 15. November 2006 dienen sollen (BT-Drucks. 16/11613, S. 53). Der Gesetzgeber hat hiermit seine Intention zum Ausdruck gebracht, wonach ein aufsichtsrechtlich gefordertes "angemessenes Risikomanagement" bei Instituten nach § 1 Abs. 2a ZAG auf diesen Geldwäschebereich ausgerichtet sein soll. Der Regelungsgehalt des § 22 Abs. 1 Satz 3 Nr. 4 ZAG ist dementsprechend nicht gleichlaufend mit dem Erfordernis zur Errichtung einer Risikocontrolling-Funktion gemäß § 25a Abs. 1 Satz 3 Nr. 3 Buchstabe c) KWG.

34. Ferner wird ergänzend darauf hingewiesen, dass die Regelungen in Bezug auf "sonstige strafbare Handlungen" gemäß § 25h KWG nicht auf nach dem ZAG zugelassene Institute anwendbar sind. Im Rahmen der derzeitig verhandelten 2. Zahlungsdiensterichtlinie könnte sich eine entsprechende Erweiterung der Anforderungen ergeben, derzeit sind diese jedoch nicht verabschiedet und deshalb auch nicht europaweit in den nationalen gesetzlichen Regelungen implementiert worden.

Vorschlag des BVZI

35. Zunächst ist im Rundschreiben darzulegen, was nach Auffassung der BaFin eine "Risikomanagement-Funktion" ist, weil derzeitig gesetzlich nur der Begriff der "Risikocontrolling-Funktion" definiert ist. Alternativ wird die Anpassung des Begriffs "Risikomanagement-Funktion" in "Risikocontrolling-Funktion" vorgeschlagen. Es sollte ferner eine Klarstellung dahingehend erfolgen, dass die Notwendigkeit einer Risikomanagement-Funktion in der im Rundschreiben geforderten Ausprägung nicht auf Institute im Sinne von § 1 Abs. 2a ZAG anwendbar ist. Vor dem Hintergrund, dass die Risikocontrolling-Funktion von Instituten im Sinne von § 1 Abs. 2a ZAG gegebenenfalls erst mit Umsetzung der Anforderungen der 2. Zahlungsdiensterichtlinie im ZAG erfüllt werden müssen, sind diese Institute insoweit von den Anforderungen ausdrücklich auszunehmen und ggf. erst zu einem späteren Zeitpunkt durch eine Überarbeitung des Rundschreibens im angemessenen Umfang aufzunehmen, soweit dies im Hinblick auf die vorgeschlagenen Änderungen des Anwendungsbereichs dieses Entwurfs eines Rundschreibens überhaupt erforderlich wäre.

Tz 6 – "Sensible Zahlungsdaten"

36. Der an dieser Stelle erstmals verwendete Begriff der "sensiblen Zahlungsdaten" nimmt im Rundschreiben eine zentrale Bedeutung ein. Deshalb sollte die Begriffsbestimmung im Rundschreiben selbst erfolgen und nicht nur in den hilfsweise enthaltenen Erläuterungen. Es wird deshalb vorgeschlagen, die derzeitig als kursive Erläuterung enthaltende Begriffsbestimmung in die Tz 6 oder im Rahmen des von uns vorgeschlagenen Definitionsabschnitts zu Beginn des Entwurfs des Rundschreibens aufzunehmen.

Kapitel 2.2 Risikoanalyse

Tz 7 – Tz 13

37. Im Rahmen der Erläuterung zur Tz 7 wird ausgeführt, dass eine Schutzbedarfsanalyse nach den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (**BSI**) erwartet wird. Hieraus ergibt sich die Notwendigkeit zur Anwendung und Umsetzung des "BSI-Standards 100-3: Risikoanalyse auf der Basis von IT-Grundschutz". Bevor überhaupt eine solche Risikoanalyse nach diesem Standard durchgeführt werden kann, müsste als Basis der "BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise" vom Institut umgesetzt sein. Auf Ebene der Kreditinstitute ist bezüglich der "technisch-organisatorischen Ausstattung" im Sinne von § 25a Abs. 1 Satz 2 Nr. 4 KWG spätestens seit der ersten Veröffentlichung von AT 7.2 Tz 2 MaRisk vom 20. Dezember 2005 sowie der diesbezüglichen Erläuterungen die Erwartung der BaFin dahingehend klargestellt, dass die Standards des BSI beziehungsweise vergleichbare Standards unter Berücksichtigung des Proportionalitätsgrundsatzes gemeint sind. Wobei das damalige Bundesaufsichtsamt für das Kreditwesen erstmalig für das Jahr 2000 berichtet hat, dass die Kontakte zum BSI verstärkt wurden, um sicherheitstechnische Untersuchungen der Electronic-Banking-Plattformen verschiedener Kreditinstitute durchzuführen (Bundesamt für das Kreditwesen, Jahresbericht 2000, S. 10). Die Strukturen auf Seiten der Kreditinstitute sind also kontinuierlich gewachsen. Gleichwohl ergibt sich hieraus, dass selbst Kreditinstitute heute nicht verpflichtet sind, eine Risikoanalyse gemäß BSI-Standard 100-3 durchzuführen. An dieser Stelle sei ebenfalls darauf hingewiesen, dass die MaRisk keine wie auch immer geartete Ausstrahlungswirkung für Institute im Sinne von § 1 Abs. 2a ZAG entfaltet (vgl. hierzu Findeisen in: Ellenberger/Findeisen/Nobbe (Hrsg), Kommentar zum Zahlungsverkehrsrecht, 2. Auflage 2013, § 22 ZAG, RdNr. 19).

38. Eine zu § 25a Abs. 1 Satz 2 Nr. 4 KWG vergleichbare Regelung ist im ZAG nicht enthalten. Angemessene Verfahren und Datenverarbeitungssysteme werden lediglich im Hinblick auf die Einhaltung der Anforderungen des Geldwäschegesetzes gefordert. Im Übrigen müssen Zahlungsinstitute im Rahmen der Antragstellung nach § 8 Abs. 3 Nr. 2 ZAG und E-Geld-Institute gemäß § 8a Abs. 3 ZAG die eingesetzten Systeme, Ressourcen und Verfahren offenlegen. In diesem Kontext wurde seitens der BaFin kein Erfordernis nach den Vorgaben, wie im Entwurf des Rundschreibens, gestellt. Das mit diesem Entwurf des Rundschreibens gestellte Erfordernis geht deshalb über den gesetzlichen Rahmen hinaus, der von Instituten im Sinne von § 1 Abs. 2a ZAG zu erfüllen ist.

Vorschlag des BVZI

39. Vor diesem Hintergrund ist das in den Erläuterungen enthaltene Erfordernis zur Anwendung einer Schutzbedarfsanalyse nach Vorgaben des BSI ersatzlos zu streichen. Es ist zudem klarzustellen, dass die Tz 7 – Tz 13 nicht auf Institute im Sinne von § 1 Abs. 2a ZAG anwendbar ist, weil dieses Erfordernis unter Berücksichtigung der Ausführungen zum Anwendungsbereich weder in den Recommendations noch in den Guidelines verlangt wird. Sollte die BaFin dennoch einen Regelungsbedarf sehen, müssten zunächst die erforderlichen gesetzlichen Rahmenbedingungen für die Institute im Sinne vom § 1 Abs. 2a ZAG geschaffen werden.

40. Außerdem ist im Rundschreiben eine Klarstellung dahingehend wünschenswert, in welchem Umfang oder Verhältnis der von der Europäischen Zentralbank am 30. Januar 2014 herausgegebene Assessment Guide for the Security of Internet Payment anwendbar ist.

Kapitel 2.3 Überwachung und Berichtswesen zu IT-Sicherheitsvorfällen

Tz 15 – "Kritische IT-Sicherheitsfälle"

41. Im Rundschreiben wird insgesamt auf kritische IT-Sicherheitsfälle abgestellt, die eine Verletzung oder Beeinträchtigung der Verfügbarkeit, Integrität, Vertraulichkeit oder Authentizität von IT-Systemen, Anwendungen oder Daten mit hohen oder sehr hohen Schutzbedarf bedeuten. Aufgrund der Formulierung geht der Anwendungsbereich erheblich über die Regelungen der Recommendations (3 – 3.4) und der Guidelines (Titel I – Tz. 3 ff) hinaus. Beide Dokumente definieren den Begriff "major payment security event" und stellen dabei die Verknüpfung für die zur Durchführung der Zahlungsdienste eingesetzten IT-Ressourcen sowie den dabei verarbeiteten Zahlungsdaten her. Im Rahmen des Rundschreibens ist diese Einschränkung aufzunehmen, um in der weiteren Folge den Begriff der kritischen IT-Sicherheitsfälle auf diese IT-Ressourcen und Zahlungsdaten zu beschränken. Außerdem ist klarzustellen, dass die Meldeverpflichtung ausschließlich in Bezug auf die IT-Ressourcen und Zahlungsdaten vorzunehmen ist, die in der Hoheit und Verantwortung des Zahlungsdienstleisters sind.

42. Zusätzlich sind wir der Auffassung, dass das Erfordernis jede Verletzung oder Beeinträchtigung der insofern definierten IT-Ressourcen oder Zahlungsdaten mit hohen oder sehr hohen Schutzbedarf zu melden, unverhältnismäßig ist. Der Umstand, dass eine Verletzung oder Beeinträchtigung vorliegt, liefert für sich genommen noch keinerlei Aussage über die potentiellen oder sich ergebenden Auswirkungen. Es ist geübte Praxis und entspricht den Vorgaben des BSI-Grundschutzes sowie anderer vergleichbarer Standards, dass zusätzlich eine Einstufung vorzunehmen ist, wie kritisch der Vorfall zu beurteilen ist. Sowohl das BSI als auch das Computer Emergency Responce Team für Bundesbehörden (**CERT-Bund**) nehmen eine Bewertung der Kritikalität des Vorfalls auf Basis eines Ampelsystems vor. Es wird vorgeschlagen, lediglich solche kritischen IT-Sicherheitsvorfälle zu melden, die einem roten Ampelstatus entsprechen.

Tz 17 – "Kooperation mit zuständigen Strafverfolgungsbehörden"

43. Der BVZI geht davon aus, dass die Worte "Acquirer" und "Zahlungsdienstleistern" gegen "abrechnende Zahlungsdienstleister" (siehe Ziffer 22 dieses Schreibens) zu ersetzen sind, da der E-Händler im Rahmen der Abwicklung der Zahlung keine vertragliche Beziehung zu einem Kreditinstitut unterhält, mit dem er bei einem "kritischen IT-Sicherheitsvorfall" kooperieren könnte.

44. Wenn Tz 17 in dieser Form wirksam werden würde, müssten alle "abrechnenden Zahlungsdienstleister" sämtliche bestehenden Verträge mit allen E-Händlern anpassen. Dies erfordert eine Zustimmung des E-Händlers, ohne dass die Möglichkeit besteht, diese Zustimmung ohne Vorhandensein entsprechender vertraglicher Regelungen zur Änderungen von Verträgen aufgrund dieses Entwurfs des Rundschreibens herbeizuführen. Aus Sicht des BVZI ist insbesondere die einseitige Auferlegung der Durchsetzung der geforderten Standards für Internet-Zahlungsdienste gegenüber den E-Händlern durch die abrechnenden Zahlungsdienstleister unverhältnismäßig. Die Einbeziehung von E-Händlern würde vielmehr eine explizite gesetzliche Grundlage auf EU Ebene erfordern, damit ein "level playing field" sichergestellt und sich die abrechnenden Zahlungsdienstleister darauf berufen können. Solange dies nicht der Fall ist, sollte für den vorliegenden Entwurf des Rundschreibens jedenfalls die Verpflichtung nur auf Neuverträge erstreckt und die Formulierung wie folgt angepasst werden:

"~~Acquirer~~Abrechnende Zahlungsdienstleister haben bei Abschluss von neuen Akzeptanzverträgen vertraglich von E-Händlern, die sensible Zahlungsdaten speichern, verarbeiten oder übertragen, zu fordern, dass diese bei kritischen IT-Sicherheitsvorfällen eines E-Händlers sowohl mit den abrechnenden Zahlungsdienstleistern als auch mit den zuständigen Strafverfolgungsbehörden kooperieren."

Tz 18 – "Rechtsfolgen bei kritischen IT-Sicherheitsvorfällen"

45. Aus dem Rundschreiben geht nicht hervor, was "angemessene Schritte" sein könnten, die unter Berücksichtigung der geschlossenen Vertragsbeziehung und unter Beachtung der zivilrechtlichen Regelungen des Bürgerlichen Gesetzbuches im Verhältnis zu den E-Händlern angewendet werden könnten, ohne sich selbst vertragswidrig zu verhalten. In diesem Kontext erschließt sich aus dem Rundschreiben ebenfalls nicht, über welchen Zeitraum sich die angemessenen Schritte erstrecken dürfen bis ggf. eine Kündigung des Vertrages durchgeführt werden müsste. Hierbei ist ferner das Stufenverhältnis unklar, in welcher Relation die mangelnde oder nicht vorhandene Kooperation des E-Händlers zur tatsächlichen Kritikalität des festgestellten schwerwiegenden Zahlungssicherheitsvorfalls stehen darf, bevor die weiteren angemessenen Schritte einzuleiten sind. Deshalb könnte es nach den derzeitigen Regelungen im Entwurf erforderlich sein, einen Akzeptanzvertrag unmittelbar durch Kündigung zu beenden, ohne Ansehung des Umfangs, der ohne jede Verletzung oder Beeinträchtigung durchgeführten übrigen Zahlungsdienste. Dabei muss aus unserer Sicht vor allem berücksichtigt werden, dass die Kündigung und der Entzug der Möglichkeit zur Akzeptanz von Zahlungen im Internet erhebliche und auch existenzgefährdende Auswirkungen auf den betroffenen E-Händler haben können. Der E-Händler wird aufgrund des Eingriffes in den von ihm ausgeübten Gewerbebetrieb versuchen, sich im Verhältnis zum abrechnenden Zahlungsdienstleister schadlos zu halten.

46. Aus den vorstehenden Überlegungen erscheint es unseres Erachtens zielführend, dass die BaFin weitere Ausführungen im Entwurf des Rundschreibens dahingehend vornimmt, was angemessene Schritte sind. Das könnte durch einen nicht abschließenden Katalog von Maßnahmen erfolgen, die als Erläuterung aufgenommen werden. Ferner sind Ausführungen darüber geboten, in welchem Umfang diese Schritte unter Berücksichtigung der übrigen Zahlungsdienste im Verhältnis zum schwerwiegenden Zahlungssicherheitsvorfall vorgenommen werden müssen.

47. Ferner kann diese Regelung nur dann die gewünschte Wirkung entfalten, wenn sie zusätzlich durch eine korrespondierende Verpflichtung der gewerbetreibenden E-Händler in der Gewerbeordnung begleitet wird. Ohne eine solche gesetzliche Verpflichtung der E-Händler wird das Risiko von Schadensersatzansprüchen des E-Händlers gegen die abrechnende Stelle im Falle der Kündigung des Akzeptanzvertrages schlagend. Dieses operationelle Risiko ist nicht kalkulierbar und würde in der Folge dazu führen, dass die in Deutschland ansässigen abrechnenden Stellen keine Ressourcen für die Durchführung von Zahlungsdiensten im Internet im Verhältnis zu E-Händlern bereitstellen könnten. Die E-Händler würden in diesem Fall abrechnende Stellen einsetzen, die ihre Zahlungsdienste im Wege des grenzüberschreitenden Dienstleistungsverkehrs erbringen. Aus gleichem Grund empfehlen wir, dass der zuvor vorgeschlagene nicht abschließende Katalog von Maßnahmen auf europäischer Ebene abgestimmt und von den jeweils zuständigen Aufsichtsbehörden in gleicher Weise kommuniziert wird.

Kapitel 2.4 Risikokontrolle und -vermeidung

Tz 19 – "Verteidigung in der Tiefe"

48. Wir schlagen vor, in Übereinstimmung mit der üblichen IT-Sprachregelung den Begriff "Sicherheitskonzept" zu verwenden. Die Festlegung einer Auswahl von unterschiedlichen Sicherungsmaßnahmen ist integraler Bestandteil eines angemessenen Sicherheitskonzepts.

Tz 21 – "Zahlungsdienstleister"

49. Zur Vermeidung von Missverständnissen und unter Berücksichtigung der verschiedenen Personenkreise, die in dem Rundschreiben besprochen werden schlagen wir folgende Anpassung vor:

> *"Netzwerke, Webseiten, Server und Kommunikationsverbindungen der Zahlungsdienstleister, die in den Anwendungsbereich dieses Rundschreibens fallen, sind gegen Missbrauch oder Angriffe zu schützen.*

Tz 24 – "Zugang"

50. Im Rahmen der Informationssicherheit werden der Zutritt, Zugang und der Zugriff unterschieden. Das Rundschreiben spricht ausschließlich die nachvollziehbare Dokumentation des Zugangs an. Dies verstehen wir dahingehend, dass es bezüglich der anderen Aspekte kein zwingendes Dokumentationserfordernis gibt.

Tz 30 – "Externe"

51. Wir bitten um Klarstellung, ob der Begriff "Externe" im Sinne einer Auslagerung von dem Zahlungsdienstleister auf einen Dienstleister (Insourcer) gemeint ist. Ferner bitten wir um Information, ob nach dem Verständnis der BaFin in diesem Fall eine wesentliche Auslagerung gegeben ist.

Tz 31 – "Sicherheit der E-Händler"

52. Im Rahmen des Rundschreibens wird die Intention der Recommendations und der Guidelines verkürzt wiedergegeben. Es wird nicht berücksichtigt, dass die abrechnende Stelle den angeschlossenen E-Händler nur in dem Fall zur Implementierung von mit den Tz 20 – 30 verpflichten sollen, wenn die E-Händler selbst mit sensiblen Zahlungsdaten umgehen. Ein Umgang mit sensiblen Zahlungsdaten liegt lediglich dann vor, wenn der E-Händler die betreffenden Daten selbst speichert, verarbeitet oder übermittelt. Anders ist dies jedoch in dem Fall, wo der Kunde im Rahmen der Initiierung des Zahlungsvorgangs beim E-Händler auf eine Seite weitergeleitet wird, die in der Hoheit der abrechnenden Stelle oder des Zahlungsdienstleisters steht, ohne dass der E-Händler die Möglichkeit zur Speicherung, Verarbeitung oder Übermittlung der sensiblen Zahlungsdaten des Kunden hat. Derartige "White-Label-Frames" sind die gängige Praxis in einer Vielzahl von Anwendungsfällen, insbesondere dann, wenn es sich um kleinere E-Händler handelt, die selbst nicht über die erforderlichen IT-Ressourcen verfügen, um sichere Zahlungsdienste im Internet ablaufen zu lassen. Das Rundschreiben ist deshalb im Gleichklang mit den Recommendations und den Guidelines zu überarbeiten, wozu folgender Wortlaut vorgeschlagen wird:

> *"~~Acquirer~~Abrechnende Zahlungsdienstleister haben von ihren ~~Online~~E-Händlern, die mit sensiblen Zahlungsdaten umgehen und diese speichern, verarbeiten oder*

übermitteln, vertraglich zu verlangen, dass diese Sicherheitsmaßnahmen in ihrer IT-Infrastruktur implementieren, die den vorgenannten Anforderungen (Tzn 21 bis 30) genügen, um einen Diebstahl dieser sensiblen Zahlungsdaten über die IT-Infrastruktur des E-Händlers zu verhindern. Dies ist jedoch nicht erforderlich, wenn die E-Händler die sensiblen Zahlungsdaten nicht selbst speichern, verarbeiten oder übermitteln."

53. Daneben ist uns aufgefallen, dass die verwendete Terminologie nicht einheitlich im Rundschreiben verwendet wird. Es werden in den einzelnen Tz unterschiedliche Begriffe verwendet, obwohl offenbar das gleiche gemeint sein soll. In der Tz 31 wird der Begriff "IT-Infrastruktur" verwendet. Zuvor wurden daneben folgende Begriffe verwendet:

(a) IT-Komponenten – Erklärung zu Tz 7

(b) Infrastruktur – Tz 11

(c) IT-Systemem – Tz 15

(d) IT-Umgebung und IT-Systeme – TZ 20

(e) IT-Umgebung und Ressourcen – Erklärung zu Tz 20

(f) Netzwerke, Webseiten, Server und Kommunikationsverbindungen – Tz 21

(g) Server – Tz 22

(h) Logischen und physische kritischen Ressourcen – Tz 24

54. Auch in den nachfolgenden Tz des Rundschreibens werden verschiedene Begriffe für die durch das Rundschreiben erfassten "IT-Ressourcen" verwendet, ohne dass sich an den einzelnen Stellen erschließt, welchen Unterscheidungsgehalt diese Differenzierung haben soll. Diesbezüglich wird um Klarstellung gebeten und einheitliche Verwendung einer im Rundschreiben definierten Terminologie, die in dem von uns vorgeschlagenen Definitionsabschnitts zu Beginn des Entwurfs des Rundschreibens aufgenommen wird.

Kapitel 2.5 Nachvollziehbarkeit von Transaktionen und E-Mandaten

55. Den Begriff "E-Mandat" verstehen wir dahingehend, dass hiermit die Erteilung und Änderung eines elektronischen Mandats für eine SEPA Lastschrift gemeint ist (Guidelines Titel I – Tz. 7). Wir bitten diesbezüglich um Klarstellung.

Tz 32 – "Dienste"

56. Den Begriff "Dienste" verstehen wir als "Internet-Zahlungsdienst" wie in Tz 2 definiert. Wir bitten um Anpassung des Begriffs.

Kapitel 3. Besondere Anforderungen an die Steuerung und die Sicherheitsmaßnahmen für die Internet-Zahlungen

Kapitel 3.1 Initiale Kundenidentifikation und Information

Tz 36 – "Kundenidentifikation"

57. Der Begriff des Kunden ist unseres Erachtens dahingehend auszulegen, dass darunter lediglich der Vertragspartner des kontoführenden Zahlungsdienstleisters gemeint ist, der

für den Vertragspartner Internet-Zahlungsdienste anbietet. Vom Kundenbegriff sind insbesondere nicht E-Händler erfasst. Der BVZI schlägt deshalb vor, die folgende Klarstellung in Tz 36 aufzunehmen:

> *"Abrechnende Zahlungsdienstleister sind nicht zur Identifikation von Kunden verpflichtet. Sie sind lediglich verpflichtet, E-Händler als Vertragspartner zu identifizieren."*

58. Außerdem erscheint zur weiteren Klarstellung eine Anpassung der Tz 36 wie folgt erforderlich:

> *"Bevor ein Zahlungsdienstleister einem Kunden Zugang zu Internet-Zahlungsdiensten gewährt ~~wird~~, ist nachweisbar eine Willenserklärung einzuholen, dass der betroffene Kunde Internet-Zahlungsdienste in Anspruch nehmen will. Zudem ist durch den Zahlungsdienstleister vorab sicherzustellen, dass der Kunde die für die Identifizierung erforderlichen Verfahren durchlaufen hat und ausreichende Ausweispapiere und damit zusammenhängende Informationen vorgewiesen hat."*

Tz 37 – "Informationen"

59. In Übereinstimmung mit den Recommendations und den Guidelines ist klarzustellen, dass dies die Verpflichtung des Zahlungsdienstleisters und nicht des abrechnenden Zahlungsdienstleisters betrifft. Folgende Anpassung der Formulierung wird vorgeschlagen:

> *"Es ist durch den Zahlungsdienstleister sicherzustellen, dass die erforderlichen vorvertraglichen Informationen, die dem Kunden ausgehändigt werden, Details zum Internet-Zahlungsdienst enthalten."*

Tz 39 – "Sperrung von Transaktionen"

60. Der hier beschriebene Sachverhalt betrifft erneut das Verhältnis des Zahlungsdienstleisters zu seinem Kunden, wie in unserer Ziffer 57 dieser Stellungnahme definiert. Der abrechnende Zahlungsdienstleister ist auch in Übereinstimmung mit den Recommendations (6.3 KC) und den Guidelines (Titel II – Tz 6.3) nicht gemeint. Deshalb wird folgende Anpassung der Formulierung vorgeschlagen:

> *"Der Rahmenvertrag des Zahlungsdienstleisters mit dem Kunden legt im Einzelnen fest, dass der Zahlungsdienstleister eine spezifische Transaktion oder das Zahlungsinstrument auf der Basis von Sicherheitsbedenken sperren darf."*

Tz 40 – "Verfahren zur Benachrichtigung"

61. Folgerichtig ist auch diese Textziffer anzupassen und auf den Zahlungsdienstleister abzustellen:

> *"Der Rahmenvertrag des Zahlungsdienstleisters mit dem Kunden hat das Verfahren und die Bedingungen der Benachrichtigung des Kunden sowie die Art und Weise festzulegen, wie der Kunde den Zahlungsdienstleister kontaktieren kann, um eine Transaktion bzw. den ~~Service~~Internet-Zahlungsdienst wieder zu entsperren. Die Festlegungen sind im Einklang mit der Zahlungsdiensterichtlinie 2007/64/EG in der jeweils geltenden Fassung zu treffen."*

Tz 41 – "Fortlaufende Information"

62. Da auch hier der Kunde des kontoführenden Zahlungsdienstleisters gemeint ist, wird folgende Anpassung vorgeschlagen:

> *"Die Kunden sind durch den Zahlungsdienstleister fortlaufend und anlassbezogen über ihre Verantwortung hinsichtlich der sicheren Nutzung des ~~Dienstes~~Internet-Zahlungsdienstes zu informieren. Dazu sind geeignete Mittel, wie z.B. Broschüren oder Internetseiten, einzusetzen."*

Kapitel 3.2 Starke Kundenauthentisierung

63. Es wird auf die Darstellungen in Ziffer 26 dieser Stellungnahme verwiesen und um Änderung in "Kundenauthentifizierung" im gesamten Kapitel gebeten.

Tz 42 – "Eingesetztes Verfahren"

64. Unter Berücksichtigung der erforderlichen Abgrenzung zwischen dem Zahlungsdienstleister und dem abrechnenden Zahlungsdienstleister wird folgende Anpassung des Wortlauts vorgeschlagen:

> *"Für die Autorisierung von Internet-Zahlungen durch einen Kunden (inkl. Sammelüberweisungen) und für die Ausgabe oder Änderung von E-Mandaten ist vom Zahlungsdienstleister eine starke ~~Kundenauthentisierung~~ Kundenauthentifizierung einzusetzen."*

65. Der BVZI versteht, dass das Rundschreiben für einen längeren Zeitraum gilt und heute bestehende Methoden, die eine starke Kundenauthentifizierung unterstützen, in den Erläuterungen nicht aufgeführt sind. Allerdings sind abrechnende Zahlungsdienstleister nicht in der Lage, solche Verfahren zu entwickeln und gegenüber sämtlichen an Zahlungssystemen Beteiligten durchzusetzen. Dies liegt vielmehr in der Hand der jeweiligen Systembetreiber. Dennoch wären wir für einen Hinweis dankbar, welche derzeit verfügbaren Verfahren den Anforderungen an eine starke Kundenauthentifizierung gerecht werden. Nach unserer Einschätzung wird beispielsweise das von VISA entwickelte 3-D SECURE, das bei VISA unter dem Namen "Verified by VISA" und bei MasterCard unter dem Namen "MasterCard®SecureCode" eingesetzt wird, den Anforderungen gerecht, indem zusätzlich zur Karte entweder eine im Internet zu verwendende, gesonderte PIN-Nummer, herausgegeben wird oder eine sogenannte Online-Prüfung bei dem herausgebenden Kreditinstitut erfolgt. Wir bitten zur Klarstellung darum, diese Einschätzung zu bestätigen.

Tz 44 – "Zugriff auf sensible Zahlungsdaten"

66. Zur Wahrung der Konsistenz wird folgende Anpassung vorgeschlagen:

> *"Der Zugriff auf sensible Zahlungsdaten und die Änderung dieser Daten (inkl. Erzeugung und Änderung von White Lists) beim Zahlungsdienstleister erfordert starke ~~Authentisierung~~ Authentifizierung."*

Tz 45 – "Anpassung auf Basis der Risikoanalyse"

67. Die Tz 45 ist hinsichtlich der verwendeten Begriffe nicht konsistent. So wird im gesamten Rundschreiben auf den Begriff der "sensiblen Zahlungsdaten" abgestellt. Der Begriff der

"sensiblen Kundendaten" findet im übrigen Rundschreiben keine Verwendung und ist ferner nicht definiert. Der Begriff ist zu streichen und die Formulierung wie folgt zu fassen:

> *"Sofern ein Zahlungsdienstleister ausschließlich solche ~~Dienste~~ Zahlungsdienste anbietet, bei denen keine ~~Transaktionen~~ Internet-Zahlungsdienste ausgeführt werden und keine sensiblen ~~Kunden oder~~ Zahlungsdaten angezeigt werden, die leicht für betrügerische Zwecke verwendet werden könnten, kann ~~er~~ der Zahlungsdienstleister seine ~~Authentisierungsanforderungen~~ Authentifizierungsanforderungen auf Basis seiner Risikoanalyse entsprechend anpassen."*

Tz 47 – "Ausgegebene Karten"

68. In Übereinstimmung mit dem definierten Anwendungsbereich ist eine Abgrenzung erforderlich und der Wortlaut sollte wie folgt geändert werden:

> *"Alle von einem Zahlungsdienstleister für die Verwendung von Internet-Zahlungsdiensten ausgegebenen Karten müssen technisch dazu in der Lage sein, mit starker Authentisierung genutzt zu werden."*

Tz 48 und Tz 49 – "Abrechnender Zahlungsdienstleister"

69. Im Anschreiben zur Konsultation wurde mitgeteilt, dass das Rundschreiben mit dem Tag der Veröffentlichung in Kraft treten wird. Allerdings wird weiter in Aussicht gestellt, dass ein ausreichender Umsetzungszeitraum von sechs Monaten eingeräumt werden soll. Wir machen darauf aufmerksam, dass insbesondere die abrechnenden Zahlungsdienstleister in Abhängigkeit der Kartenorganisationen sowie der kartenausgebenden Zahlungsdienstleistern stehen. Erst wenn diese Unternehmen Verfahren entwickelt und getestet haben, können auch die abrechnenden Zahlungsdienstleister ihrerseits die technischen Voraussetzungen schaffen, dass die betreffenden Verfahren in der Praxis eingesetzt werden können. Sofern bereits Verfahren entwickelt und getestet sind, wie nach unserer Einschätzung zum Beispiel das vorgenannte 3-D Secure-Verfahren, müssen die kartenausgebenden Zahlungsdienstleister diese auch implementiert haben. Im Falle von 3-D-Secure kann damit eine Kundeninformation (z.B. Versenden von PIN-Briefen) verbunden sein. Gleiches gilt für äquivalente Verfahren in der Regel auch. Berücksichtigt man die jeweiligen Entwicklungs- und Testphasen sowie die jeweiligen Release-Zyklen bei allen involvierten Parteien und die Zeiträume für den Massenversand von Kundenanschreiben, dann ist für die Einführung eines solchen neuen Verfahrens mindestens ein Zeithorizont von 24 Monaten erforderlich. Folglich ist der vorgeschlagene Zeithorizont von 6 Monaten schon aus technischen Gründen nicht darstellbar.

70. Aufgrund der zuvor dargestellten Abhängigkeit von den Umsetzungsmaßnahmen der kartenherausgebenden Zahlungsinstitute sollte der Zeitpunkt festgelegt werden, wann ein Verfahren als einsatzbereit gilt. Diesbezüglich schlagen wir vor, dass ein Verfahren als „einsatzbereit" gilt, wenn es vom kartenausgebenden Zahlungsdienstleister und abrechnenden Zahlungsdienstleister technisch implementiert ist und die notwendigen Schnittstellen zu den kartenausgebenden Zahlungsdienstleistern etabliert sind, die das Verfahren anzuwenden beabsichtigen. Die Existenz und/oder faktische Nutzung der Karten durch den Kunden sind nicht entscheidend.

71. Hinsichtlich des E-Mandates weisen wir darauf hin, dass der European Payment Council (**EPC**) festgestellt hat, dass die rechtssichere Erteilung von SEPA Direct Debit (**SDD**) Mandaten noch nicht europaweit harmonisiert ist und sich in Abstimmung des Euro Retail

Payments Boards unter Vorsitz der Europäischen Zentralbank befindet. Die europaweite Festlegung wird im Laufe des Jahres 2015 erwartet. Danach schließen sich die notwendigen technischen Implementierungen an. Auch bei diesem Bezahlverfahren ist eine Umsetzung innerhalb von 6 Monaten technisch nicht darstellbar.

72. Daneben wird zusätzlich Bezug genommen auf die Ausführungen zur Bestimmung des Begriffs "abrechnender Zahlungsdienstleister" in den Ziffern 21 ff. und folgende Änderung der Formulierung vorgeschlagen:

> *"Tz 48*
>
> *~~Acquirer~~ Abrechnende Zahlungsdienstleister haben nach angemessener Implementierungsphase mindestens eine Technologie~~n~~ zu unterstützen, die es dem ~~Kartenausgeber~~ kartenausgebenden Zahlungsdienstleister erlauben, starke ~~Authentisierung~~ Kundenauthentifizierung des Kunden (Karteninhabers) ~~für~~ im Rahmen von Internet-Zahlungsdiensten ~~Kartenzahlungssysteme~~ durchzuführen, an denen der ~~Acquirer~~ abrechnende Zahlungsdienstleister teilnimmt. Die Implementierungsphase sollte 24 Monate nach Einführung einer solchen Technologie durch eine führende Kartenorganisation (z.B. Deutsche Kreditwirtschaft, Visa, MasterCard) oder Festlegungen durch das European Payment Council (im Falle von SEPA Direct Debit im Internet) nicht übersteigen.*
>
> *Tz 49*
>
> *~~Acquirer~~ Abrechnende Zahlungsdienstleister haben beim Abschluss von neuen Akzeptanzverträgen von ihren ~~Online-Händlern~~ E-Händlern zu fordern, mindestens eine Lösung~~en~~ zu unterstützen, die es dem ~~Kartenherausgeber~~ kartenausgebenden Zahlungsdienstleister erlauben, starke ~~Authentisierung~~ Kundenauthentifizierung des Kunden (Karteninhabers) für Kartentransaktionen ~~über das Internet~~ im Rahmen von Internet-Zahlungsdiensten durchzuführen."*

Tz 51 – "Haftung"

73. Die Verbindung zwischen den technischen Anforderungen und zivilrechtlicher Haftungsregelungen ist originäre Aufgabe des Gesetzgebers für die relevanten Vorschriften im Bürgerlichen Gesetzbuch. Da diese seit der 1. Zahlungsdiensterichtlinie im Wege der Vollharmonisierung auf EU Ebene vorgegeben werden, bedarf es zunächst einer entsprechenden EU Initiative.

74. Abgesehen davon lässt sich die Notwendigkeit für eine derartige Regelung weder aus den Recommendations noch aus den Guidelines erkennen. Deshalb ist unter Berücksichtigung des "level playing fields" eine Streichung dieser Regelung erforderlich.

Tz 52 und Tz 53 – "Wallet-Lösungen"

75. Mit dieser Formulierung werden zahlreiche neue Begriffe eingeführt, ohne dass diese im Vorfeld bestimmt wurden. Zum einen erschließt sich nicht ohne weiteres, um welche Person es sich bei dem "Anbieter von Wallet-Lösungen" handeln soll. Es ist das Verständnis des BVZI, dass ausschließlich Kreditinstitute und E-Geld-Institute, aufgrund der ihnen gegenüber erteilten Erlaubnis, berechtigt sind eine Wallet-Lösung anzubieten. Folglich würde es sich um die Zahlungsdienstleister im Sinne des Anwendungsbereichs dieses Rundschreibens handeln. Vor diesem Hintergrund ist entweder der Begriff des Zahlungsdienstleister zu verwenden oder eine Definition des Begriffs vorzunehmen.

76. Zum anderen ist nicht ersichtlich worin der Unterschied zwischen dem bisher verwendeten Begriff "Kunde" und dem nunmehr bezeichneten "legitimierten Karteninhaber" bestehen sollte. Allein unter Beachtung der geldwäscherechtlichen Regelungen müsste der Karteninhaber vom kartenausgebenden Zahlungsdienstleister vollständig identifiziert werden, womit er ebenfalls als Kunde anzusehen wäre.

77. Abschließend ist zu klären, worin der Unterschied zwischen einer "Wallet-Lösung" und einem "Wallet-Zahlungsdienst" besteht. Sofern die Begriffe synonym zu verstehen sind, wovon unsererseits ausgegangen wird, sollte auch nur ein Begriff verwendet werden, um unnötige Missverständnisse zu vermeiden. Der BVZI schlägt deshalb folgende Formulierung vor:

> *"Tz 52*
>
> *~~Für Kartenzahlungssysteme haben Anbieter von~~ Zahlungsdienstleister die ihren Kunden die Übertragung von E-Geld zwischen zwei E-Geld-Konten (Wallet-Lösungen) über das Internet anbieten, müssen ~~von den Kartenausgebern~~ starke ~~Authentisierung~~ Kundenauthentifizierung ~~zu~~ verlangen, wenn der ~~legitimierte Karteninhaber~~ Kunde die Kartendaten erstmalig registriert.*
>
> *Tz 53*
>
> *~~Anbieter von~~ Zahlungsdienstleister mit Wallet-Lösungen haben starke ~~Authentisierung~~ Kundenauthentifizierung für die Fälle zu unterstützen, wenn Kunden sich in ~~den Wallet-Zahlungsdienst~~ die Wallet-Lösung einloggen oder Kartentransaktionen über das Internet durchführen."*

Tz 55 und Tz 56 – "Virtuelle Karten"

78. Der Begriff der "virtuellen Karte" ist gesetzlich und auch in diesem Rundschreiben nicht definiert. Der Begriff sollte in Anlehnung an Titel I – Tz. 12 der Guidelines im Rundschreiben definiert werden.

Tz 57 – "Bilaterale Authentifizierung"

79. Der BVZI versteht das Erfordernis dahingehend, dass sowohl die Zahlungsdienstleister als auch die mehrheitlich in Vertragsbeziehung mit E-Händler stehenden abrechnenden Zahlungsdienstleister angesprochen sind. Die Formulierung sollte daher wie folgt gefasst werden:

> *"Während der Kommunikation der Zahlungsdienstleister oder soweit involviert der abrechnenden Zahlungsdienstleister mit ~~Online-Händlern~~ E-Händlern zum Zweck der Initiierung von ~~Internet-Zahlungen~~ Internet-Zahlungsdiensten und dem Zugriff auf sensible Zahlungsdaten ist ordnungsgemäße bilaterale ~~Authentisierung~~ Kundenauthentifizierung sicherzustellen."*

Kapitel 3.3 Registrierung und Ausgabe von Authentisierungswerkzeugen und/oder Software an Kunden

80. Es wird auf die Darstellungen in Ziffer 26 dieser Stellungnahme verwiesen und um Änderung in "Kundenauthentifizierung" im gesamten Kapitel gebeten.

Tz 58 bis Tz 64– "Zahlungsdienstleister / abrechnende Zahlungsdienstleister"

81. Die Tz 55 bis 64 unterscheiden nicht dahingehend, ob die jeweilige Verpflichtung lediglich den Zahlungsdienstleister, den abrechenden Zahlungsdienstleister oder im Einzelfall gegebenenfalls beide trifft. Die Unterscheidung ist für die praktische Umsetzung von wesentlicher Bedeutung. Außerdem lässt der vorliegende Entwurf keine Rückschlüsse darauf zu, was eine "sicherer und vertrauenswürdige Umgebung" im Sinne des Rundschreibens sein soll. Im Rahmen einer grundsätzlichen Betrachtung geht der BVZI davon aus, dass die in diesem Kapitel 3.3 getroffenen Regelungen von Zahlungsdienstleistern im Verhältnis zu ihren Kunden zu erfüllen sind. Deshalb sollte durchgängig auf den Zahlungsdienstleister abgestellt werden.

Kapitel 3.4 Login-Versuche, Session-Timeout, Gültigkeit der Authentisierung

82. Es wird auf die Darstellungen in Ziffer 26 dieser Stellungnahme verwiesen und um Änderung in "Kundenauthentifizierung" im gesamten Kapitel gebeten.

Tz 65 und Tz 66 – "Minimum"

83. Im Rahmen der Tz 65 wird darauf abgestellt, dass die Gültigkeit von Einmalpasswörtern auf das notwendige Minimum begrenzt werden muss. Dabei ist dem Rundschreiben nicht zu entnehmen, wie das notwendige Minimum zeitlich bestimmt werden kann. Je nach Zahlungsdienstleister und E-Händler können die zeitlichen Varianzen erheblich voneinander abweichen. Insofern erscheint eine Vorgabe hilfreich, wann nach Auffassung der BaFin das Minimum erreicht ist (z.B. 1 Stunde).

84. Daneben wird auch in Tz 66 vom Minimum im Verhältnis zu den Login- oder Authentifizierungsversuchen gesprochen. Wären die Erwartungen der BaFin erfüllt, wenn die Sperrung nach 10 erfolglosen Versuchen erfolgt und die temporäre Sperrung auf 10 Minuten beschränkt ist?

Kapitel 3.5 Transaktionsüberwachung

Tz 69 bis Tz 71, Tz 73 bis Tz 74 – "Zahlungsdienstleister"

85. In Übereinstimmung mit den Recommendations (10) und den Guidelines (Titel I – Tz. 10 ff) sollte bestimmt werden, welche Personen von der Regelung erfasst sind. Die hier benannten Tz 69 bis Tz 71 sowie Tz 73 und Tz 74 sind nach dem Verständnis des BVZI von Zahlungsdienstleistern zu erfüllen, nicht aber von abrechnenden Zahlungsdienstleistern.

Tz 72 – "Abrechnender Zahlungsdienstleister"

86. Gemäß der geltenden Gesetzeslage sind Institute im Sinne von § 1 Abs. 2a ZAG nicht verpflichtet, Maßnahmen zur Abwehr von "sonstigen strafbaren Handlungen" im Sinne von § 25h KWG vorzunehmen. Die Auferlegung eines solchen Erfordernisses ist zum gegenwärtigen Zeitpunkt nicht gesetzeskonform. Deshalb ist die Tz 72 ersatzlos zu streichen.

87. Unabhängig davon, haben abrechnende Zahlungsdienstleister im Rahmen ihrer eigenen geschäftsstrategischen Erwägungen Maßnahmen ergriffen, um betrügerisches Handeln durch E-Händler zu erkennen und entsprechende Gegenmaßnahmen durchzuführen. Es wird allerdings klargestellt, dass es sich hierbei um freiwillige Maßnahmen der Unternehmen oder um von Zahlungssystemen geforderte Maßnahmen handelt.

Kapitel 3.6 Schutz sensibler Zahlungsdaten Transaktionsüberwachung

Tz 75 bis Tz 79 – "Zahlungsdienstleister"

88. Es ist das Verständnis des BVZI, dass die Regelungen zum Schutz sensibler Zahlungsdaten auf den Recommendations 11 sowie den Guidelines Titel I – 11 beruhen. In den zugrundeliegenden Dokumenten ist nicht ersichtlich, dass die abrechnenden Zahlungsdienstleister an dieser Stelle verpflichtet werden sollten. Deshalb ist zum einen klarzustellen, dass die Regelungen des Kapitels 3.6 ausschließlich auf Zahlungsdienstleister anwendbar sind. Zum anderen ist den Vorgaben kein Verbot zu entnehmen, dass mit dem Entwurf der Tz 77 des Rundschreibens korrespondiert. Dieses dort geregelte Verbot würde auch im Widerspruch zu Tz 17 und Tz 78 des Entwurfs stehen. Deshalb ist Tz 77 ersatzlos zu streichen.

89. Ferner wird in Tz 76 eine sichere Ende zu Ende Verschlüsselung zwischen "Bank und Kunde" während des gesamten Dialoges gefordert. Der Begriff "Bank" ist nicht Gegenstand des Rundschreibens vielmehr zielt dieses auf den Zahlungsdienstleister ab, der seinen Kunden Internet-Zahlungsdienste anbietet. Insofern ist der Begriff "Bank" durch "Zahlungsdienstleister" zu ersetzen. Für die Erklärungen gilt das Gleiche.

Kapitel 4 Schutz der Kunden

Kapitel 4.1 Kundenschulung und Kommunikation

Tz 80 bis Tz 87 – "Zahlungsdienstleister"

90. Es ist das Verständnis des BVZI, dass die Regelungen Tz 80 bis Tz 87 unter Beachtung des Anwendungsbereichs ausschließlich auf insoweit erfasste Zahlungsdienstleister zutreffen.

Tz 88 – "optische Trennung"

91. Unter Beachtung unserer Ausführungen zu abrechenbaren Zahlungsdienstleistern schlagen wir folgende Formulierung vor:

> *"~~Acquirer~~ Abrechnende Zahlungsdienstleister werden bei Abschluss von neuen Akzeptanzverträgen die ~~haben Online-Händler~~ E-Händler dazu ~~aufzufordern~~ auffordern, zahlungsrelevante Prozesse klar vom Online-Shop zu trennen, um es für Kunden einfacher zu machen, zu erkennen, wann sie mit dem Zahlungsdienstleister und nicht mit dem ~~Zahlungsempfänger~~ E-Händler kommunizieren (z. B. ~~im Falle einer Umleitung eines~~ durch Weiterleitung des Kunden ~~durch~~ und Öffnen eines neuen Fensters, so dass der ~~Bezahlvorgang~~ Internet-Zahlungsdienst nicht ~~im Rahmen des Online-Händlers~~ innerhalb eines Frames des E-Händler angezeigt wird)."*

92. Aus Sicht des BVZI wäre dies eine Abkehr einer für die Betrugsbekämpfung anerkannten Sicherheitsmaßnahme. Danach werden Zahlungsvorgänge in Online-Shops technisch in einem eigenen "Frame" eingegeben, wobei dieser "Frame" allerdings graphisch in die Internetseite integriert ist, so dass ein Kunde weiterhin davon ausgeht, sich auf der gleichen Webseite zu befinden. Aufgrund dieser bisherigen Praxis kann aus Sicht des BVZI nicht das Risiko ausgeschlossen werden, dass Kunden Zahlungsvorgänge dann abbrechen werden, wenn sich ein neues Fenster öffnet und der Eindruck entsteht, dass er die Seite des E-Händlers verlassen hat. Kunden wurden bereits über mehrere Jahre

sensibilisiert, keine Zahlungsdaten in sogenannte „Pop-Up-Fenster“ einzugeben, da diese im Vergleich zu vorgenannter Implementierung vergleichsweise leicht zu fälschen sind.

93. Aus diesem Grund schlagen wir die ersatzlose Streichung des Tz 88 vor.

Zusammenfassung

94. Vorbehaltlich der vorstehenden detaillierten Ausführungen fassen wir unsere wesentliche Punkte wie folgt zusammen:

(a) Die Umsetzung der EBA Guidelines mit dem geplanten Rundschreiben gefährdet zum derzeitigen Zeitpunkt das "level playing field" auf Ebene der Europäischen Mitgliedsstaaten und führt aus Sicht des BVZI zur Verdrängung der in Deutschland ansässigen Zahlungsinstitute durch grenzüberschreitend tätige Zahlungsinstitute, die diesen weitergehenden Regelungen nicht unterliegen.

(b) Der offene Ausgang der Verhandlungen über die 2. Zahlungsdiensterichtlinie sollte abgewartet werden. Ferner sollte zunächst eine nationale Umsetzung der 2. Zahlungsdiensterichtlinie erfolgen, bevor das Rundschreiben in der vorliegenden Entwurfsfassung in Kraft tritt.

(c) Das Rundschreiben sollte den EBA Guidelines entsprechen. Dabei sollte allerdings berücksichtigt werden, dass aufgrund der zahlreichen Beteiligten für die komplexen technischen Entwicklungs- und Implementierungszyklen mindestens ein Umsetzungszeitraum von 2 Jahren zur Anwendung kommen sollte.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Bundesverband der Zahlungsinstitute e.V.

gez.	gez.
Nicolas Adolph	Christof Kohns
Mitglied des Vorstands	Mitglied des Vorstands