Stellungnahme

BITKOM vertritt mehr als 2.200 Unternehmen der digitalen Wirtschaft, davon gut 1.400 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 200 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 76 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 10 Prozent kommen aus Europa, 9 Prozent aus den USA und 5 Prozent aus anderen Regionen. BITKOM setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Steffen von Blumröder
Bereichsleiter
Banking & Financial Services
Tel.: +49.30.27576-126
s.vonblumroeder@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

BITKOM – Stellungnahme zum Entwurf „Mindestanforderungen an die Sicherheit von Internetzahlungen“ der der Bundesanstalt für Finanzdienstleistungsaufsicht Februar 2015

In den letzten Jahren haben sich die Voraussetzungen für den digitalen Zahlungsverkehr dramatisch verändert. Das Volumen des digitalen Zahlungsverkehrs hat sich enorm erhöht und neue Geschäftsmodelle im Zahlungsverkehr hervorgebracht. Das allgemeine Ziel ist die Harmonisierung des Europäischen Zahlungsverkehrs. Die Einführung der SEPA Verordnung war dabei ein wichtiger Schritt auf dem Weg zu standardisierten Prozessen im Euroraum und der EU.

In seiner Stellungnahme möchte der BITKOM auf einige wichtige Parameter in Bezug auf die unterschiedlichen Ansätze eingehen, die unerlässlich sind um Sicherheit bei Zahlungen im Internet herzustellen.

Position Paper
BITKOM Position Paper towards the
"Recommendations for the security of mobile payments"
page 2

1. Allgemeines

BITKOM ist der Meinung, dass der allgemeine regulatorische Rahmen der Europäischen Union bereits ein geeignetes Umfeld für Innovation und Wachstum im E- und M-Commerce, inklusive der entsprechenden Zahlungsdienste, bietet. Die EU-Gesetzgebung zu Zahlungsdiensten, E-Geld und Verbraucherrechten gehört weltweit zu den fortschrittlichsten und dient vielen Ländern als Vorbild bei der Umsetzung ähnlicher Marktstandardisierungen; umso mehr als die Empfehlungen der Europäischen und nationalen Finanzdienstleistungsaufsichten, sowie der EU-Gesetzgebung sich einander sehr gut ergänzen.

BITKOM unterstützt die Initiative für einen sicheren Internet-Zahlungsverkehr und den Schutz der Verbraucherinteressen. Wir sind aber auch der Meinung, dass die Perspektive wirtschaftlichen Erfolgs einer der Kernschlüssel für mehr Innovation und Wohlstand ist. Und: Mehr Regulierung wird nicht automatisch zu mehr Verbraucherschutz führen.

Die Geschwindigkeit mit der sich heute Innovationen im Zahlungsverkehr entwickeln, hat in den vergangenen Jahren vor allem durch die zur Verfügung stehenden Internetbandbreite und neuen Technologien zugenommen. Die Evolution ist derzeit ein laufender Prozess und ein Endszenario ist noch nicht abzusehen.

Allen Marktteilnehmern ist im eigenen Interesse daran gelegen, ihre Sicherheitsanforderungen permanent weiterzuentwickeln und zugleich eine gute Balance zwischen Sicherheit und Nutzerfreundlichkeit aufrechtzuerhalten. In den letzten Jahrzehnten wurde deshalb eine Reihe von Sicherheitskonzepten im Zahlungsverkehr eingeführt, die zum Teil jedoch angesichts neuer Technologien und neuer Angriffsstrategien hinfällig wurden und durch weiterentwickelte, noch sicherere Lösungen ersetzt werden mussten.

Ein präskriptiver regulatorischer Ansatz verändert diese Ausgangssituation völlig: Zum einen birgt er die Gefahr, dass die Marktteilnehmer sich vor allem darum bemühen werden, rechtliche Vorgaben einzuhalten und bei der Suche nach besseren Lösungen nachlassen. Zum anderen ist das Risiko unverkennbar, dass sichere Lösungen mit den unflexiblen regulatorischen Vorgaben nicht in Übereinstimmung zu bringen sind und daher nicht eingeführt werden.

Schon zum Zeitpunkt der Veröffentlichung der dem vorliegenden Rundschreiben-Entwurf zugrundeliegenden Empfehlungen des SecuRePay-Forums entsprachen die darin beschriebenen Sicherheitsvorschriften nicht mehr völlig dem aktuellsten Stand der Möglichkeiten. Seitdem sind über zwei Jahre vergangen. Die Techniken und Methoden der Gewährleistung von Zahlungsverkehrssicherheit, aber auch des Zahlungsbetrugs sind in dieser Zeit nicht stehengeblieben.

Das spiegelt sich auch in der aktuellen Diskussion zur Zahlungdiensterichtlinie 2 hinsichtlich der sicheren Authentifizierung bei Zahlungen im Internet wider. Sehr eindringlich verweisen wichtige Verbände der Marktteilnehmer darauf, dass die fixe einheitliche Vorgabe der Zwei-Faktoren Authentifizierung die Sicherheit von Zahlungen auf mittlere Sicht eher unterminieren als befördern wird. (Siehe etwa:

„E-COMMERCE AND ONLINE PAYMENTS INDUSTRIES URGE EU POLICY-MAKERS TO ALLOW FOR INNOVATION IN DIGITAL PAYMENT SECURITY" unter http://pr.euractiv.com/pr/e-commerce-and-online-payments-industries-urge-eu-policy-makers-allow-innovation-digital-payment).

Es wäre daher ein weit überlegener Ansatz, wenn die präskriptiven Anforderungen an sichere Zahlungen im Internet im Rundschreiben-Entwurf als **ein** möglicher Standard verstanden werden, während es den Unternehmen im Anwendungsbereich des Rundschreibens zugleich ermöglicht würde, nachzuweisen, dass auch andere Herangehensweisen – etwa die risikobasierte Authentifizierung unsicherer Transaktionen - zu vergleichbar guten oder gar besseren Ergebnissen führen können.

Aus diesem Grund empfehlen wir eindringlich wieder auf die in den EZB SecuRe Pay Empfehlungen verankerten Prinzipien des „Comply or Explain" zurückzugreifen und keine strikten Handlungsanweisungen zu formulieren. Diese tragen den unterschiedlichen technologischen Ansätzen in keinster Weise Rechnung.

Die regulatorische Neutralität in diesem Ökosystem ist von großer Bedeutung um den unterschiedlichen Ansätzen und Methoden von Zahlungslösungen Rechnung zu tragen. Aus Sicht des BITKOM ist es unbedingt nötig, bei Neuregelungen diese regulatorische Neutralität beizubehalten. BITKOM möchte darauf hinweisen, dass wesentliches Ziel der Rechtsvereinheitlichung im europäischen Zahlungsmarkt ist, einen modernen und kohärenten rechtlichen Rahmen für Zahlungsdienste zu schaffen, der technologisch neutral ist und gleiche Wettbewerbsbedingungen für alle Zahlungssysteme gewährleistet. Der Rechtsrahmen sollte zudem gewährleisten, dass die Mitgliedstaaten ihre aufsichtsrechtlichen Anforderungen aufeinander abstimmen (Erwägungsgründe 4 und 5 der Zahlungsdiensterichtlinie 2007/64/EG). Die Tatsache, dass die EZB SecuRePay Empfehlungen bzw. die EBA Guidelines zur Sicherheit von Internetzahlungen in einzelnen Mitgliedstaaten umgesetzt werden und in anderen nicht (offenbar zumindest in Großbritannien), wirkt dem diametral entgegen. Da es sich um aufsichtsrechtliche Anforderungen handelt, die dem Prinzip der Herkunftslandsaufsicht unterliegen, können zukünftig britischen Zahlungsdienstleister in Deutschland Internetzahlungsdienste zu anderen Bedingungen erbringen, als einheimische – etwa ohne starke Kundenauthentifikation und ohne sichere Kundenkommunikation, um nur Beispiele zu nennen. Eine im Vergleich zu anderen Ländern vorzeitige Festlegung wird, bei allem Verständnis für die Bemühungen um mehr Sicherheit im Zahlungsverkehr, zu einem weiteren erheblichen Wettbewerbsvorsprung der ausländischen Zahlungsdienstleister führen. Diese Ungleichbehandlung ist angesichts des europäischen Passes, der auch die Grundlage für die Zahlungsdiensterichtlinie ist, nicht hinnehmbar.

Der Entwurf berücksichtigt nur regulierte Zahlverfahren. Unregulierte Verfahren im Onlineshop wie z.B. Rechnungskauf sind davon nicht betroffen. Auch hier nimmt die Regulierung steuernd auf den Zahlungsmix Einfluss. Händler werden den Payment-Mix auf Zahlverfahren mit Zahlungsziel verlegen (Rechnungskauf oder Factoring), um so die Abbruchrate im Shop durch starke Authentifikation minimieren. Dies ist mit einem sozialpolitischen Kontext verbunden: Kunden mit

guter Bonität (= Qualifikation für Rechnungskauf) können weiter „bequem“ einkaufen, Kunden mit schlechter Bonität werden in unbequeme Zahlprozesse gezwungen (= starke Authentifikation beim Kauf).

2. Zeitpunkt der Implementierung

BITKOM ist der Meinung, dass sämtliche Initiativen zur verbindlichen Implementierung der Empfehlungen des European Forum on the Security oft Retail Payments vom 01.12.2013 („Recommendations“) und der Guidelines on the security of internet payments der European Banking Authority vom 19.12.2014 („Guidelines“) den gesetzlichen EU-Grundlagen Rechnung tragen müssen. Daher schlagen wir vor, die finalen Vorlagen der Zahlungsdiensterichtlinie 2 als Grundlage für die weitere Ausgestaltung der Sicherheit von Zahlungen im Internet, sowie auf mobilen Endgräten, zu nehmen und insofern die Verabschiedung der Zahlungdiensterichtlinie 2 abzuwarten. Die darin enthaltenen Vorschriften zur Authentifizierung von Zahlungstransaktionen befinden sich – unseres Erachtens zu Recht – noch stark in der Diskussion und werden sich im Vergleich zur voraussichtlich noch deutlich verändern. Es spricht daher vieles dafür, dass man mit Festlegungen noch abwartet, bis in der Diskussion zur Zahlungdiensterichtlinie 2 mehr Klarheit herrscht.

Nur so kann zum einen sichergestellt werden, dass sowohl auf nationaler als auch auf europäischer Ebene einheitliche, harmonisierte Bedingungen gewährleistet sind und zum anderen, dass die Unternehmen ausreichend Zeit zur Implementierung haben.

Schließlich sei darauf hingewiesen, dass auch zwischen dem vorliegenden Rundschreiben-Entwurf und dem Entwurf des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) Schnittstellen insofern bestehen, dass Meldepflichten für IT-Sicherheitsvorfälle in beiden Vorschriften enthalten sind. Hier gilt es, Definitionen, Meldepflichten und Meldewege so miteinander in Übereinstimmung zu bringen, dass die betroffene Wirtschaft sich keinen Doppelbelastungen oder gar widersprüchlichen Vorgaben gegenübersieht.

3. Änderungsanträge

Tz 2

Das Rundschreiben richtet sich an alle Zahlungsdienstleister im Sinne des §1 Abs.1 Zahlungsdiensteaufsichtsgesetz (ZAG), die Zahlungsgeschäfte i.S.d. §1 Abs.2 Nr.2 ZAG im Massenzahlungsverkehr über das Internet anbieten (Internet-Zahlungsdienste).

Im Gegensatz dazu geben die Leitlinien der Europäischen Bankaufsichtsbehörde (EBA) vor, dass die zuständigen Behörden in den 28 Mitgliedstaaten der Europäischen Union sicherstellen sollen, „dass die in Artikel 1 der PSD definierten Zahlungsdienstleister **unter ihrer Aufsicht** diese Leitlinien anwenden."

BITKOM ist der Meinung, dass angesichts dessen klargestellt werden muss, dass das vorgesehene Rundschreiben nur für inländische Zahlungsdienstleister anwendbar ist. Es ist sehr wahrscheinlich, dass die verschiedenen nationalen Aufsichtsbehörden die Empfehlungen und die Guidelines in unterschiedlicher Weise umsetzen werden.

Würde das Rundschreiben auch für ausländische Zahlungsdienstleister Anwendung finden, kann nicht ausgeschlossen werden, dass grenzüberschreitend tätige Zahlungsdienstleister unterschiedliche oder gar sich widersprechende Anforderungen einzuhalten hätten und damit den europäischen Dienstleistungsverkehr behindern würde.

In diesem Sinne muss der erste Satz der Tz 2 des Entwurfes wie folgt lauten:

> „Das Rundschreiben ist auf alle Zahlungsdienstleister im Sinne des § 1 Abs. 1 Zahlungsdiensteaufsichtsgesetz (ZAG) **mit Sitz im Inland** anwendbar, die Zahlungsgeschäfte i. S. d. § 1 Abs. 2 Nr. 2 ZAG im Massenzahlungsverkehr über das Internet anbieten (Internet-Zahlungsdienste)."

Im Rundschreiben wird geschrieben, dass die Mindestanforderungen an die Sicherheit von Internetzahlungen der BaFin betreffen Zahlungen sind, die kundenseitig von Menschen über Webbrowser ausgelöst werden.

Es stellt sich hier die Frage, ob mit „Kunde" der Verbraucher oder der Firmenkunde gemeint ist? Hier muss es eine Klarstellung geben, ob Firmenkunden einbezogen oder ausgeschlossen sind.

Anders als bei den Guidelines werden auch Online-Banking-Clients mit einbezogen, für die angemessene Sicherheitsvorkehrungen zu treffen sind, die ein vergleichbares Schutzniveau gewährleisten, wie für Internet-Zahlungen. Es ist klarzustellen, was genau unter Online-Banking-Clients fällt. Sind hier auch Programme und/oder Apps für das Online-Banking gemeint? Damit wären auch Mobile Payments Anwendungen betroffen, deren Sicherheit nach unserem Verständnis durch eine gesonderte noch in der Entstehung begriffene Empfehlung geregelt werden sollten. Während die Guidelines, das Telefonbanking ausnehmen, werden sie in dem Rundschreiben mit einbezogen. BITKOM fordert, diese aus wettbewerblichen Gründen weiterhin auszunehmen.

Tz 15

Der Rundschreiben-Entwurf sieht in Kapitel 2.3 Maßnahmen zur Überwachung von und ein Berichtswesen zu IT-Sicherheitsvorfällen vor. Insbesondere sollen Zahlungsdienstleister kritische Sicherheitsvorfälle an die Bundesanstalt für Finanzdienstleistungsaufsicht und gegebenenfalls an die Strafverfolgungsbehörden und zuständigen Datenschutzbeauftragten melden.

Meldepflichten für IT-Sicherheitsvorfälle sind auch im Regierungsentwurf des „Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz) vorgesehen, der in den kommenden Monaten im parlamentarischen Verfahren behandelt werden wird.

Auch wenn der genaue Anwendungsbereich der Meldepflichten nach dem IT-Sicherheitsgesetz noch nicht feststeht, da der Erlass der Rechtsverordnung nach § 10 BSI-Gesetz durch das Bundesministerium des Inneren noch aussteht, durch die die kritische Infrastrukturen im Sinne des IT-Sicherheitsgesetzes bestimmt werden, besteht doch ausweislich der Gesetzesbegründung (s. S. 54 ITSG-E) die Möglichkeit, dass Zahlungsdienstleister als Meldepflichtige beider Vorhaben bestimmt werden. Daraus resultiert die Gefahr, dass die Definition eines kritischen IT-Sicherheitsvorfalls, die Meldepflichten und Meldewege in beiden Rechtsvorgaben nicht übereinstimmen, die betroffene Wirtschaft damit doppelt belastet wird und sich im schlimmsten Falle sogar widersprüchlichen Vorgaben gegenüber sieht.

Sinnvoll wäre es daher, den Umgang mit kritischen IT-Sicherheitsvorfällen für Zahlungsdienstleister nur an einer Stelle zu regeln und dann für eine sinnvolle – und rechtssichere – Weiterverarbeitung der Meldungen verwaltungsintern zu sorgen. Dem diente der explizite Verweis im § 8c, Abs. 2 ITSG-E auf die durch das vorliegende BaFin-Rundschreiben entstehende vergleichbare Regelung für den Sektor Finanzwesen. Ein solcher Vorrang speziellerer Anforderungen für bestimmte Sektoren wird im Entwurf des IT-Sicherheitsgesetzes bereits für öffentlich zugängliche Telekommunikationsdienste im TKG oder für Betreiber von Energieversorgungsnetzen und Energieanlagen im Energiewirtschaftsgesetz vorgesehen.

Daneben ist darauf hinzuweisen, dass Meldepflichten im Zahlungsverkehrsbereich immer auch so ausgestaltet werden müssen, dass sie den hohen Standards an den Kundendatenschutz und die Vertraulichkeit von Bankgeschäften entsprechen.

Tz 17

Kunden von Acquirern sollen vertraglich zur Kooperation bei IT-Sicherheitsvorfällen verpflichtet werden. Der Acquirer ist verpflichtet, IT-Sicherheitsvorfälle der BaFin, der Staatsanwaltschaft und/ oder der Datenschutzbehörde zu melden. Das würde bedeuten, dass diese Behörden bei oder gegen die Kunden (z.B. Händler) ermitteln, wenn etwa dort ein Datendiebstahl stattgefunden hat. Die Kooperation des Händlers kann deshalb nur so weit

gehen, dass er sich nicht selbst Risiken (Reputation, vor allem auch Strafverfolgung) aussetzt. Vertraulichkeit der weitergegebenen Informationen muss gewährleistet sein. Das wäre in Tz 17 zu ergänzen.

Tz 31

Zahlungsdienstleister müssen dem Online-Händler im Wesentlichen die Pflichten der Tz 20 bis 30 vertraglich auferlegen. Ähnlich auch unten in Tz 78. Das bedeutet, dass Online-Händler demnächst ihre IT und Geschäftsprozesse, entsprechend organisieren müssen.

Tz 31 schießt aber über das Ziel hinaus; die durch Verweis einbezogenen Tz 20 bis 30 befassen sich nicht nur mit zahlungsspezifischen Fragen, sondern sind sehr allgemein gefasst und würden in dieser Allgemeinheit die gesamte IT-Infrastruktur des Händlers erfassen.

Tz 31 sollte daher dahingehend beschränkt werden, dass die Pflichten des Händlers nur eingreifen, wenn dieser sensible Zahlungsdaten verarbeitet. Die Beschränkung sollte weiterhin dahin gehen, dass der Händler die Verarbeitung sensibler Zahlungsdaten vollständig oder teilweise auf technische Zahlungsdienstleister auslagern kann und insoweit nur der technische Zahlungsdienstleister diese Voraussetzungen erfüllen muss.

Es übersteigt zudem die Möglichkeiten fast jedes Zahlungsdienstleisters, solche umfassenden Regelungen zur IT-Infrastruktur des Kunden (Online-Händlers) gegenüber großen oder mittelgroßen Kunden vertraglich durchzusetzen, geschweige denn die Einhaltung solcher Vertragsbestimmungen zu gewährleisten oder gar zu überwachen.

Tz 42

Das Rundschreiben fordert, dass für die Autorisierung von Internet-Zahlungen durch einen Kunden (inkl. Sammelüberweisungen) und für die Ausgabe oder Änderung von E-Mandaten starke Kundenauthentisierung einzusetzen ist.

Die generelle Absicht, digitale Zahlungen so sicher wie möglich zu gestalten wird vom BITKOM begrüßt. Allerdings sehen wir die Anforderungen einer starken Authentifikation als “one fits all”-Lösung kritisch, weil diese nicht den unterschiedlichen technisch möglichen und auch risikobasierten Ansätzen Rechnung trägt.

Die Authentifikation hängt immer an der Art der Transaktion und damit auch dem entsprechenden Checkout-Prozess, welcher für Endverbraucher von entscheidender Bedeutung ist.

Aus BITKOM Sicht stellen sich hierzu folgende Fragen:

Sind auch Programme gemeint, mit denen Firmenkunden Dateien elektronisch unterschreiben und an die Hausbank übertragen? Wenn dies der Fall ist, wäre der DFÜ-Standard EBICS und FileAct betroffen, bei denen heute in der Regel

keine starke Kundenauthentifizierung im Sinne des Rundschreibens gefordert ist (Verwendung von Besitz und einem statischen Passwort). Wir fordern eine Klarstellung.

Darüber hinaus ist klarzustellen, ob mit E-Mandaten auch im Internet erteilte Mandate gemeint sind, an der die Bank des Debitors nicht beteiligt ist. Unter Berücksichtigung des im Deutschen SEPA-Rat gefundenen Kompromiss kann nur die Erteilungen und Änderungen von E-Mandaten gemeint sein, bei denen die Bank des Debitors aktiv beteiligt ist (also e-Mandate im Sinne der EPC-Rulebooks). Die heute im Internet vom Zahlungspflichtigen per Mausklick dem Händler gegenüber erteilten Mandate sind rechtlich valide und sind daher explizit von den Anforderungen des Rundschreibens auszuschließen.

Tz 43, Tz 50 & Tz 54

BITKOM unterstreicht, dass es beim Thema Authentifikation eben nicht nur einen „one fits all" Ansatz geben kann, sondern dass immer auch die Verhältnismäßigkeit von Sicherheitsmechanismen betrachtet wird und alternative Verfahren zum Einsatz kommen können.

Angesichts dessen, wäre wünschenswert wenn BaFin sich mit der EBA bezüglich der Hinweise zur Auslegung der Ausnahmen in Tz 43 (s.a. Tz 50/54) absprechen würde, um eine europaweit einheitliche Auslegung sicherzustellen. Es wird leider im Wesentlichen die Vorlage übersetzt. Hier ist insbesondere die White List für den Online-Handel entscheidend. Die Kunden (Endkunden) müssen diese White Lists selbst festlegen (und dafür starke Authentisierung einsetzen). Hier wäre z.B. zu wünschen, dass zentrale Dienstleister wie z.B. „Trusted Shop" für Endkunden solche „White Lists" anbieten können, so dass hier großflächig alternative Authentisierenden eingesetzt werden können.

Die BaFin sollte darüber hinaus Hinweise zu solchen alternativen Methoden geben (s.a. Tz 50/54); dazu schweigt der Entwurf der MASin und leider auch die SecurRePay Empfehlungen, EBA Guidelines und EZB Assessment Guide vom Februar 2015.

Dies gilt auch für Tz 50/54: Hier sind von der BaFin Ausführungen zu erwarten, wie die „vordefinierten Kategorien von Transaktionen mit niedrigem Risiko" aussehen können.

Es würde der Zahlungsindustrie sehr helfen, wenn sie Auslegungshinweise zur Frage der alternative Authentisierungsverfahren erhielte. Der BITKOM als größter Branchenverband der IT-Industrie ist hier selbstverständlich gerne bereit, bei der Entwicklung solcher Auslegungshinweise und von Authentisierungsverfahren beratend mitzuwirken.

Und: Eine zukünftige Auslegung von sicherer Autorisierung darf nicht zu einer Unterminierung des Verbraucherschutzes durch eine entsprechende Haftungsverlagerung führen.

Tz 52 & Tz 53

Adressaten des Rundschreibens nur Zahlungsdienstleister sind im Sinne des ZAG. Insofern ist fraglich, wie die Formulierungen bezüglich der Wallet-Anbieter zu verstehen sind. Wallet-Anbieter können, müssen aber keine, Zahlungsdiensteanbieter iSd ZAG sein. Es ist ebenfalls klarzustellen, welche Form der Wallets durch den Entwurf des Rundschreibens erfasst sein sollen.

Insofern ist streng darauf zu achten, dass die Begrifflichkeiten sorgfältig definiert sind und Verpflichtungen nur diejenigen treffen, die diese auch erfüllen können.

Tz 78

Hinsichtlich der Speicherung und Verarbeitung sensibler Kundendaten durch Online-Händler; wäre ein Hinweis sinnvoll, dass ein Online-Händler, der die Verarbeitung auf einen technischen Dienstleister auslagert, diese Pflichten erfüllt, wenn er einen zuverlässigen technischen Dienstleister auswählt. Eine Haftung besteht also nur für ein etwaiges Auswahlverschulden.

Tz 88

Die Forderung nach einer Trennung von Shop und Zahlprozess geht über die einheitlichen SecurePay-Vorschriften hinaus. Händler müssen Ihre Prozesse gegebenenfalls massiv ändern.

Ein Zahlungsfenster in der gewohnten Händlershop-Umgebung bringt deutlich weniger Kaufabbrüche und Konfusion des Kunden mit sich, als in Fällen, in denen der Zahlprozess außerhalb des Shops des Händlers liegt. Dies bestätigt auch der Handel.

Die Vorschrift zur Trennung von Shop und Zahlprozess zwingt Händler von in Deutschland regulierten Zahlungsanbietern also zu kundenunfreundlchen Prozessänderungen und wird zu Umsatzeinbußen führen, während Händler mit Anbietern aus dem Ausland diese Vorschriften nicht haben. Der Handel wird darauf vermutlich so reagieren, dass er mit Zahlungsanbieter aus dem EU-Ausland kontrahiert statt mit deutschen Zahlungsanbietern, die einer strengeren Regulierung unterliegen. Dies führt zu einem weiteren, starken Incentive für Zahlungsdienstleister, ihren Firmensitz ins EU-Ausland zu verlagern bzw. schwächt Inlandsanbieter.

Tz 93

Im Vergleich zu den Guidelines werden hier die Anforderungen verschärft. Es soll dem Kunden ermöglicht werden, seine Transaktionen und Kontosalden jederzeit in Echtzeit in einer sicheren und vertrauenswürdigen Umgebung zu überprüfen. Die Guidelines sprechen jedoch lediglich von „near real-time“. Aus BITKOM Sicht sollte hier die originale Anforderung der Guidelines übernommen

werden und es den Marktteilnehmern ermöglicht werden, schnellere Service-Levels im Wettbewerb einzuführen.

Tz. 95

Diese Regelung steht im Zusammenhang mit dem der einzurichtenden Kommunikation über einen sicheren Kanal (Tz 80). Unsichere Kanäle wie SMS, Email oder Brief dürfen dementsprechend nur noch maskierte Zahlungsdaten enthalten. Die Kommunikation per Brief hier aufzunehmen, dürfte allerdings über das Ziel hinausschießen, immerhin ist dieser durch das Briefgeheimnis geschützt.