Deutsche Bank

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Referat BA 57
Herr Martin
Graurheindorfer Str. 108
53117 Bonn

Deutsche Bank AG
Dr. Jan Boehm
Unter den Linden 13-15
10117 Berlin
Tel.: +49 30 3407 3157
jan.boehm@db.com

Per Email: Konsultation-02-15@bafin.de

Berlin, 19. März 2015

Stellungnahme der Deutschen Bank zu Konsultation 02/2015 – Mindestanforderungen an die Sicherheit von Internetzahlungen

Sehr geehrter Herr Martin,

am 4. Februar 2015 hat Ihr Haus den Entwurf eines Rundschreibens zum o.g. Thema vorgelegt. Wir greifen dankend die Möglichkeit auf, zum Entwurf des Schreibens und den beiden Anlagen Stellung nehmen zu können.

Die Digitalisierung unserer Dienstleistungen ist eine der entscheidenden Herausforderungen für unser Geschäft, die wir gern und aktiv annehmen und vorantreiben. Die große Mehrheit unserer Kunden erwartet heute von uns, dass wir ihnen unsere Produkte und Dienstleistungen jederzeit und über alle denkbaren Kanäle zur Verfügung stellen. Wir stellen dabei täglich den Schutz der Daten und Einlagen unserer Kunden sicher. Wir legen die höchsten Standards an die Sicherheit des Bezahlens im Internet, ebenso wie an alle anderen Kanäle.

Wir unterstützen ausdrücklich die Absicht der BaFin, ihre Anforderungen so eng wie möglich an den Empfehlungen des European Forum on the Security of Retail Payments zu orientieren. Dies schafft gleiche, sachgerechte Standards im europäischen Bankgeschäft und ermöglicht die von der EU-Kommission ausdrücklich vorgesehene Möglichkeit von Cross-Border-Angeboten. Daher treten wir dafür ein, die Vorgaben der EBA nicht zu überschreiten und kommenden gesetzlichen Regelungen wie dem IT-Sicherheitsgesetz oder der Novelle der EU-Zahlungsdienstleistungs-Richtlinie (PSD II) nicht vorwegzugreifen. In diesem Zusammenhang konzentrieren wir uns im Anhang auf die für uns wesentlichen Fragen. Die detailliertere Darstellung in der Stellungnahme der Deutschen Kreditwirtschaft (DK), zu der wir aktiv beigetragen haben, unterstützen wir darüber hinaus vollständig.

Für eventuelle Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Dr. Jan Boehm
Managing Director
Head of Government & Regulatory Affairs (GRAD) Germany
Deutsche Bank

ANHANG – Mindestanforderungen an die Sicherheit von Internetzahlungen – Kernpunkte aus Sicht der Deutsche-Bank-Gruppe

1) Telefon-Banking (Tz 2)

Telefon-Banking stellt kein Internet-Bezahlverfahren dar. Es ist vielmehr ein alternativer Kanal. In unserem Geschäft werden beide Kontaktmöglichkeiten des Kunden vollkommen getrennt behandelt (z.B. mit separaten PINs). Das Telefon-Banking wurde bei den SecuRePay/EBA-Richtlinien explizit ausgeschlossen (vgl. Punkt 11 der EBA-Guideline). Somit ist die vorgesehene Bestimmung nicht nur eine über die Mindestanforderungen hinausgehende Bestimmung – sie widerspricht vielmehr klar der EBA-Regelung. Wir empfehlen daher die Streichung jeglicher Anforderungen an das Telefon-Banking aus dem Rundschreiben. Dies umfasst auch die Streichung jeglicher Beispiele für konkrete Produkte (auch für Online-Banking-Clients wie z.B. FinTS).

2) Standards für die Schutzbedarfsanalyse (Tz 7)

Im kursiven Text wird eine Schutzbedarfsanalyse gemäß BSI-Vorgaben benannt. Diese basiert auf einem rein nationalen Standard. Wir empfehlen die Anwendung international gültiger Standards (wie ISO 27001). Damit wird eine europäische Umsetzung im Sinne der EZB und EBA erleichtert.

3) Meldung kritischer Vorfälle (Tz 15)

Die hier niedergelegten Anforderungen gehen über die EBA-Guidelines weit hinaus und greifen dem geplanten IT-Sicherheitsgesetz der Bundesregierung vor. Wir würden empfehlen, mit der detaillierten Regelung in diesem Feld bis zur Verabschiedung des IT-Sicherheitsgesetzes zu warten. Zudem wäre eine praxisbezogenere Regelung der verpflichtenden Meldungen wünschenswert: Es sollten klare Anforderungen formuliert werden, was gemeldet werden soll, z.B. welche Anwendungen konkret davon betroffen sind. Meldungen von Sicherheitsvorfällen sollten nur an eine einzige Stelle abzugeben sein. Es sollte genau durch den/die Empfänger definiert sein, was mit den gemeldeten Daten passiert. In jedem Fall muss die Vertraulichkeit der Informationen garantiert werden und diese sollten nur nach Rücksprache mit dem betroffenen Unternehmen an eine andere Behörde weitergegeben werden. Eine Erweiterung der Anforderungen auf Bereiche außerhalb von Internet-Zahlungen wie Bargeld-Versorgung oder Karten-Zahlungsverkehr halten wir zudem für nicht sachgemäß.

4) Einsatz von Kreditkarten (Tz 36)

Derzeit enthalten Verträge zwischen Kartenausgeber und -inhabern nicht explizit die verschiedenen Einsatzmöglichkeiten einer Karte. Allerdings kann heute davon ausgegangen werden, dass allen Kreditkarten-Inhaber bewusst ist, dass sie diese für das Bezahlen beim Online-Shopping verwenden können. Damit sollte diese Möglichkeit auch ohne explizite Auflistung im Vertrag als vereinbarte Funktion gelten. Sollte die BaFin an der hier vorgesehenen Regelung festhalten wollen, dann sollte sie klarstellen, dass dies nur für zukünftige Kreditkartenverträge gilt, damit nicht mit allen Bestandskunden, die heute bereits Kreditkarten im Internet nutzen, neue Verträge zu vereinbaren sind.

5) TAN-Generierung (Tz 42)

Die Ausführungen im zweiten Satz der Erläuterung geht über die Anforderungen der EBA-Guideline hinaus: Weder wird gefordert, dass wesentliche Transaktionsdaten in die Generierung der TAN eingehen müssen, noch wird gefordert, dass die 2FA unabhängig von der primären Verbindung zu erfolgen hat.