IK
Interessengemeinschaft
Kreditkarten

IK Interessengemeinschaft Kreditkarten · Im Uhrig 7 · 60433 Frankfurt

Bundesanstalt für Finanzdienstleistungsaufsicht
Grundsatz Cybersicherheit und Regulierung
Zahlungsverkehr
Referat GIT 1
Graurheindorfer Straße 108
53117 Bonn

IK
Interessengemeinschaf Kreditkarten
c/o PaySys Consultancy GmbH
Im Uhrig 7
60433 Frankfurt

Tel.: +49(69)95 11 77-10
Fax: +49 (69) 52 10 90

vorab per e-mail

München, 13 September 2018

Dr. Markus Escher markus.escher@gsk.de
Dr. Hugo Godschalk hgodschalk@paysys.de

- **Stellungnahme zu den finalen EBA Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2) (EBA/GL/2018/05) vom 18.07.2018**
- **Ausblick auf Umsetzung durch die BaFin**
- **Zum Betrugstyp „CEO Fraud“**

Sehr geehrter Herr Dr. Strassmair-Reinshagen,

wir wenden uns an Sie im Auftrag der Interessengemeinschaft Kreditkarten (nachfolgend „**IK**“).
Die IK ist eine rechtlich nicht verselbständigte, wettbewerbsneutrale Plattform für Unternehmen, die im Kredit- oder Debitkartengeschäft in Deutschland Kartenissuer, -acquirer, -Netzbetreiber oder Prozessoren sowie Lizenzgeber informiert und Stellungnahmen zu Gesetzgebungs- und Regulierungsvorhaben mit Auswirkungen auf das Kartengeschäft abgibt.

Die folgenden Teilnehmer an der IK haben bei Erarbeitung dieser Stellungnahme mitgewirkt:

- BS Payone GmbH
- Bayern Card-Services GmbH
- Commerzbank AG
- Concardis GmbH

- Deutsche Telekom AG
- Elavon Financial Services DAC
- EVO Payments International GmbH
- First Data Deutschland GmbH
- InterCard AG
- LogPay Financial Services GmbH
- Lufthansa AirPlus Servicekarten GmbH
- MasterCard Europe S.A.
- S-Payment GmbH
- TeleCash GmbH & Co. KG
- transact Elektronische Zahlungssysteme GmbH
- Verband der Sparda-Banken e.V.
- VISA Europe
- equensWorldline SE
- Wirecard Bank AG

Im Vorgriff auf die Entwicklung einer deutschen Verwaltungspraxis der BaFin zum Betrugsmeldewesen nach § 54 (5) ZAG und einer etwaigen diesbezüglichen Umsetzung der jüngst seitens der European Banking Authority („EBA“) veröffentlichten finalisierten EBA Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2) (EBA/GL/2018/05) (im Folgenden „EBA Guidelines“ oder „Final Report“) gibt die IK im Folgenden eine spezifische Stellungnahme zum Aspekt des Betrugstyps „CEO Fraud“ ab:

1. Sog. „CEO-Fraud“ unterfällt bereits gemäß Art. 96 (6) PSD2 nicht dem Anwendungsbereich des Betrugsmeldewesens. Die IK ist daher der Auffassung, dass sich aus dieser Richtlinienbestimmung keine Erstreckung auf „CEO-Fraud“ ergibt und entsprechend durch die BaFin auch nicht in die deutsche Aufsichtspraxis übertragen werden sollte:

a) Aus Sicht der IK, berücksichtigt der in den GL 1.1.b definierte Betrugstyp “manipulation of the payer” Umstände, die über den vorgesehen Anwendungsbereich des Fraud Reportings hinausgehen:

> *„payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee (‘manipulation of the payer’).”*

Gemäß Art. 96(6) PSD2 sollten nur die Sachverhalte dem Anwendungsbereich der Meldepflichten unterfallen, in denen ein Betrüger direkten Einfluss auf die Zahlungstransaktion oder die Autorisierung – aber nicht die **Motivation** des Zahlers – hat.

Dies ergibt sich aus Rz.14 des EBA Entwurfs:

"*Across the PSD 2, provisions and recitals make various references to payment fraud-related terms, such as "unauthorized or fraudulent use of the payment instrument", "unauthorized or fraudulent initiation of a payment transaction", "payer acting fraudulently" or "fraud relating to different means of payment".*"

Danach bezieht sich eine betrügerische Zahlungstransaktion immer auf eine Zahlungstransaktion oder mindestens auf einen Autorisierungsvorgang einer Transaktion. Der Betrug oder die Täuschung des Zahlers als **Individuum** war hingegen noch nie vom Begriff der "betrügerischen Zahlungstransaktion" umfasst. So muss zwischen den Parteien einer Zahlungstransaktion, der Übertragung von zahlungs- oder autorisierungsbezogener Daten und dem Betrug gegenüber bzw. der Täuschung einer Partei ohne Manipulation der Zahlungstransaktion (sog. "CEO Fraud") unterschieden werden.

b) Gerade Fälle des sog. "CEO Fraud", führen zu **ordnungsgemäß autorisierten Zahlungstransaktionen**. Eine Manipulation der Transaktion oder der Transaktionsdaten findet gerade nicht statt. Angesichts der Definition von betrügerischen Zahlungstransaktionen, sollten daher derartige Manipulationen nicht von der PSD 2 (und der Verwaltungspraxis nach Art. 96 (6) PSD 2 bzw. § 54 (5) ZAG umfasst sein. Denn die Manipulation ist in diesen Fällen nur auf den Zahler als individuelle Person gerichtet. Die Zahlungstransaktion selbst ist gerade nicht betroffen, sodass der Anwendungsbereich der PSD 2 im Fall derartiger betrügerischer Aktionen **vor** der Zahlung nicht eröffnet ist. Auch wird die Motivation des Zahlers nicht durch die PSD 2 geschützt. Dies entspricht auch dem Sinn und Zweck der PSD 2, da derartige Sachverhalte gerade **kein technisches Risiko für den Zahlungsmarkt** darstellen. Tatsächlich unterliegen derartige betrügerische Manipulationen, die auf das geistige Bild bzw. die Vorstellung des Zahlers einwirken, den allgemeinen strafrechtlichen Bestimmungen.

c) Vergleichsweise, ist es bei der Überwachung von Zahlungsmärkten in Fällen von **nicht autorisierten Transaktionen** gerade nicht von Bedeutung, ob der Betrüger das Zahlungsinstrument geraubt, gestohlen oder einfach nur gefunden hat. Die Transaktion selbst ist nicht autorisiert und folglich eine betrügerische Transaktion durch einen Dritten zu Lasten des Karteninhabers – unabhängig von der im Einzelfall begangenen Straftat.

d) Im Gegensatz dazu sollten Fälle, in denen sich z.B. Betrüger (i) als Verwandte älterer Menschen (ii) oder als CEO einer Buchhaltungskraft gegenüber ausgeben und diese manipuliert werden, Geld auf ein fremdes Konto zu überweisen, keineswegs als Betrug bei Überwachung von **Zahlungstransaktionen**, sondern als Straftat klassifiziert und mit den allgemeinen Mitteln des Rechtsstaats sanktioniert werden. Dies allerdings jenseits des Anwendungsbereichs der PSD 2.

e) Ein weiterer Grund für die Nichtanwendung des Betrugsmeldewesens auf Fälle der "Manipulation des Zahlers" ist der Umstand, dass es den Zahlungsdienstleistern unmöglich ist, diesen Betrugsaktivitäten durch SKA oder durch Authentifizierung mit an-

deren Sicherheitsstandards vorzubeugen, weil diese Zahlungstransaktionen in der Tat **ordnungsgemäß durch den Zahler autorisiert und ggf. authentifiziert** wurden, der wiederum durch den Betrüger getäuscht bzw. betrogen wurde, die Transaktion durchzuführen. Dies ist vielmehr ein allgemeines Kriminalitätsrisiko und nicht ein technisch bedingtes Sicherheitsrisiko des Zahlungsmarkts. Daneben ist es den Zahlungsdienstleistern nicht möglich, persönliche Manipulationen des Zahlers festzustellen und entsprechend zu berichten.

f) Die Einbeziehung von ordnungsgemäß erteilten Transaktionen (wie beim „CEO-Fraud“) unter die Meldepflichten würde daher zu einer verzerrten Einschätzung der Effektivität von SKA führen. Auch sieht der Markt in der Einbeziehung derartiger Transaktionen unter die Meldepflichten des Betrugsmeldewesens eine Ausweitung des Anwendungsbereichs der PSD 2 (vgl. Referenz-Nummer 41 des Response Table der EBA GL).

g) Zahlungsbetrug und Fälle des sog. „CEO fraud“ sind zwei völlig unterschiedliche Bereiche und sollten dementsprechend auch nicht für regulatorische Zwecke vermischt werden. Wie bereits ausgeführt, findet „CEO fraud“ durch betrügerisches Einwirken auf die Motivation des Bezahlers, und gerade nicht mittels Angriff auf die Zahlungstransaktion selbst oder auf die Verarbeitung von Daten im Zusammenhang mit der Autorisierung oder Authentifikation der Zahlung, statt. Ausschließlich Letzteres sollte in statistische Beobachtungen in Bezug auf Zahlungsbetrug einbezogen werden, andere kriminelle Tätigkeiten jenseits der Zahlungstransaktionskette hingegen nicht. Denn wie bereits erläutert, können derartige kriminelle, betrügerische Aktivitäten keineswegs durch Anwendung von irgendeinem Sicherheitslevel vermieden werden, sondern nur durch Information der Verbraucher durch allgemeine verbraucherschützende Medien, wie z.B. „Aktenzeichen XY“ oder Berichte über Verbraucherfallen. Dort sind allerdings nicht die Zahlungsinstrumente zu verbessern, sondern der Selbstschutz der Verbraucher vor allgemeinen Lebens- und Betrugsrisiken.

h) Des Weiteren sollte im Rahmen der deutschen Verwaltungspraxis durch die BaFin berücksichtigt werden, dass nicht jeder Konflikt zwischen Zahler und Zahlungsempfänger im Zusammenhang mit der zugrundeliegenden Transaktion als Betrug oder betrügerische Transaktion anzusehen ist. Dies wurde auch durch die EBA im Rahmen der Konsultation der EBA GL bestätigt (vgl. Referenz-Nummer 54 des Response Table der EBA GL). Wie bereits im Zusammenhang mit dem Betrugstyp der “Manipulation des Zahlers” erläutert, sollten sämtliche Umstände und Geschehnisse, die über die Zahlungstransaktion, deren Autorisierung und Authentifizierung hinaus gehen, klar vom Begriff des Zahlungsbetrugs abgegrenzt werden. Dies ist insbesondere für „Umtausch- oder Reklamationsfälle“ wichtig, denen stets ordnungsgemäß autorisierte Zahlungstransaktionen, aber ggf. mangelhafte Sachleistungen oder allgemeine Unzufriedenheit der Käufer zu Grunde liegen. Derartige „Retouren“ oder sonstige Leistungsstörungen aus dem Kauf-Grundverhältnis dürfen ebenfalls nicht mit dem Betrugsbegriff, der sich auf eine Zahlungstransaktion bezieht, vermischt werden, wobei weitgehend die glei-

chen Argumente zur Anwendung kommen, wie beim „CEO-Fraud“, v.a. die Unmöglichkeit der Zahlungsdienstleister, solche Leistungsstörungen zu verhindern.

i) Da Betrugsbegriff und Betrugsstatistik nicht nur eine folgenlose statistische Meldung betreffen, sondern bei Anwendung der Ausnahmen zur SKA-Pflicht wie den risikobasierten Ausnahmen nach Art. 18 RTS gerade auch sehr materielle Geschäftsauswirkung haben, dürfen nur Betrugsfälle melderelevant sein, die unter einer operationellen Kontrolle des jeweiligen Zahlungsdienstleisters stattfinden. Anderenfalls würden einem Zahlungsdienstleister statistisch Betrugsfälle zur Last fallen – und damit ggf. die Anwendung von SKA-Ausnahmen nach Art. 18 RTS ausschließen – obwohl der jeweilige Zahlungsdienstleister in keiner Weise dagegen etwas unternehmen kann, da der Betrug nicht aus dem Umfeld seines jeweiligen Kunden stammt. So kann ein Kartenacquirer nichts bei Betrugsfällen eines Karteninhabers unternehmen (da nicht sein Kunde) und andererseits kann ein Kartenissuer nichts bei Betrug eines Händlers unternehmen (da nicht sein Kunde, sondern Kunde des Acquirers).

2. Sofern die BaFin, entgegen der Auffassung der IK, den Betrugstyp der “Manipulation des Zahlers” in die deutsche Verwaltungspraxis übertragen möchte, empfiehlt die IK im Rahmen der Verwaltungspraxis klarzustellen, dass entsprechende Meldepflichten im Zusammenhang mit diesem Betrugstyp nur auf Cyber-Attacken oder Manipulationen von IT-Systemen **unter der Kontrolle des Zahlungsdienstleisters des Zahlers** bezogen werden, bei denen eine Zahlungstransaktion eines Zahlers technisch so manipuliert wird, dass eine Zahlung an einen Betrüger erfolgen würde, ohne dass der Zahler dies erkennt oder bewusst wahrnimmt. Es muss darauf hingewiesen werden, dass nur diejenigen **Manipulationen von Systemen oder Mechanismen**, die von dem Zahlungsdienstleister des Zahlers verwendet oder kontrolliert werden, als zusätzlicher Betrugstyp angesehen werden können – jenseits von unautorisierten Transaktionen durch betrügende Dritte oder betrügerischen Transaktionen des Zahlers selbst (Betrug des Zahlungsdienstleisters durch den Zahler). Wie bereits zuvor ausgeführt, stellt hingegen die bloße Täuschung eines Zahlers durch einen Betrüger, mit dem Ergebnis, dass der Zahler einem Irrtum unterliegt, auf dessen Grundlage er eine Zahlung wirksamen autorisiert, keinen „Zahlungsbetrug“, sondern einen “Motivationsbetrug“ dar.

Gerne erläutern wir weitere Hintergründe zu dieser Stellungnahme noch in einem persönlichen Gespräch.

Mit freundlichen Grüßen

Für die IK (Interessengemeinschaft Kreditkartengeschäft):

Dr. Markus Escher
Rechtsanwalt