Verband der Auslandsbanken
in Deutschland e.V.
Association of Foreign Banks in Germany

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

per E-Mail an Konsultation-02-15@bafin.de

19. März 2015

Konsultation 02/2015

Sehr geehrte Damen und Herren,

haben Sie vielen Dank für die Zusendung des Konsultationspapiers 02/2015 vom 4. Februar 2015 über den Entwurf für ein Rundschreiben zu den Mindestanforderungen an die Sicherheit von Internetzahlungen. Gerne nehmen wir die Möglichkeit zur Stellungnahme wahr.

Der Verband der Auslandsbanken in Deutschland vertritt gegenwärtig über 200 ausländische Banken, Kapitalverwaltungsgesellschaften und Finanzdienstleistungsinstitute, die sich in Deutschland mit Tochtergesellschaften und Zweigstellen niedergelassen haben. Im Zusammenhang mit der Einführung von Mindestanforderungen an die Sicherheit von Internetzahlungen steht für die meisten Auslandsbanken, die im Inland meist nur sehr begrenzt Zahlungsdienstleistungen für Verbraucher anbieten, vor allem die Frage im Vordergrund, ob diese Anforderungen auch für das Geschäft mit Firmen- und Geschäftskunden Anwendung finden müssen.

Darüber hinaus sollte die derzeit vorgesehene zeitnahe Umsetzung überdacht werden, da, wie auch in Ihrem Anschreiben an die Verbände festgestellt wird, die Arbeiten an der novellierten EU-Zahlungsdiensterichtlinie („PSD 2“) noch nicht abgeschlossen sind, was eine Anpassung der Mindestanforderungen nach Veröffentlichung der PSD 2 wahrscheinlich macht.

Nachfolgend erlauben wir uns, Ihnen, einige Vorschläge zu bestimmten Anliegen zu unterbreiten, zu denen aus Sicht der Auslandsbanken noch Klärungsbedarf besteht. Es würde uns freuen, wenn diese Eingang in das Rundschreiben finden.

Andreas Kastl

Verband der Auslandsbanken
Weißfrauenstraße 12-16
60311 Frankfurt am Main
Tel: +49 69 975850 0
Fax: +49 69 975850 10
andreas.kastl@vab.de
www.vab.de

Interessenvertretung
ausländischer Banken,
Kapitalverwaltungsgesellschaften,
Finanzdienstleistungsinstitute
und Repräsentanzen

Eingetragen im Transparenzregister
der Europäischen Kommission,
Registrierungsnummer:
95840804-38

zu Textziffer 2: Anwendungskreis des Rundschreibens

In Tz. 2 werden die von den Mindestanforderungen erfassten Internet-Zahlungsdienste definiert als solche, die Zahlungsdienstleister im Massenzahlungsverkehr über das Internet anbieten. Wie bereits angedeutet, besteht aus unserer Sicht große Notwendigkeit an einer Klarstellung, dass die in dem Rundschreiben vorgesehenen Mindestanforderungen keine Anwendung finden sollte für Zahlungen von Zahlungsdienstenutzern, die nicht Verbraucher sind. Die dem Rundschreiben zu Grunde liegenden Empfehlungen des von der EZB beauftragten European Forum on the Security of **Retail** Payments („SecuRe Pay") legen den Fokus auf das Retail-Geschäft. Auch in Ihrem Anschreiben an die Verbände vom 4. Februar 2015 heißt es zum einen, dass das Rundschreiben das Vertrauen des **Verbrauchers** in Internetzahlungsdienste stärken soll. Eine Anwendung über der Privatkundengeschäft hinaus würde unseres Erachtens eine Abweichung von den europäischen Vorgaben bedeuten, was im Sinne einer einheitlichen Anwendung der von der EZB aufgestellten Empfehlungen durch die EU-Mitgliedstaaten zu vermeiden ist.

Viele Zahlungen von Firmen- und Geschäftskunden werden automatisiert aus deren ERP-Programmen erzeugt und über die kontoführenden Stellen abgewickelt. Somit werden solche Zahlungen nicht explizit durch einen Menschen über einen Webbrowser angestoßen, was gemäß Satz 1 des Erklärungstextes zur Tz. 2 als Voraussetzung aufgestellt wird, um von den Mindest-anforderungen erfasst zu sein: „Werden von Zahlungsdienstleistern Internet-Zahlungsdienste angeboten, so geht das Rundschreiben davon aus, dass die Zahlungen kundenseitig von Menschen über Webbrowser ausgelöst werden".

Der Satz 2 im Erklärungstext zur Tz. 2 besagt weiter, dass bei der Bereitstellung von Verfahren zur Nutzung von endkundenorientierten Online-Banking-Clients (z. B. FinTS) angemessene Sicher-heitsvorkehrungen zu treffen seien, die ein vergleichbares Schutzniveau gewährleisten. Aus unserer Sicht sollte klargestellt werden, dass mit den hier genannten endkundenorientierten Online-Banking-Clients (z.B. FinTS) keine Applikationen wie die o. g. ERP-Programme oder auch solche Applikationen gemeint sind, die Firmen- und Geschäftskunden zur Unterstützung des Finanzmanagements ihres Unternehmens nutzen, wie z. B. MultiCash. Denn zum eröffnet der Zahlungsdienstleister oft lediglich eine Schnittstelle zur Einlieferung von Zahlungsaufträgen von Firmen- und Geschäftskunden, wie beispielsweise für die Übertragungsform EBICS, die sich in Form von Clients manifestieren kann, es aber nicht muss. Welche „Software" kundenseitig genutzt wird, bleibt dem Kunden überlassen. Eine Bank kann somit keine einheitliche Beratung und Information, wie im Rundschreiben beschreiben, für die Firmen- und Geschäftskunden gewährleisten, weil die kundenseitig vorliegenden IT-Infrastrukturen sehr stark variieren. Zum anderen ist bei Firmen- und Geschäftskunden allgemein von einem höheren IT-Sicherheits- bzw. -Schutzniveau auszugehen als bei Privatkunden, da diese schon aus Eigeninteresse entsprechende Maßnahmen im Unternehmen treffen. Die in dem Rundschreiben im Abschnitt 3.1 „Initiale Kundenidentifikation und Information" beschriebenen Maßnahmen, welche die Banken und andere Zahlungsdienstleister umzusetzen haben, passen somit oftmals nicht auf die Situation von Firmen- und Geschäftskunden.

Darüber hinaus ist auszugehen, dass der im Anschreiben vorgestellte Erfüllungsaufwand für die Wirtschaft von ca. 20,3 Mio. EUR insgesamt mit Sicherheit sehr viel höher ausfallen würde, wenn auch der Zahlungsverkehr von Firmen- und Geschäftskunden von den Mindestanforderungen erfasst wäre. Denn insbesondere bei den Auslandsbanken in Deutschland, die zu einem großen

Teil grenzüberschreitend tätige Konzerne bzw. Unternehmen als Kunden im Zahlungsverkehr betreuen, würde dies einen hohen Aufwand bedeuten, da die vorwiegend genutzten Electronic-Banking-Systeme für Firmen- und Geschäftskunden aus dem jeweiligen Herkunftsstaat stammen, wo die Konzern- bzw. Unternehmenszentrale der Auslandsbank sitzt. Zudem muss bedacht werden, dass bei grenzüberschreitend tätigen Unternehmen der Ansprechpartner für den Zahlungsverkehr (Buchführung, Cash-Management), der über eine Auslandsbank in Deutschland abgewickelt wird, oftmals nicht in Deutschland sitzt, sondern im Ausland, wo gegebenenfalls abweichende Sicherheitsanforderungen gelten.

Das Rundschreiben sollte sich nur auf Zahlungen (bzw. Zahlungsdienste) von Verbrauchern beziehen, um eine einheitliche Umsetzung in der EU zu gewährleisten.

VORSCHLAG: Die Textziffer 2 sollte folgendermaßen ergänzt werden:
„(1) Das Rundschreiben ist auf alle Zahlungsdienstleister im Sinne des § 1 Abs. 1 Zahlungsdiensteaufsichtsgesetz (ZAG) anwendbar, die Zahlungsgeschäfte i. S. d. § 1 Abs. 2 Nr. 2 ZAG im Massenzahlungsverkehr über das Internet <u>für Verbraucher</u> anbieten (Internet-Zahlungsdienste).“

zu Textziffer 7: Definition der Risikomanagement-Funktion

Im Hinblick auf die beschriebene Risikomanagement-Funktion sollte im Rundschreiben klargestellt werden, dass es sich hierbei nicht um die Risikokontrollfunktion nach MaRisk AT 4.4.1 handeln muss, insbesondere aufgrund der vielfachen technischen Anforderungen und Wirkungsbereiche, die mit dieser Funktion einhergehen. Zudem müssen nicht alle Anbieter von Zahlungsdienstleistungen die MaRisk erfüllen.

VORSCHLAG: In Textziffer 7 sollte Satz 1 folgendermaßen angepasst werden:
„(1) Zahlungsdienstleister haben durch ihre zuständige Risikomanagement-Funktion<u>, die nicht mit der Risikokontrollfunktion nach den MaRisk übereinstimmen muss,</u> für Zahlungen im Internet und die zugehörigen Dienste eine detaillierte Risikoidentifikation und Schwachstellenanalyse (Risikoanalyse) durchzuführen und zu dokumentieren.“

zu Textziffer 7: Definition der Risikoanalyse

Es sollte in dem Rundschreiben klargestellt werden, dass die in Textziffer 7 Satz 2 beschriebene Risikoanalyse entweder organisatorisch alleinstehend eingerichtet werden oder mit der Risikoanalyse, welche Verpflichtete i. S. d. Geldwäschegesetzes (GwG) für Zwecke der Gefährdungsanalyse vornehmen, verbunden werden kann. Darüber hinaus sollte das Rundschreiben eine Orientierung geben zum Umfang und zur Herleitung der geforderten Risikoanalyse, gegebenenfalls in Anlehnung an die Auslegungs- und Anwendungshinweise (AuA) zur Geldwäscheprävention und -bekämpfung.

VORSCHLAG: In Textziffer 7 sollte Satz 2 folgendermaßen angepasst werden:
„(2) In die Risikoanalyse<u>, die entweder organisatorisch alleinstehend eingerichtet oder mit der Risikoanalyse, welche Verpflichtete i. S. d. Geldwäschegesetzes (GwG) für Zwecke der Gefährdungsanalyse vornehmen, verbunden werden kann,</u> sind insbesondere einzubeziehen (...)“

zu Textziffer 7: Durchführung der Risikoanalyse

Es sollte in dem Rundschreiben klargestellt werden, dass die Risikoanalyse lediglich vor der Einführung neuer Dienste durchzuführen ist. Andernfalls könnte der Eindruck erweckt werden, dass alle bereits bestehenden Zahlungsdienste nach Inkrafttreten des Rundschreibens bis zu dem Zeitpunkt eingestellt werden müssten, zu dem die Risikoanalyse abgeschlossen wurde.

VORSCHLAG: In Textziffer 7 sollte Satz 3 folgendermaßen angepasst werden:
„3Die Risikoanalyse ist vor der Einführung ~~der~~ neuer Dienste durchzuführen und anschließend regelmäßig zu wiederholen."

zu Textziffer 7: Vorgaben des BSI

Im Erklärungstext zu Tz. 7 wird auf Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI) verwiesen. Diese sollen im Rahmen einer Schutzbedarfsanalyse eingehalten werden, werden aber nicht explizit benannt. Dahingehend bitten wir um eine Spezifizierung, welche Standards dies sind. Unseres Erachtens sollte es sich dabei um die folgenden Standards handeln:

- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz,
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise.

VORSCHLAG: Der erste Satz des Erklärungstextes zu Textziffer 7 sollte folgendermaßen ergänzt werden:
„1Im Rahmen der Risikoidentifikation und -analyse wird eine Schutzbedarfsanalyse nach Vorgaben 100-2 und 100-3 des Bundesamts für Sicherheit in der Informationstechnik (BSI) erwartet, welche eine Schutzbedarfsfeststellung umfasst."

zu Textziffer 7: Form der Schutzbedarfsanalyse

Im Erklärungstext zu Tz. 7 wird nicht eindeutig festgelegt, ob die Schutzbedarfsanalyse in die Risikoanalyse integriert werden kann oder ob es sich dabei um zwei getrennte Dokumente handeln soll. Aus unserer Sicht sollten beide Wege möglich sein.

VORSCHLAG: Der Erklärungstext zu Textziffer 7 sollte um einen neuen Satz 2 ergänzt werden:
„2Die Schutzbedarfsanalyse und die daraus abzuleitende Schutzbedarfsfeststellung kann entweder in die Risikoanalyse integriert werden oder getrennt von dieser erstellt werden."

Textziffer 15: Meldepflichten zu kritischen IT-Sicherheitsvorfällen

Im Erklärungstext zu Tz. 15 werden bestimmte bankfachlichen Prozesse genannt, bei denen im Falle eines Ausfalls oder Teilausfalls ein kritischer IT-Sicherheitsvorfall vorliegen soll. Diese bankfachlichen Prozesse umfassen nicht nur Online-Banking einschließlich Mobile-Banking, sondern auch die Bargeldversorgung und **jeglichen Zahlungsverkehr** einschließlich Kartenzahlungen. Hiermit geht das Rundschreiben im Hinblick auf die Meldung kritischer IT-Sicherheitsvorfälle über den

Anwendungsbereich der zugrunde liegenden EZB-Empfehlungen und EBA-Leitlinien hinaus, da dies nicht nur die in Tz 2. Satz 1 genannten Internet-Zahlungsdienste betrifft. Unseres Erachtens sollten sich auch die Meldepflichten zu kritischen IT-Sicherheitsvorfällen an den eigentlichen Anwendungsbereich des Rundschreibens richten.

VORSCHLAG: Der Erklärungstext zu Textziffer 15 sollte folgendermaßen angepasst werden:
„1Als Beispiele für kritische IT-Sicherheitsvorfälle sind insbesondere zu nennen:
- Ausfälle oder Teilausfälle ~~der nachgenannten~~ des bankfachlichen Prozesses zur Bereitstellung des Online-Bankings einschließlich Mobile-Bankings über einen Zeitraum von mehr als ~~1~~ eine Stunde.~~:~~
~~o Bargeldversorgung~~
~~o Jeglicher Zahlungsverkehr einschließlich Kartenzahlung~~
~~o Online-Banking einschließlich Mobile-Banking;~~
(...)“

zu Textziffer 28: Prüfungen durch vertrauenswürdige und unabhängige (interne bzw. externe) Experten

Die Prüfungen der Sicherheitsmaßnahmen, die gemäß den Mindestanforderungen getroffen werden sollen, sollen von vertrauenswürdigen und unabhängigen (internen bzw. externen) Experten durchgeführt werden. Neben einer Klarstellung, wer in diesem Kontext vertrauenswürdige und, gegebenenfalls zur Abgrenzung, wer nicht-vertrauenswürdige Experten sein könnten, wären wir sehr dankbar.

Darüber hinaus sollte anhand von Beispielen klargestellt werden, wer die internen (gegebenenfalls die interne Revision) und die externen (gegebenenfalls die Jahresabschlussprüfer) Experten sein können.

Zudem sollte die Einschränkung, dass diese Experten in keinster Weise in die Entwicklung, Implementierung oder den Betrieb des Internet-Zahlungsdienstes eingebunden sein dürfen, aufgeweicht werden. Denn gerade bei den personell eher schmal aufgestellten Auslandsbanken in Deutschland, bei denen viele Querschnittsfunktionen (IT, Organisation, Compliance etc.) durch die jeweilige Unternehmenszentrale im Ausland wahrgenommen werden, mag es in vielen Fällen keinen Experten für Sicherheitsfragen im Zahlungsverkehr geben, der **nicht** in der Zahlungsverkehrsabteilung bzw. -funktion arbeitet.

VORSCHLAG: In Textziffer 28 sind die neuen Sätze 3 und 4 einzufügen und der Satz 5 (vorher 3) folgendermaßen anzupassen:
„2Die Prüfungen sind von vertrauenswürdigen und unabhängigen (internen bzw. externen) Experten durchzuführen. 3Die internen Experten können beispielsweise die interne Revision sein. 4Die externen Experten können beispielsweise die Jahresabschlussprüfer sein. 5Diese Experten ~~dürfen~~ sollten möglichst nicht ~~in irgendeiner Weise~~ in die Entwicklung, Implementierung oder den Betrieb des Internet-Zahlungsdienstes eingebunden sein.“

zu Textziffer 30: Externe Ausübung der Sicherheitsfunktionen

Gemäß Tz. 30 sollen die Zahlungsdienstleister sicherstellen, dass im Falle einer Ausübung der Sicherheitsfunktionen durch Externe diese die Anforderungen dieses Rundschreibens einhalten. In diesem Zusammenhang sollte zum einen klargestellt werden, welche einzelnen Sicherheitsfunktionen damit gemeint sein können, und zum anderen, wer in diesem Zusammenhang als extern gilt. Bei den Auslandsbanken in Deutschland ist es nicht auszuschließen, dass einzelne sog. Sicherheitsfunktionen durch verbundene Unternehmen im gleichen Konzern, beziehungsweise bei Zweigniederlassungen und Zweigstellen ausländischer Banken (gemäß §§ 53, 53b, 53c KWG) durch die jeweilige Hauptniederlassung ausgeübt werden. Diese verbundenen Unternehmen bzw. Hauptniederlassungen erfüllen regelmäßig die Sicherheitsanforderungen im jeweiligen Sitzstaat. Daher sollte das Rundschreiben eine Öffnungsklausel für vergleichbare Sicherheitsanforderungen in EU-Mitgliedstaaten und Drittstaaten enthalten.

VORSCHLAG: Die Textziffer 30 ist um den folgenden Satz 2 zu ergänzen:
„1Übernehmen Externe Sicherheitsfunktionen für den Zahlungsdienstleister, so hat der Zahlungsdienstleister sicherzustellen, dass der Externe die Anforderungen dieses Rundschreibens einhält. 2Insofern Sicherheitsfunktionen durch ein im Ausland belegenes Konzernunternehmen oder die Hauptniederlassung im Herkunftsstaat erfüllt werden, ist im Falle des EU-Auslands regelmäßig und im Falle eines Drittstaats nach Einzelfallprüfung von vergleichbaren Sicherheitsanforderungen auszugehen, weshalb eine Sicherstellung durch den inländischen Zahlungsdienstleister entfallen kann.“

Nichtbeanstandungsregelung

Im Anschreiben an die Verbände vom 4. Februar 2015 wird festgestellt, dass das Rundschreiben mit Veröffentlichung in Kraft treten soll. Jedoch soll es eine Nichtbeanstandungsregelung geben, wonach die Nichteinhaltung der Mindestanforderungen bis zu sechs Monate nach Veröffentlichung des Rundschreibens von der Aufsicht nicht beanstandet werden soll. Die Rückmeldung aus dem Kreis der Mitglieder war hierzu eindeutig, dass es realistischerweise zumindest zwölf Monate Nichtbeanstandungszeit geben sollte. In den nordischen EU-Mitgliedstaaten sollen die Institute 18 bis 24 Monate Zeit bekommen haben, um die Vorgaben aus den EZB-Empfehlungen (bzw. den EBA-Leitlinien) umzusetzen.

Für Rückfragen stehen wir Ihnen gerne, auch im Rahmen eines persönlichen Gesprächs, zur Verfügung.

Mit freundlichen Grüßen

Markus Erb Andreas Kastl