EBA/GL/2018/05

17/09/2018

# Leitlinien

# über die Anforderungen an die Meldung von Betrugsfällen gemäß Artikel 96 Absatz 6 der Richtlinie (EU) 2015/2366 (PSD2)

# 1. Verpflichtung zur Einhaltung der Leitlinien und Meldepflichten

## Status dieser Leitlinien

1. Das vorliegende Dokument enthält Leitlinien, die gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 herausgegeben wurden.[1] Gemäß Artikel 16 Artikel 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden und Finanzinstitute alle erforderlichen Anstrengungen unternehmen, um diesen Leitlinien nachzukommen.

2. Die Leitlinien legen fest, was nach Ansicht der EBA angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind oder wie das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Dazu sollten die zuständigen Behörden gemäß Artikel 2 Absatz 4 der Verordnung (EU) Nr. 1093/2010 die an sie gerichteten Leitlinien in geeigneter Weise in ihre Aufsichtspraktiken (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren) integrieren, einschließlich der Leitlinien in diesem Dokument, die in erster Linie an Institute gerichtet sind.

## Meldepflichten

3. Nach Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden der EBA bis zum 19.11.2018 mitteilen, ob sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen, oder die Gründe nennen, warum sie dies nicht tun. Geht innerhalb der genannten Frist keine Mitteilung ein, geht die EBA davon aus, dass die zuständige Behörde den Anforderungen nicht nachkommt. Die Mitteilungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/GL/2018/05“ an compliance@eba.europa.eu zu senden. Die Mitteilungen sollten durch Personen erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer Behörde zu übermitteln. Jegliche Änderungen des Status der Einhaltung müssen der EBA ebenfalls gemeldet werden.

4. Die Meldungen werden gemäß Artikel 16 Absatz 3 der EBA-Verordnung auf der Website der EBA veröffentlicht.

[1] 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 (ABl. L 331 vom 15.12.2010, S. 12).

# 2. Gegenstand, Anwendungsbereich und Begriffsbestimmungen

## Gegenstand

5. Diese Leitlinien enthalten detaillierte Angaben zu statistischen Daten über Betrug in Verbindung mit unterschiedlichen Zahlungsmitteln, die Zahlungsdienstleister ihren zuständigen Behörden melden müssen, sowie zu den aggregierten Daten, welche die zuständigen Behörden gemäß Artikel 96 Absatz 6 der Richtlinie (EU) 2015/2366 (PSD2) der EBA und der EZB zur Verfügung stellen müssen.

## Anwendungsbereich

6. Diese Leitlinien gelten für die Meldung von Zahlungsdienstleistern an die zuständigen Behörden im Zusammenhang mit statistischen Daten zu Betrug bei Zahlungsvorgängen, die ausgelöst und ausgeführt (gegebenenfalls auch angenommen und abgerechnet) worden sind, einschließlich der Annahme und Abrechnung (Acquiring) von Zahlungsvorgängen für Kartenzahlungen, die anhand folgender Kriterien ermittelt werden: (a) betrügerische Zahlungsvorgangsdaten über einen festgelegten Zeitraum und (b) Zahlungsvorgänge in demselben festgelegten Zeitraum.

7. Die im Rahmen der Aufschlüsselung der Überweisungen gemeldeten Daten sollten Überweisungen von Geldausgabeautomaten mit Überweisungsfunktion umfassen. Überweisungen, die zum Ausgleich ausstehender Salden von Vorgängen unter Nutzung von Karten mit einer Kredit- oder einer „verzögerten“ Debitfunktion verwendet werden, sollten ebenfalls erfasst sein.

8. Die im Rahmen der Aufschlüsselung von Lastschriftverfahren erfassten Daten sollten Lastschriften umfassen, die zum Ausgleichausstehender Salden von Vorgängen unter Nutzung von Karten mit einer Kredit- oder einer „verzögerten“ Debitfunktion verwendet werden.

9. Die im Rahmen der Aufschlüsselung von Kartenzahlungen gemeldeten Daten sollten Daten zu allen Zahlungsvorgängen (elektronisch und nicht elektronisch) mit Zahlungskarten umfassen. Zahlungen mit Karten nur mit E-Geld-Funktion (z. B. Prepaid-Karten) sollten nicht in Kartenzahlungen umfasst, sondern als E-Geld gemeldet werden.

10. In diesen Leitlinien wird auch dargelegt, wie die zuständigen Behörden die in Absatz 6 genannten Daten aggregieren sollten, die der EZB und der EBA gemäß Artikel 96 Absatz 6 PSD2 zur Verfügung zu stellen sind.

11. Die Leitlinien unterliegen dem Grundsatz der Verhältnismäßigkeit, d. h. alle Zahlungsdienstleister, die in den Anwendungsbereich der Leitlinien fallen, müssen die Anforderungen jeder einzelnen Leitlinie erfüllen, die konkreten Anforderungen, einschließlich

der Berichtsfrequenz, können jedoch je nach verwendetem Zahlungsinstrument, Art der erbrachten Dienstleistungen oder Größe des Zahlungsdienstleisters abweichen.

## Adressaten

12. Die vorliegenden Leitlinien richten sich an:

- Zahlungsdienstleister im Sinne von Artikel 4 Absatz 11 der Richtlinie (EU) 2015/2366 (PSD2) sowie in der Definition von „Finanzinstitute“ in Artikel 4 Absatz 1 der Verordnung (EU) Nr. 1093/2010 in Bezug genommen, mit Ausnahme von Kontoinformationsdienstleistern, und

- Zuständige Behörden im Sinne von Artikel 4 Absatz 2 Punkt I der Verordnung (EU) Nr. 1093/2010.

## Begriffsbestimmungen

13. Soweit nicht anderweitig festgelegt haben die in der Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge, in der Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro, in der Richtlinie (EU) 2015/2366 vom 25. November 2015 über Zahlungsdienste im Binnenmarkt und in der Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten verwendeten Begriffe in diesen Leitlinien dieselbe Bedeutung.

## Geltungsbeginn

14. Diese Leitlinien gelten ab 1. Januar 2019, mit Ausnahme der Meldung von Daten im Zusammenhang mit den Ausnahmen von der Verpflichtung zur Verwendung einer starken Kundenauthentifizierung gemäß der Delegierten Verordnung (EU) 2018/389 der Kommission zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation, die ab dem 14. September 2019 gelten werden. ►A1Die Daten zu diesen Ausnahmen sind in Anhang 2 unter den Datenaufschlüsselungen A (1.3.1.2.4 bis 1.3.1.2.9 und *1.3.2.2.4 bis 1.3.2.2.8*), C (3.2.1.3.4 bis 3.2.1.3.10 und 3.2.2.3.4 bis 3.2.3.3.8), D (4.2.1.3.4 und 4.2.1.3.8 und *4.2.2.3.4 bis 4.2.2.3.7*) und F (6.1.2.4 bis 6.1.2.11 und 6.2.2.4 bis 6.2.2.8) aufgeführt.

# 3.1. Leitlinien zur Verpflichtung von Zahlungsdienstleistern zur Meldung von Betrugsfällen

## Leitlinie 1 Zahlungsvorgänge und betrügerische Zahlungsvorgänge

1.1 Für die Meldung statistischer Daten über Betrug gemäß diesen Leitlinien sollte der Zahlungsdienstleister für jeden Berichtszeitraum folgende Angaben machen:

a. Vorgenommene nicht autorisierte Zahlungsvorgänge, auch infolge von Verlust, Diebstahl oder missbräuchlicher Verwendung sensibler Zahlungsdaten oder eines Zahlungsinstruments, unabhängig davon, ob sie für den Zahler vor der Zahlung erkennbar waren, durch grobe Fahrlässigkeit des Zahlers herbeigeführt oder ohne Zustimmung des Zahlers durchgeführt worden sind ( „nicht autorisierte Zahlungsvorgänge“) und

b. Zahlungsvorgänge, die dadurch erfolgen, dass der Betrüger den Zahler mit dem Ziel der Erteilung eines Zahlungsauftrags oder der entsprechenden Anweisung an den Zahlungsdienstleister manipuliert hat, die Zahlung in gutem Glauben auf ein Zahlungskonto zu leisten, das nach seiner Auffassung zu einem rechtmäßigen Zahlungsempfänger gehört („Manipulation des Zahlers“).

1.2 Für die Zwecke der Leitlinie 1.1 sollte der Zahlungsdienstleister (gegebenenfalls einschließlich des Zahlungskartenemittenten) nur Zahlungsvorgänge melden, die ausgelöst und ausgeführt (gegebenenfalls auch angenommen und abgerechnet) worden sind. Der Zahlungsdienstleister sollte keine Daten zu Zahlungsvorgängen melden, auch wenn sie mit den in Leitlinie 1.1 genannten Umständen verbunden sind, nicht ausgeführt worden sind und nicht zu einem Transfer von Geldbeträgen gemäß den PSD2-Bestimmungen geführt haben.

1.3 Bei Finanztransfers, bei denen Geldbeträge von einem Zahlungsdienstleister des Zahlers an den Finanztransferdienstleister eines Zahlers übertragen wurden (als Bestandteil eines Finanztransfer-Zahlungsvorgangs), ist der Zahlungsdienstleister des Zahlers (und nicht der Finanztransferdienstleister) derjenige, der die Zahlungsvorgänge vom Zahlungsdienstleister des Zahlers an den Finanztransferdienstleister melden sollte. Solche Zahlungsvorgänge sollten nicht vom Zahlungsdienstleister des Begünstigten des Finanztransfervorgangs gemeldet werden.

1.4 Zahlungsvorgänge und betrügerische Zahlungsvorgänge, bei denen ein Finanztransferdienstleister Geldbeträge von seinen Konten auf ein Empfängerkonto überwiesen hat, auch durch Verrechnung des Werts mehrerer Zahlungsvorgänge

(Nettingvereinbarungen), sollte der Finanztransferdienstleister gemäß Datenaufschlüsselung G in Anhang 2 melden.

1.5 Zahlungsvorgänge und betrügerische Zahlungsvorgänge, bei denen E-Geld von einem E-Geld-Anbieter an ein Empfängerkonto überwiesen wurde, einschließlich der Fälle, bei denen der Zahlungsdienstleister des Zahlers mit dem Zahlungsdienstleister des Zahlungsempfängers identisch ist, sollte der E-Geld-Anbieter gemäß Datenaufschlüsselung F im Anhang 2 melden. Sind die Zahlungsdienstleister nicht identisch, so wird die Zahlung nur vom Zahlungsdienstleister des Zahlers gemeldet, um Doppelzählungen zu vermeiden.

1.6 Die Zahlungsdienstleister sollten alle Zahlungsvorgänge und betrügerischen Zahlungsvorgänge wie folgt melden:

a. „Betrügerische Zahlungsvorgänge insgesamt“ bezieht sich auf alle in der Leitlinie 1.1 genannten Zahlungsvorgänge, unabhängig davon, ob der Betrag des betrügerischen Zahlungsvorgangs wiedererlangt worden ist.

b. „Verluste aufgrund von Betrug je Haftungsträger“ bezieht sich auf die Verluste des meldenden Zahlungsdienstleisters, seiner Zahlungsdienstnutzer oder Dritten, und spiegelt die tatsächlichen Auswirkungen des Betrugs auf einer Cashflow-Basis wider. Da die Verbuchung der zu tragenden finanziellen Verluste zeitlich von den eigentlichen betrügerischen Vorgängen getrennt sein könnte, und zur Vermeidung von Revisionen der gemeldeten Daten allein aufgrund dieser immanenten zeitlichen Verzögerung, sollten die endgültigen Betrugsverluste in dem Zeitraum gemeldet werden, in dem sie in den Büchern des Zahlungsdienstleisters verbucht werden. Bei den endgültigen Zahlen zu Betrugsfällen sollten Erstattungen von Versicherungsunternehmen nicht berücksichtigt werden, da sie nicht im Zusammenhang mit der Betrugsprävention im Sinne von PSD2 stehen.

c. „Änderung eines Zahlungsauftrags durch den Betrüger“ ist eine Art nicht autorisierter Zahlungsvorgang im Sinne der Leitlinie 1.1 Buchstabe a und bezieht sich auf eine Situation, in der der Betrüger während der elektronischen Kommunikation zwischen dem Gerät des Zahlers und dem Zahlungsdienstleister (z. B. durch Schadprogramme oder Angriffe, durch welche die Angreifer die Kommunikation zwischen zwei rechtmäßig kommunizierenden Hosts abhören können (Man-in-the-Middle-Angriffe)) einen rechtmäßigen Zahlungsauftrag abfängt und ändert oder den Zahlungsauftrag im System des Zahlungsdienstleisters ändert, bevor der Zahlungsauftrag freigegeben und durchgeführt wird.

d. „Erteilung eines Zahlungsauftrags durch den Betrüger“ ist eine Art nicht autorisierter Zahlungsvorgang im Sinne der Leitlinie 1.1 Buchstabe a und bezieht sich auf eine Situation, in der ein gefälschter Zahlungsauftrag vom Betrüger erteilt wird, nachdem er die sensiblen Zahlungsdaten des Zahlers/Zahlungsempfängers in betrügerischer Weise erhalten hat.

## Leitlinie 2 Allgemeine Datenanforderungen

2.1 Der Zahlungsdienstleister sollte statistische Daten über Folgendes vorlegen:

a. Gesamte Zahlungsvorgänge im Einklang mit den verschiedenen Aufschlüsselungen in Anhang 2 und gemäß Leitlinie 1 und

b. Gesamte betrügerische Zahlungsvorgänge im Einklang mit den verschiedenen Aufschlüsselungen in Anhang 2 und gemäß der Definition in Leitlinie 1.6 Buchstabe a.

2.2 Der Zahlungsdienstleister sollte die in Leitlinie 2.1 genannten statistischen Angaben in Bezug auf sowohl das Volumen (d. h. die Anzahl der Zahlungsvorgänge oder betrügerischen Zahlungsvorgänge) als auch den Wert (d. h. Betrag der Zahlungsvorgänge oder betrügerischen Zahlungsvorgänge) melden. Sie sollten Volumina und Werte in tatsächlichen Einheiten mit zwei Dezimalstellen für Werte angeben.

2.3 Ein in einem Mitgliedstaat der Eurozone autorisierter Zahlungsanbieter oder eine dort niedergelassene Zweigstelle sollte die Werte in Euro angeben, während ein in einem Mitgliedstaat außerhalb der Eurozone autorisierter Zahlungsdienstleister oder eine dort niedergelassene Zweigstelle die Werte in der Währung dieses Mitgliedstaats angeben sollte. Die meldenden Zahlungsdienstleister sollten die Daten für Werte von Vorgängen oder betrügerischen Vorgängen in einer anderen Währung als dem Eurooder der offiziellen Währung des betreffenden Mitgliedstaats in die Währung konvertieren, in der sie die Meldung abgeben, und zwar unter Verwendung der für diese Zahlungsvorgänge geltenden Wechselkurse oder des durchschnittlichen Referenzwechselkurses der EZB für den betreffenden Berichtszeitraum.

2.4 Der Zahlungsdienstleister sollte nur Zahlungsvorgänge melden, die ausgeführt worden sind, einschließlich der Zahlungsvorgänge, die von einem Zahlungsauslösedienstleister ausgelöst worden sind. Verhinderte betrügerische Zahlungsvorgänge, die aufgrund eines Betrugsverdachts vor ihrer Ausführung blockiert werden, sollten nicht berücksichtigt werden.

2.5 Der Zahlungsdienstleister sollte die statistischen Daten mit einer Aufschlüsselung gemäß den in Leitlinie 7 aufgeführten und in Anhang 2 zusammengestellten Aufschlüsselungen melden.

2.6 Der Zahlungsdienstleister sollte die jeweils zutreffenden Datenaufschlüsselung(en) je nach den bereitgestellten Zahlungsdienst(en) und Zahlungsinstrument(en) angeben und die entsprechenden Daten der zuständigen Behörde übermitteln.

2.7 Der Zahlungsdienstleister sollte sicherstellen, dass alle der zuständigen Behörde gemeldeten Daten gemäß Anhang 2 mit Querverweisen versehen werden können.

2.8 Der Zahlungsdienstleister sollte jeden Zahlungsvorgang jeweils nur einer Unterkategorie in jeder Zeile jeder Datenaufschlüsselung zuordnen.

2.9 Falls eine Reihe von Zahlungsvorgängen oder eine Reihe von betrügerischen Zahlungsvorgängen ausgeführt wird, so sollte der Zahlungsdienstleister jeden Zahlungsvorgang oder betrügerischen Zahlungsvorgang der Reihe einzeln berücksichtigen.

2.10 Der Zahlungsdienstleister kann Null („0“) melden, wenn im Berichtszeitraum keine Zahlungsvorgänge oder betrügerischen Zahlungsvorgänge für einen bestimmten Indikator stattgefunden haben. Wenn der Zahlungsdienstleister keine Daten für eine bestimmte Aufschlüsselung melden kann, weil diese bestimmte Datenaufschlüsselung für ihn nicht anwendbar ist, sollten die Daten als „NA“ gemeldet werden.

2.11 Um eine Doppelzählung zu vermeiden, sollte der Zahlungsdienstleister des Zahlers Daten in seiner Emittenten- (oder Auslöser-) Funktion übermitteln. Abweichend davon sollten die Daten für Kartenzahlungen sowohl vom Zahlungsdienstleister des Zahlers als auch vom Zahlungsdienstleister des Zahlungsempfängers gemeldet werden, der den Zahlungsvorgang annimmt und abrechnet. Die beiden Perspektiven sollten getrennt und mit verschiedenen Aufschlüsselungen gemäß Anhang 2 gemeldet werden. Gibt es mehr als einen annehmenden und abrechnenden Zahlungsdienstleister, sollte der Dienstleister, der in einem Vertragsverhältnis zum Zahlungsempfänger steht, die Meldung vorlegen. Darüber hinaus müssen Lastschriftvorgänge vom Zahlungsdienstleister des Zahlungsempfängers gemeldet werden, da diese Zahlungsvorgänge vom Zahlungsempfänger ausgelöst werden.

2.12 Um eine Doppelzählung bei der Berechnung der gesamten Zahlungsvorgänge und betrügerischen Zahlungsvorgänge bei allen Zahlungsinstrumenten zu vermeiden, sollte der Zahlungsdienstleister , der die von einem Zahlungsauslösedienstleister ausgelösten Überweisungen ausführt, bei der Meldung gemäß Datenaufschlüsselung A angeben, wie sich das Volumen und der Wert der gesamten Zahlungsvorgänge und betrügerischen Zahlungsvorgänge, die über einen Zahlungsauslösedienstleister ausgelöst wurden, aufteilen.

## Leitlinie 3 Häufigkeit, Berichtsfrist und Berichtszeitraum

3.1. Der Zahlungsdienstleister sollte die Daten auf der Grundlage der in Anhang 2 aufgeführten Datenaufschlüsselung(en) alle sechs Monate melden.

3.2. Die Zahlungsdienstleister, die eine Ausnahme nach Artikel 32 PSD2 in Anspruch nehmen können, und die E-Geld-Institute, die die Ausnahme nach Artikel 9 der Richtlinie 2009/110/EG über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten in Anspruch nehmen können, sollten nur die Daten melden, die im Rahmen des (der) anwendbaren Formulars (Formulare) in Anhang 2 verlangt werden, und zwar auf Jahresbasis mit Daten, die in zwei Zeiträume von sechs Monaten aufgeschlüsselt sind.

3.3. Der Zahlungsdienstleister sollte die Daten innerhalb der von den jeweils zuständigen Behörden festgelegten Fristen übermitteln.

## Leitlinie 4 Geografische Aufschlüsselung

4.1 Der Zahlungsdienstleister sollte Daten für inländische Zahlungsvorgänge, grenzüberschreitende Zahlungsvorgänge innerhalb des Europäischen Wirtschaftsraums (EWR) und grenzüberschreitende Zahlungsvorgänge außerhalb des EWR melden.

4.2 Bei nicht kartengebundenen Zahlungsvorgängen und kartengebundenen Fernzahlungsvorgängen beziehen sich „inländische Zahlungsvorgänge“ auf Zahlungsvorgänge, die von einem Zahler oder von einem oder über einen Zahlungsempfänger ausgelöst werden, wenn der Zahlungsdienstleister des Zahlers und der Zahlungsdienstleister des Zahlungsempfängers in demselben Mitgliedstaat ansässig sind.

4.3 Bei kartengebundenen Nicht-Fernzahlungsvorgängen beziehen sich „inländische Zahlungsvorgänge“ auf Zahlungsvorgänge, bei denen der Zahlungsdienstleister des Zahlers (Emittent), der Zahlungsdienstleister des Zahlungsempfängers (Acquirer) und die verwendete Verkaufsstelle (POS) bzw. der verwendete Geldautomat (ATM) im selben Mitgliedstaat gelegen sind.

4.4 Bei Zweigstellen im EWR beziehen sich inländische Zahlungsvorgänge auf Zahlungsvorgänge, bei denen sowohl der Zahlungsdienstleister des Zahlers als auch der des Zahlungsempfängers in dem Aufnahmemitgliedstaat, in dem die Zweigniederlassung niedergelassen ist, ansässig sind.

4.5 Bei nicht kartengebundenen Zahlungsvorgängen und kartengebundenen Fernzahlungsvorgängen bezieht sich „grenzüberschreitender Zahlungsvorgang innerhalb des EWR“ auf einen Zahlungsvorgang, der von einem Zahler oder von einem oder über einen Zahlungsempfänger ausgelöst wird, wenn der Zahlungsdienstleister des Zahlers und der Zahlungsdienstleister des Zahlungsempfängers in verschiedenen Mitgliedstaaten ansässig sind.

4.6 Bei kartengebundenen Nicht-Fernzahlungsvorgängen beziehen sich „grenzüberschreitende Zahlungsvorgänge innerhalb des EWR“ auf Zahlungsvorgänge, bei denen der Zahlungsdienstleister des Zahlers (Emittent) und der Zahlungsdienstleister des Zahlungsempfängers (Acquirer) sich in verschiedenen Mitgliedstaaten befinden oder der Zahlungsdienstleister des Zahlers (Emittent) seinen Sitz in einem anderen Mitgliedstaat als dem der Verkaufsstelle oder des Geldautomaten hat.

4.7 „Grenzüberschreitende Zahlungsvorgänge außerhalb des EWR“ beziehen sich auf Zahlungsvorgänge, die von einem Zahler oder von einem oder über einen Zahlungsempfänger ausgelöst werden und bei denen der Zahlungsdienstleister entweder des Zahlers oder des Zahlungsempfängers seinen Sitz außerhalb des EWR hat, während der andere seinen Sitz im EWR hat.

4.8 Ein Zahlungsdienstleister, der Zahlungsauslösedienste anbietet, sollte die von ihm ausgelösten ausgeführten Zahlungsvorgänge und die von ihm ausgelösten ausgeführten betrügerischen Zahlungsvorgänge gemäß den folgenden Vorgaben melden:

a. „Inländische Zahlungsvorgänge“ beziehen sich auf Zahlungsvorgänge, bei denen der Zahlungsauslösedienstleister und der kontoführende Zahlungsdienstleister ihren Sitz in demselben Mitgliedstaat haben,

b. „Grenzüberschreitende Zahlungsvorgänge innerhalb des EWR“ beziehen sich auf Zahlungsvorgänge, bei denen der Zahlungsauslösedienstleister und der kontoführende Zahlungsdienstleister in verschiedenen Mitgliedstaaten ansässig sind;

c. „Grenzüberschreitende Zahlungsvorgänge außerhalb des EWR“ beziehen sich auf Zahlungsvorgänge, bei denen der Zahlungsauslösedienstleister innerhalb des EWR ansässig ist und der kontoführende Zahlungsdienstleister außerhalb des EWR ansässig ist.

## Leitlinie 5 Meldung an die zuständige Behörde

5.1. Der Zahlungsdienstleister soll an die zuständige Behörde des Herkunftsmitgliedstaats melden.

5.2. Der Zahlungsdienstleister sollte Daten von all seinen Agenten aufzeichnen, die Zahlungsdienstleistungen im EWR erbringen, und diese Daten mit den übrigen Daten zusammenführen, bevor er sie der zuständigen Herkunftslandbehörde übermittelt. Dabei spielt der Standort des Agenten für die Bestimmung der geografischen Perspektive keine Rolle.

5.3. Im Rahmen der Überwachung und Berichterstattung gemäß Artikel 29 Absatz 2 PSD2 und Artikel 40 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen sollte eine Zweigstelle eines EWR-Zahlungsdienstleisters der zuständigen Behörde des Aufnahmemitgliedstaats, in dem sie niedergelassen ist, getrennt von den Berichtsdaten des Zahlungsdienstleisters des Herkunftsmitgliedstaats Bericht erstatten.

5.4. Bei der Übermittlung der Daten an die entsprechende zuständige Behörde sollte ein Zahlungsdienstleister die in Anhang 1 genannten Identifikationsangaben vorlegen.

## Leitlinie 6 Aufzeichnungs-/Bezugsdaten

6.1 Das von den Zahlungsdienstleistern für die Buchung von Zahlungsvorgängen und betrügerischen Zahlungsvorgängen zum Zweck dieser statistischen Berichterstattung zu berücksichtigende Datum ist der Tag, an dem der Zahlungsvorgang gemäß PSD2 ausgeführt wurde. Bei einer Reihe von Vorgängen sollte das aufgezeichnete Datum das Datum sein, an dem jeder einzelne Zahlungsvorgang ausgeführt wurde.

6.2 Der Zahlungsdienstleister sollte alle betrügerischen Zahlungsvorgänge ab dem Zeitpunkt der Feststellung des Betrugs (z. B. durch eine Kundenbeschwerde oder andere Mittel) melden.

Dabei spielt es keine Rolle, ob der Fall, der mit dem betrügerischen Zahlungsvorgang in Zusammenhang steht, bis zum Zeitpunkt der Datenmeldung abgeschlossen ist.

6.3 Der Zahlungsdienstleister sollte alle Anpassungen der Daten melden, die sich auf einen beliebigen vorangegangenen Berichtszeitraum beziehen, der mindestens ein Jahr zurückliegt, und zwar während des nächsten Berichtsfensters, nachdem die Informationen, die eine Anpassung erfordert haben, ermittelt worden waren. Er sollte darauf hinweisen, dass es sich bei den gemeldeten Daten um überarbeitete Zahlen für den vergangenen Zeitraum handelt, und sollte diese Überarbeitung nach der von der jeweils zuständigen Behörde festgelegten Methode melden.

## Leitlinie 7 Datenaufschlüsselung

7.1 Bei E-Geld-Zahlungsvorgängen im Sinne der Richtlinie 2009/110/EG sollte der Zahlungsdienstleister Daten gemäß Aufschlüsselung F in Anhang 2 vorlegen.

7.2 Bei der Bereitstellung von Daten über E-Geld-Zahlungsvorgänge sollte der Zahlungsdienstleister E-Geld-Zahlungsvorgänge berücksichtigen,

a. wenn der Zahlungsdienstleister des Zahlers mit dem Zahlungsdienstleister des Zahlungsempfängers identisch ist oder

b. wenn eine Karte mit E-Geld-Funktionalität verwendet wird.

7.3 Für die Zwecke von E-Geld-Zahlungsvorgängen sollte der Zahlungsdienstleister Daten zu den Volumina und Werten aller Zahlungsvorgänge sowie zu den Volumina und Werten betrügerischer Zahlungsvorgänge mit den folgenden Aufschlüsselungen melden:

a. geografische Perspektive,

b. Zahlungsweg,

c. Authentifizierungsmethode,

d. Grund für die Nichtanwendung einer starken Kundenauthentifizierung (unter Bezugnahme auf die Ausnahmen für eine starke Kundenauthentifizierung in Kapitel III der technischen Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation, Delegierte Verordnung (EU) 2018/389 der Kommission►A1 oder ggf. auf eine der beiden Kategorien „Vom Händler ausgelöste Zahlungsvorgänge“ und „Sonstiges“), und

e. Betrugsarten.

7.4 Für Finanztransferleistungen sollte der Zahlungsdienstleister Daten gemäß Datenaufschlüsselung G in Anhang 2 und gemäß Leitlinie 1.3 liefern. Der Zahlungsdienstleister, der diese Dienste anbietet, sollte Daten zu den Volumina und Werten aller Zahlungsvorgänge und betrügerischen Zahlungsvorgänge in Leitlinie 2.1 mit der geografischen Perspektive melden.

7.5 Bei der Erbringung von Zahlungsauslösediensten sollte der Zahlungsdienstleister Daten nach Datenaufschlüsselung H in Anhang 2 vorlegen. Der Zahlungsdienstleister sollte die von ihm ausgelösten ausgeführten Zahlungsvorgänge und die von ihm ausgelösten betrügerischen Zahlungsvorgänge sowohl volumen- als auch wertmäßig melden.

7.6 Bei Zahlungsvorgängen, die für Datenaufschlüsselung H in Anhang 2 infrage kommen, sollte der Zahlungsdienstleister, der Zahlungsauslösedienste anbietet, Daten zu Volumina und Werten mit den folgenden Aufschlüsselungen aufzeichnen und melden:

a. geografische Perspektive,

b. Zahlungsinstrument,

c. Zahlungsweg und

d. Authentifizierungsmethode.

7.7 Ein Zahlungsdienstleister, der das Konto des Zahlungsdienstnutzers nicht verwaltet, jedoch mit der Ausgabe und Ausführung von kartengebundenen Zahlungen betraut ist (ein Emittent von kartengebundenen Zahlungsinstrumenten), sollte Daten zu Volumina und Werten gemäß Datenaufschlüsselung C bzw. E in Anhang 2 liefern. Werden solche Daten bereitgestellt, so sollte der kontoführende Zahlungsdienstleister sicherstellen, dass solche Zahlungsvorgänge nicht doppelt gemeldet werden.

7.8 Der Zahlungsdienstleister, der Überweisungen und kartengebundene Zahlungsdienste anbietet, sollte in Abhängigkeit von dem Zahlungsinstrument, das für einen bestimmten Zahlungsvorgang verwendet wird, und unter Berücksichtigung der Rolle des Zahlungsdienstleisters Daten gemäß den Datenaufschlüsselungen A, C bzw. D in Anhang 2 liefern. Diese Daten umfassen:

a. geografische Perspektive,

b. Zahlungsweg,

c. Authentifizierungsmethode,

d. Grund für die Nichtanwendung einer starken Kundenauthentifizierung (unter Bezugnahme auf die Ausnahmen für eine starke Kundenauthentifizierung in Kapitel 3 der technischen Regulierungsstandards (RTS) zu starker Kundenauthentifizierung und sicherer Kommunikation, ►**A1** oder ggf. auf eine der beiden Kategorien „Vom Händler ausgelöste Zahlungsvorgänge“ und „Sonstiges“),

e. Betrugsarten,

f. Kartenfunktion für Datenaufschlüsselungen C und D, und

g. über einen Zahlungsauslösedienstleister ausgelöste Zahlungsvorgänge für Datenaufschlüsselung A

7.9 Der Zahlungsdienstleister sollte Daten gemäß Datenaufschlüsselung A in Anhang 2 für alle Zahlungsvorgänge und betrügerischen Zahlungsvorgänge zur Verfügung stellen, welche mithilfe von Überweisungen ausgeführt worden sind.

7.10 Der Zahlungsdienstleister sollte Daten gemäß Datenaufschlüsselung B in Anhang 2 für alle Zahlungsvorgänge und betrügerischen Zahlungsvorgänge zur Verfügung stellen, welche mithilfe von Lastschriftverfahren ausgeführt worden sind. Diese Daten umfassen:

a. geografische Perspektive,

b. den für die Erteilung der Zustimmung verwendeten Kanal und

c. Betrugsarten.

7.11 Der Zahlungsdienstleister sollte Daten nach Datenaufschlüsselung C in Anhang 2 für alle Zahlungsvorgänge und betrügerischen Zahlungsvorgänge auf der Emittentenseite angeben, bei denen eine Zahlungskarte verwendet wurde und der Zahlungsdienstleister der Zahlungsdienstleister des Zahlers war.

7.12 Der Zahlungsdienstleister sollte Daten nach Datenaufschlüsselung D in Anhang 2 für alle Zahlungsvorgänge und betrügerischen Zahlungsvorgänge auf der Acquirer-Seite angeben, bei denen eine Zahlungskarte verwendet wurde und der Zahlungsdienstleister der Zahlungsdienstleister des Zahlungsempfängers war.

7.13 Der Zahlungsdienstleister, der Daten gemäß den Datenaufschlüsselungen A bis F in Anhang 2 liefert, sollte alle Verluste aufgrund von Betrug je Haftungsträger während des Berichtszeitraums angeben.

7.14 Der Zahlungsdienstleister, der Kartenzahlungsvorgänge gemäß den Datenaufschlüsselungen C und D in Anhang 2 meldet, sollte Barabhebungen und Bareinlagen ausschließen.

7.15 Der ausstellende Zahlungsdienstleister (sollte Daten gemäß Datenaufschlüsselung E in Anhang 2 für alle Barabhebungen und betrügerischen Barabhebungen ►**A1** an Geldautomaten (einschließlich über Apps), an Bankschaltern und über Einzelhändler („Cashback“) mithilfe einer Karte liefern.

# 3.2. Leitlinien für die Meldung von aggregierten Betrugsdaten durch die zuständigen Behörden an die EBA und die EZB

## Leitlinie 1 Zahlungsvorgänge und betrügerische Zahlungsvorgänge

1.1. Für die Zwecke der Meldung statistischer Daten über Betrugsfälle an die EBA und die EZB gemäß diesen Leitlinien und gemäß Artikel 96 Absatz 6 PSD2 sollte die zuständige Behörde für jeden Berichtszeitraum Folgendes angeben:

a. Vorgenommene nicht autorisierte Zahlungsvorgänge, auch infolge von Verlust, Diebstahl oder missbräuchlicher Verwendung sensibler Zahlungsdaten oder eines Zahlungsinstruments, ungeachtet dessen, ob sie durch den Zahler vor einer Zahlung erkennbar waren, durch grobe Fahrlässigkeit des Zahlers herbeigeführt wurden oder ohne Zustimmung des Zahlers erfolgt sind (nachstehend „nicht autorisierter Zahlungsvorgang“), und

b. Zahlungsvorgänge, die dadurch erfolgen, dass der Betrüger den Zahler mit dem Ziel der Erteilung eines Zahlungsauftrags oder der entsprechenden Anweisung an den Zahlungsdienstleister manipuliert, die Zahlung in gutem Glauben auf ein Zahlungskonto zu leisten, das nach seiner Auffassung zu einem rechtmäßigen Zahlungsempfänger gehört („Manipulation des Zahlers“).

1.2. Für die Zwecke der Leitlinie 1.1 sollte die zuständige Behörde nur Zahlungsvorgänge melden, die von Zahlungsdienstleistern (gegebenenfalls einschließlich Ausstellern von kartengebundenen Zahlungsinstrumenten) ausgelöst und ausgeführt (gegebenenfalls auch angenommen und abgerechnet) wurden. Die zuständige Behörde sollte keine Daten zu Zahlungsvorgängen melden, die ungeachtet dessen, wie sie an die in Leitlinie 1.1 genannten Umstände geknüpft sind, nicht ausgeführt worden sind und nicht zu einem Transfer von Geldbeträgen gemäß den PSD2-Bestimmungen geführt haben.

1.3. Die zuständige Behörde sollte alle Zahlungsvorgänge und betrügerischen Zahlungsvorgänge wie folgt melden:

a. Bei nicht kartengebundenen Zahlungsvorgängen und kartengebundenen Fernzahlungsvorgängen beziehen sich „inländische Zahlungsvorgänge“ auf Zahlungsvorgänge, die von einem Zahler oder von einem oder über einen Zahlungsempfänger ausgelöst werden, wenn der Zahlungsdienstleister des Zahlers

und der Zahlungsdienstleister des Zahlungsempfängers in demselben Mitgliedstaat ansässig sind.

b. Bei Zweigstellen im EWR beziehen sich inländische Zahlungsvorgänge auf Zahlungsvorgänge, bei denen sowohl der Zahlungsdienstleister des Zahlers als auch der des Zahlungsempfängers in dem Aufnahmemitgliedstaat, in dem die Zweigniederlassung niedergelassen ist, ansässig sind.

c. Bei nicht kartengebundenen Zahlungsvorgängen und kartengebundenen Fernzahlungsvorgängen beziehen sich „grenzüberschreitende Zahlungsvorgänge innerhalb des EWR“ auf Zahlungsvorgänge, die von einem Zahler oder von einem oder über einen Zahlungsempfänger ausgelöst werden, wenn der Zahlungsdienstleister des Zahlers und der Zahlungsdienstleister des Zahlungsempfängers in verschiedenen Mitgliedstaaten ansässig sind.

d. Bei kartengebundenen Nicht-Fernzahlungsvorgängen beziehen sich „inländische Zahlungsvorgänge“ auf Zahlungsvorgänge, bei denen der Zahlungsdienstleister des Zahlers (Emittent), der Zahlungsdienstleister des Zahlungsempfängers (Acquirer) und die Verkaufsstelle (POS) oder der Geldautomat (ATM) im selben Mitgliedstaat gelegen sind. Wenn der Zahlungsdienstleister des Zahlers und der Zahlungsdienstleister des Zahlungsempfängers in verschiedenen Mitgliedstaaten ansässig sind oder der Zahlungsdienstleister des Zahlers (Emittent) sich in einem anderen Mitgliedstaat als die Verkaufsstelle oder der Geldautomat befindet, handelt es sich bei dem Zahlungsvorgang um einen „grenzüberschreitenden Zahlungsvorgang innerhalb des EWR“.

e. „Grenzüberschreitende Zahlungsvorgänge außerhalb des EWR“ beziehen sich auf Zahlungsvorgänge, die von einem Zahler oder von einem oder über einen Zahlungsempfänger ausgelöst werden und bei denen der Zahlungsdienstleister entweder des Zahlers oder des Zahlungsempfängers seinen Sitz außerhalb des EWR hat, während der andere seinen Sitz im EWR hat.

f. „Betrügerische Zahlungsvorgänge insgesamt“ beziehen sich auf alle in der Leitlinie 1.1 genannten Zahlungsvorgänge, ungeachtet dessen, ob der Betrag des betrügerischen Zahlungsvorgangs wiedererlangt worden ist.

g. „Änderung eines Zahlungsauftrags durch den Betrüger“ ist eine Art nicht autorisierter Zahlungsvorgang im Sinne der Leitlinie 1.1 Buchstabe a und bezieht sich auf eine Situation, in der der Betrüger während der elektronischen Kommunikation zwischen dem Gerät des Zahlers und dem Zahlungsdienstleister (z. B. durch Schadprogramme oder Man-in-the-Middle-Angriffe) einen rechtmäßigen Zahlungsauftrag abfängt und ändert oder den Zahlungsauftrag im System des Zahlungsdienstleisters ändert, bevor der Zahlungsauftrag freigegeben und durchgeführt wird.

h. „Erteilung eines Zahlungsauftrags durch den Betrüger“ ist eine Art nicht autorisierter Zahlungsvorgang im Sinne der Leitlinie 1.1 Buchstabe a und bezieht

sich auf eine Situation, in der ein gefälschter Zahlungsauftrag vom Betrüger erteilt wird, nachdem er die sensiblen Zahlungsdaten des Zahlers/Zahlungsempfängers in betrügerischer Weise erhalten hat.

1.4. Die zuständigen Behörden sollten Daten von Zahlungsdienstleistern, die Zahlungsauslösedienste anbieten, wie folgt melden:

a. „Inländische Zahlungsvorgänge“ beziehen sich auf Zahlungsvorgänge, bei denen der Zahlungsauslösedienstleister und der kontoführende Zahlungsdienstleister ihren Sitz in demselben Mitgliedstaat haben.

b. „Grenzüberschreitende Zahlungsvorgänge innerhalb des EWR“ beziehen sich auf Zahlungsvorgänge, bei denen der Zahlungsauslösedienstleister und der kontoführende Zahlungsdienstleister in verschiedenen Mitgliedstaaten ansässig sind.

c. „Grenzüberschreitende Zahlungsvorgänge außerhalb des EWR“ beziehen sich auf Zahlungsvorgänge, bei denen der Zahlungsauslösedienstleister sich innerhalb des EWR befindet und der kontoführende Zahlungsdienstleister sich außerhalb des EWR befindet.

## Leitlinie 2 Datenerhebung und -aggregation

2.1 Die zuständige Behörde sollte statistische Daten über Folgendes übermitteln:

a. Gesamte Zahlungsvorgänge im Einklang mit den verschiedenen Aufschlüsselungen in Anhang 2 und gemäß Leitlinie 1.2 und

b. Gesamte betrügerische Zahlungsvorgänge im Einklang mit den verschiedenen Aufschlüsselungen in Anhang 2 und gemäß der Definition in Leitlinie 1.3 Buchstabe f.

2.2 Die zuständige Behörde sollte die statistischen Daten in Leitlinie 2.1 sowohl in Bezug auf das Volumen (d. h. die Anzahl der Zahlungsvorgänge oder betrügerischen Zahlungsvorgänge) als auch den Wert (d. h. den Betrag der Zahlungsvorgänge oder betrügerischen Zahlungsvorgänge) melden. Sie sollte Volumina und Werte in tatsächlichen Einheiten mit zwei Dezimalstellen für Werte angeben.

2.3 Die zuständige Behörde sollte die Werte in Euro angeben. Sie sollte die Daten für Werte von Vorgängen oder betrügerischen Vorgängen in einer anderen Währung als der Euro-Währung unter Verwendung der für diese Zahlungsvorgänge geltenden Wechselkurse oder des durchschnittlichen Referenzwechselkurses der EZB für den betreffenden Berichtszeitraum konvertieren.

2.4 Die zuständige Behörde kann Null („0“) melden, wenn im Berichtszeitraum keine Zahlungsvorgänge oder betrügerischen Zahlungsvorgänge für einen bestimmten Indikator stattgefunden haben.

2.5 Die zuständige Behörde sollte die in ihrem Mitgliedstaat erhobenen Daten von den Adressaten dieser Leitlinien aggregieren, indem sie die für jeden einzelnen

Zahlungsdienstleister gemeldeten Daten im Einklang mit den Datenaufschlüsselungen in Anhang 2 zusammenfasst.

2.6 Die zuständige Behörde sollte die sicheren Kommunikationsverfahren und das Format für die Meldung der Daten durch die Zahlungsdienstleister festlegen. Die zuständige Behörde sollte auch sicherstellen, dass Zahlungsdienstleistern eine angemessene Frist eingeräumt wird, um die Qualität der Daten zu gewährleisten und die potenzielle Verzögerung bei der Meldung betrügerischer Zahlungsvorgänge zu berücksichtigen.

2.7 Die zuständige Behörde sollte sicherstellen, dass die gemäß diesen Leitlinien gemeldeten Daten mit Querverweisen versehen und von der EBA und der EZB gemäß den Datenaufschlüsselungen in Anhang 2 verwendet werden können.

## Leitlinie 3 Praktische Datenmeldung

3.1 Die zuständige Behörde sollte die Volumina und Werte von Zahlungsvorgängen und betrügerischen Zahlungsvorgängen entsprechend den Leitlinien 2.1 und 2.2 melden. Um Doppelzählungen zu vermeiden, sollten die Daten nicht nach den verschiedenen Datenaufschlüsselungen in Anhang 2 aggregiert werden.

3.2 Die zuständige Behörde sollte Anpassungen der Daten zu allen Zahlungsvorgängen und betrügerischen Zahlungsvorgängen, die in einem beliebigen vergangenen Berichtszeitraum gemeldet wurden, zum nächsten Berichterstattungszeitpunkt melden nachdem die Informationen, die die Anpassungen erforderlich machen, von dem/den betreffenden Zahlungsdienstleister(n) erhalten worden sind, und zwar bis zu 13 Monate, nachdem der Zahlungsvorgang ausgeführt (bzw. angenommen und abgerechnet) wurde, damit der Zahlungsdienstnutzer sein Recht auf Benachrichtigung des Zahlungsdienstleisters bis spätestens 13 Monate nach Ausführung des Vorgangs gemäß Artikel 71 PSD2 ausüben kann.

3.3 Die zuständige Behörde sollte jederzeit sicherstellen, dass die Vertraulichkeit und Integrität der gespeicherten und ausgetauschten Informationen sowie die ordnungsgemäße Identifizierung der Daten bei der Übermittlung der Daten an die EZB und die EBA gewährleistet sind.

3.4 Die zuständige Behörde sollte die aggregierten Daten innerhalb von sechs Monaten ab dem Tag nach dem Ende des Berichtszeitraums an die EZB und die EBA senden.

3.5 Die zuständige Behörde sollte mit der EZB und der EBA die sicheren Kommunikationsverfahren und das spezifische Format, in dem die zuständige Behörde die Daten melden sollte, vereinbaren.

## Leitlinie 4 Zusammenarbeit zwischen zuständigen Behörden

4.1 Gibt es in einem Mitgliedstaat mehr als eine zuständige Behörde gemäß der PSD2, sollten die zuständigen Behörden die Datenerhebung koordinieren, um sicherzustellen, dass der EZB und der EBA nur ein Datensatz für diesen Mitgliedstaat gemeldet wird.

4.2 Auf Anfrage der zuständigen Behörde in einem Herkunftsmitgliedstaat sollte die zuständige Behörde in einem Aufnahmemitgliedstaat Informationen und Daten zur Verfügung stellen, die ihr von Zweigstellen gemeldet worden sind.

# Anhang 1 – Allgemeine Daten, die von allen meldenden Zahlungsdienstleistern bereitzustellen sind

## Allgemeine Angaben zum meldenden Zahlungsdienstleister

**Name:** vollständiger Name des Zahlungsdienstleisters, der dem Verfahren für die Datenmeldung unterliegt, wie er im geltenden nationalen Register für Kreditinstitute, Zahlungsinstitute oder E-Geld-Institute erscheint.

**Eindeutige Identifikationsnummer:** die in jedem Mitgliedstaat verwendete eindeutige Kennnummer zur Identifizierung des Zahlungsdienstleisters (falls zutreffend).

**Zulassungsnummer:** Zulassungsnummer des Herkunftsmitgliedstaats (falls zutreffend).

**Land der Zulassung:** Herkunftsmitgliedstaat, in dem die Lizenz erteilt wurde.

**Ansprechpartner:** Vor- und Zuname der für die Übermittlung der Daten verantwortlichen Person, oder, falls ein Drittanbieter im Namen des Zahlungsdienstleisters meldet, Vor- und Zuname der Person, die für die Datenverwaltung oder einen ähnlichen Bereich auf der Ebene des Zahlungsdienstleisters zuständig ist.

**E-Mail:** E-Mail-Adresse, an die gegebenenfalls erforderliche Rückfragen zu richten sind. Hierbei kann es sich um eine individuelle [alternativ: einer Person zugeordnete] oder um eine Firmen-E-Mail-Adresse handeln.

**Telefonnummer des Ansprechpartners:** Telefonnummer, an die gegebenenfalls Rückfragen zu richten sind. Hierbei kann es sich um eine individuelle [alternativ: einer Person zugeordnete] oder um eine Firmentelefonnummer handeln.

## Datenaufschlüsselung

Alle von den Zahlungsdienstleistern unter Verwendung der verschiedenen Aufschlüsselungen in Anhang 2 übermittelten Daten sollten der nachstehend definierten geografischen Aufschlüsselung folgen und sowohl die Anzahl der Zahlungsvorgänge *(tatsächliche Einheiten, Gesamtsumme für den Zeitraum)* als auch den Wert der Zahlungsvorgänge *(EUR/lokale Währung, tatsächliche Einheiten, Gesamtsumme für den Zeitraum)* angeben.

| | Wert und Volumen |
|---|---|
| Bereich | Inland,<br>Grenzübergreifend *innerhalb des EWR, und*<br>Grenzübergreifend *außerhalb des EWR* |

# Anhang 2 – Anforderungen an Datenmeldungen für Zahlungsdienstleister

## A- Aufschlüsselung der Daten für Überweisungen

| | Posten | Zahlungsvorgänge | Betrügerische Zahlungsvorgänge |
|---|---|---|---|
| **1** | **Überweisungen** | **X** | **X** |
| **1.1** | davon durch Zahlungsauslösedienstleister ausgelöst | X | X |
| **1.2** | davon nicht elektronisch ausgelöst | X | X |
| **1.3** | davon elektronisch ausgelöst | X | X |
| **1.3.1** | davon über Fernzahlungswege ausgelöst | X | X |
| **1.3.1.1** | **davon durch starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Überweisungen nach Betrugsarten:* | | |
| **1.3.1.1.1** | Erteilung eines Zahlungsauftrags durch den Betrüger | | X |
| **1.3.1.1.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **1.3.1.1.3** | Manipulation des Zahlers durch den Betrüger zur Ausstellung eines Zahlungsauftrags | | X |
| **1.3.1.2** | **davon durch nicht starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Überweisungen nach Betrugsarten:* | | |
| **1.3.1.2.1** | Ausstellung eines Zahlungsauftrags durch den Betrüger | | X |
| **1.3.1.2.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **1.3.1.2.3** | Manipulation des Zahlers durch den Betrüger zur Ausstellung eines Zahlungsauftrags | | X |
| | *davon aufgeschlüsselt nach Gründen für die Authentifizierung durch nicht starke Kundenauthentifizierung* | | |
| **1.3.1.2.4** | Kleinbetragszahlungen (Art. 16 RTS) | X | X |

| | | | |
|---|---|---|---|
| **1.3.1.2.5** | Überweisungen zwischen Konten, die von derselben natürlichen oder juristischen Person gehalten werden (Art. 15 RTS) | X | X |
| **1.3.1.2.6** | Vertrauenswürdige Empfänger (Art. 13 RTS) | X | X |
| **1.3.1.2.7** | Wiederkehrende Zahlungsvorgänge (Art. 14 RTS) | X | X |
| **1.3.1.2.8** | Von Unternehmen genutzte sichere Zahlungsprozesse und -protokolle (Art. 17 RTS) | X | X |
| **1.3.1.2.9** | Transaktionsrisikoanalyse (Art. 18 RTS) | X | X |
| **1.3.2** | davon über Zahlungsweg ohne Fernzugang ausgelöst | X | X |
| **1.3.2.1** | **davon durch starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Überweisungen nach Betrugsarten* | | |
| **1.3.2.1.1** | Ausstellung eines Zahlungsauftrags durch den Betrüger | | X |
| **1.3.2.1.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **1.3.2.1.3** | Manipulation des Zahlers durch den Betrüger zur Ausstellung eines Zahlungsauftrags | | X |
| **1.3.2.2** | **davon durch nicht starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Überweisungen nach Betrugsarten:* | | |
| **1.3.2.2.1** | Ausstellung eines Zahlungsauftrags durch den Betrüger | | X |
| **1.3.2.2.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **1.3.2.2.3** | Manipulation des Zahlers durch den Betrüger zur Ausstellung eines Zahlungsauftrags | | X |
| | *davon aufgeschlüsselt nach Gründen für die nicht starke Kundenauthentifizierung* | | |
| **1.3.2.2.4** | Überweisungen zwischen Konten, die von derselben natürlichen oder juristischen Person gehalten werden (Art. 15 RTS) | X | X |
| **1.3.2.2.5** | Vertrauenswürdiger Empfänger (Art. 13 RTS) | X | X |
| **1.3.2.2.6** | Wiederkehrende Zahlungsvorgänge (Art. 14 RTS) | X | X |
| **1.3.2.2.7** | Kontaktlose Zahlungen an der Verkaufsstelle (Art. 11 RTS) | X | X |
| **1.3.2.2.8** | Unbeaufsichtigte Terminals für Nutzungsentgelte und Parkgebühren (Art. 12 RTS) | X | X |

| **Verluste aufgrund von Betrug je Haftungsträger:** | Gesamtverlust |
|---|---|
| Der meldende Zahlungsdienstleister | X |

| | |
|---|---|
| Der Zahlungsdienstnutzer (Zahler) | X |
| Sonstige | X |

## Validierung

| |
|---|
| 1.2 + 1.3 = 1; 1.1 entspricht nicht 1, sondern ist eine Teilmenge von 1 |
| 1.3.1 + 1.3.2 = 1.3 |
| 1.3.1.1 + 1.3.1.2 = 1.3.1 |
| 1.3.2.1 + 1.3.2.2 = 1.3.2 |
| 1.3.1.1.1 + 1.3.1.1.2 + 1.3.1.1.3 = Summe der betrügerischen Zahlungsvorgänge in 1.3.1.1; 1.3.1.2.1 + 1.3.1.2.2 + 1.3.1.2.3 = Summer der betrügerischen Zahlungsvorgänge in 1.3.1.2; 1.3.2.1.1 + 1.3.2.1.2 + 1.3.2.1.3 = Summe der betrügerischen Zahlungsvorgänge in 1.3.2.1; 1.3.2.2.1 + 1.3.2.2.2 + 1.3.2.2.3 = Summe der betrügerischen Zahlungsvorgänge in 1.3.2.2 |
| 1.3.1.2.4 + 1.3.1.2.5 + 1.3.1.2.6 + 1.3.1.2.7 + 1.3.1.2.8 + 1.3.1.2.9 = 1.3.1.2 |
| 1.3.2.2.4 + 1.3.2.2.5 + 1.3.2.2.6 + 1.3.2.2.7 + 1.3.2.2.8 = 1.3.2.2 |

## B- Datenaufschlüsselung für Lastschriften

| | Posten | Zahlungsvorgänge | Betrügerische Zahlungsvorgänge |
|---|---|---|---|
| **2** | **Lastschriften** | X | X |
| **2.1** | davon über elektronisches Mandat erteilte Zustimmung | X | X |
| | *davon betrügerische Lastschriften nach Betrugsart:* | | |
| **2.1.1.1** | Nicht autorisierte Zahlungsvorgänge | | X |
| **2.1.1.2** | Manipulation des Zahlers durch den Betrüger zum Erhalt der Zustimmung zu einer Lastschrift | | X |
| **2.2** | davon in einer anderen Form als einem elektronischen Mandat erteilte Zustimmung | X | X |
| | *davon betrügerische Lastschriften nach Betrugsart:* | | |
| **2.2.1.1** | Nicht autorisierte Zahlungsvorgänge | | X |
| **2.2.1.2** | Manipulation des Zahlers durch den Betrüger zum Erhalt der Zustimmung zu einer Lastschrift | | X |

| **Verluste aufgrund von Betrug je Haftungsträger:** | Gesamtverlust |
|---|---|
| Der meldende Zahlungsdienstleister | X |
| Der Zahlungsdienstnutzer (Zahlungsempfänger) | X |
| Sonstige | X |

**Validierung**

| |
|---|
| 2.1 + 2.2 = 2 |
| 2.1.1.1 + 2.1.1.2 = Wert von betrügerischem Zahlungsvorgang von 2.1 |
| 2.2.1.1 + 2.2.1.2 = Wert von betrügerischem Zahlungsvorgang von 2.2 |

## C- Datenaufschlüsselung für kartengebundene Zahlungsvorgänge, welche durch den ▶A1 ausstellenden Zahlungsdienstleister zu melden sind

| | Posten | Zahlungs-vorgänge | Betrügerische Zahlungs-vorgänge |
|---|---|---|---|
| **3** | **Kartenzahlungen (außer Karten nur mit E-Geldfunktion)** | X | X |
| **3.1** | davon nicht elektronisch ausgelöst | X | X |
| **3.2** | davon elektronisch ausgelöst | X | X |
| **3.2.1** | davon über Fernzahlungswege ausgelöst | X | X |
| | *davon nach Kartenfunktion aufgeschlüsselt:* | | |
| **3.2.1.1.1** | Zahlungen mit Karten mit Debitfunktion | X | X |
| **3.2.1.1.2** | Zahlungen mit Karten mit einer Kredit- oder einer „verzögerten“ Debitfunktion | X | X |
| **3.2.1.2** | **davon durch starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Kartenzahlungen nach Betrugsarten:* | | |
| **3.2.1.2.1** | Ausstellung eines Zahlungsauftrags durch einen Betrüger | | X |
| **3.2.1.2.1.1** | Verlorene oder gestohlene Karte | | X |
| **3.2.1.2.1.2** | Karte nicht erhalten | | X |
| **3.2.1.2.1.3** | Gefälschte Karte | | X |
| **3.2.1.2.1.4** | Diebstahl von Kartendaten | | X |
| **3.2.1.2.1.5** | Sonstiges | | X |
| **3.2.1.2.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **3.2.1.2.3** | Manipulation des Zahlers zur Erteilung einer Kartenzahlung | | X |
| **3.2.1.3** | ***davon* durch nicht starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Kartenzahlungen nach Betrugsarten:* | | |
| **3.2.1.3.1** | Ausstellung eines Zahlungsauftrags durch einen Betrüger | | X |
| **3.2.1.3.1.1** | Verlorene oder gestohlene Karte | | X |
| **3.2.1.3.1.2** | Karte nicht erhalten | | X |
| **3.2.1.3.1.3** | Gefälschte Karte | | X |
| **3.2.1.3.1.4** | Diebstahl von Kartendaten | | X |
| **3.2.1.3.1.5** | Sonstiges | | X |

| | | | |
|---|---|---|---|
| **3.2.1.3.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **3.2.1.3.3** | Manipulation des Zahlers zur Leistung einer Kartenzahlung | | X |
| | *davon aufgeschlüsselt nach Gründen für die nicht starke Kundenauthentifizierung* | | |
| **3.2.1.3.4** | Geringer Wert (Art. 16 RTS) | X | X |
| **3.2.1.3.5** | Vertrauenswürdiger Begünstigter (Art. 13 RTS) | X | X |
| **3.2.1.3.6** | Wiederkehrende Zahlungsvorgänge (Art. 14 RTS) | X | X |
| **3.2.1.3.7** | Verwendung sicherer Unternehmenszahlungsverfahren oder -protokolle (Art. 17 RTS) | X | X |
| **3.2.1.3.8** | Vorgangsrisikoanalyse (Art. 18 RTS) | X | X |
| **►A1 3.2.1.3.9** | Vom Händler ausgelöste Zahlungsvorgänge[2] | X | X |
| **►A1 3.2.1.3.10** | Sonstiges | X | X |
| **3.2.2** | davon über Zahlungsweg ohne Fernzugang ausgelöst | X | X |
| | *davon nach Kartenfunktion aufgeschlüsselt:* | | |
| **3.2.2.1.1** | Zahlungen mit Karten mit Debitfunktion | X | X |
| **3.2.2.1.2** | Zahlungen mit Karten mit einer Kredit- oder einer „verzögerten“ Debitfunktion | X | X |
| **3.2.2.2** | **davon durch starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Kartenzahlungen nach Betrugsarten:* | | |
| **3.2.2.2.1** | Ausstellung eines Zahlungsauftrags durch einen Betrüger | | X |
| **3.2.2.2.1.1** | Verlorene oder gestohlene Karte | | X |
| **3.2.2.2.1.2** | Karte nicht erhalten | | X |
| **3.2.2.2.1.3** | Gefälschte Karte | | X |
| **3.2.2.2.1.4** | Sonstiges | | X |
| **3.2.2.2.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **3.2.2.2.3** | Manipulation des Zahlers zur Leistung einer Kartenzahlung | | X |
| **3.2.2.3** | **davon durch nicht starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Kartenzahlungen nach Betrugsarten:* | | |
| **3.2.2.3.1** | Ausstellung eines Zahlungsauftrags durch einen Betrüger | | X |
| **3.2.2.3.1.1** | Verlorene oder gestohlene Karte | | X |

[2] **►A1** z. B. kartengebundene Zahlungsvorgänge, die die von der Europäischen Kommission in F&A 2018_4131 und F&A 2018_4031 genannten Bedingungen erfüllen und die daher als vom Zahlungsempfänger ausgelöst gelten und nicht der Anforderung an die Anwendung einer starken Kundenauthentifizierung gemäß Artikel 97 PSD2 unterliegen.

| | | | |
|---|---|---|---|
| **3.2.2.3.1.2** | Karte nicht erhalten | | X |
| **3.2.2.3.1.3** | Gefälschte Karte | | X |
| **3.2.2.3.1.4** | Sonstiges | | X |
| **3.2.2.3.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **3.2.2.3.3** | Manipulation des Zahlers zur Leistung einer Kartenzahlung | | X |
| | *davon aufgeschlüsselt nach Gründen für die nicht starke Kundenauthentifizierung* | | |
| **3.2.2.3.4** | Vertrauenswürdiger Begünstigter (Art. 13 RTS) | X | X |
| **3.2.2.3.5** | Wiederkehrende Zahlungsvorgänge (Art. 14 RTS) | X | X |
| **3.2.2.3.6** | Kontaktlose Kleinbetragszahlungen (Art. 11 RTS) | X | X |
| **3.2.2.3.7** | Unbesetztes Terminal für Beförderungs- und Parkgebühren (Art. 12 RTS) | X | X |
| **►A1 3.2.2.3.8** | Sonstiges | X | X |

| **Verluste aufgrund von Betrug je Haftungsträger:** | Gesamtverlust |
|---|---|
| Der meldende Zahlungsdienstleister | X |
| Der Zahlungsdienstnutzer (Zahler) | X |
| Sonstige | X |

## Validierung

| |
|---|
| 3.1 + 3.2 = 3 |
| 3.2.1 + 3.2.2 = 3.2 |
| 3.2.1.1.1 + 3.2.1.1.2 = 3.2.1; 3.2.2.1.1 + 3.2.2.1.2 = 3.2.2 |
| 3.2.1.2 + 3.2.1.3 = 3.2.1; 3.2.2.2 + 3.2.2.3 = 3.2.2 |
| 3.2.1.2.1 + 3.2.1.2.2 + 3.2.1.2.3 = Summe der betrügerischen Zahlungsvorgänge 3.2.1.2; 3.2.1.3.1 + 3.2.1.3.2 + 3.2.1.3.3 = Summe der betrügerischen Zahlungsvorgänge 3.2.1.3; 3.2.2.2.1 + 3.2.2.2.2 + 3.2.2.2.3 =Summe de betrügerischen Zahlungsvorgänge 3.2.2.2; 3.2.2.3.1 + 3.2.2.3.2 + 3.2.2.3.3 = 3.2.2.3 |
| 3.2.1.2.1.1 + 3.2.1.2.1.2 + 3.2.1.2.1.3 + 3.2.1.2.1.4 + 3.2.1.2.1.5 = Summe der betrügerischen Zahlungsvorgänge 3.2.1.2.1; 3.2.1.3.1.1 + 3.2.1.3.1.2 + 3.2.1.3.1.3 + 3.2.1.3.1.4 + 3.2.1.3.1.5 = Summe der betrügerischen Zahlungsvorgänge 3.2.1.3.1; 3.2.2.2.1.1 + 3.2.2.2.1.2 + 3.2.2.2.1.3 + 3.2.2.2.1.4 =Summe der betrügerischen Zahlungsvorgänge 3.2.2.2.1; 3.2.2.3.1.1 + 3.2.2.3.1.2 + 3.2.2.3.1.3 + 3.2.2.3.1.4 = 3.2.2.3.1 |
| **►A1** 3.2.1.3.4 + 3.2.1.3.5 + 3.2.1.3.6 + 3.2.1.3.7 + 3.2.1.3.8 + 3.2.1.3.9 + 3.2.1.3.10 = 3.2.1.3; 3.2.2.3.4 + 3.2.2.3.5 + 3.2.2.3.6 + 3.2.2.3.7 + 3.2.2.3.8 = 3.2.2.3 |

## D- Datenaufschlüsselung für kartengebundene Zahlungsvorgänge, die vom ►A1 annehmenden und abrechnenden Zahlungsdienstleister (mit einem Vertragsverhältnis mit dem Zahlungsdienstnutzer) zu melden sind

| | Posten | Zahlungsvorgänge | Betrügerische Zahlungsvorgänge |
|---|---|---|---|
| **4** | **Angenommene und abgerechnete Kartenzahlungen (außer Karten nur mit E-Geldfunktion)** | X | X |
| **4.1** | davon nicht elektronisch ausgelöst | X | X |
| **4.2** | davon elektronisch ausgelöst | X | X |
| **4.2.1** | davon über einen Kanal mit Fernzugang angenommen und abgerechnet | X | X |
| | *davon nach Kartenfunktion aufgeschlüsselt:* | | |
| **4.2.1.1.1** | Zahlungen mit Karten mit Debitfunktion | X | X |
| **4.2.1.1.2** | Zahlungen mit Karten mit einer Kredit- oder einer „verzögerten“ Debitfunktion | X | X |
| **4.2.1.2** | **davon durch starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Kartenzahlungen nach Betrugsarten:* | | |
| **4.2.1.2.1** | Ausstellung eines Zahlungsauftrags durch einen Betrüger | | X |
| **4.2.1.2.1.1** | Verlorene oder gestohlene Karte | | X |
| **4.2.1.2.1.2** | Karte nicht erhalten | | X |
| **4.2.1.2.1.3** | Gefälschte Karte | | X |
| **4.2.1.2.1.4** | Diebstahl von Kartendaten | | X |
| **4.2.1.2.1.5** | Sonstiges | | X |
| **4.2.1.2.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **4.2.1.2.3** | Manipulation des Zahlers zur Leistung einer Kartenzahlung | | X |
| **4.2.1.3** | **davon durch nicht starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Kartenzahlungen nach Betrugsarten:* | | |
| **4.2.1.3.1** | Ausstellung eines Zahlungsauftrags durch einen Betrüger | | X |
| **4.2.1.3.1.1** | Verlorene oder gestohlene Karte | | X |
| **4.2.1.3.1.2** | Karte nicht erhalten | | X |
| **4.2.1.3.1.3** | Gefälschte Karte | | X |
| **4.2.1.3.1.4** | Diebstahl von Kartendaten | | X |

| | | | |
|---|---|---|---|
| **4.2.1.3.1.5** | Sonstiges | | X |
| **4.2.1.3.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **4.2.1.3.3** | Manipulation des Zahlers zur Leistung einer Kartenzahlung | | X |
| | *davon aufgeschlüsselt nach Gründen für die nicht starke Kundenauthentifizierung* | | |
| **4.2.1.3.4** | Geringer Wert (Art. 16 RTS) | X | X |
| **4.2.1.3.5** | Wiederkehrender Zahlungsvorgang (Art. 14 RTS) | X | X |
| **4.2.1.3.6** | Vorgangsrisikoanalyse (Art. 18 RTS) | X | X |
| **►A1 4.2.1.3.7** | Vom Händler ausgelöste Zahlungsvorgänge[3] | X | X |
| **►A1 4.2.1.3.8** | Sonstiges | X | X |
| **4.2.2** | davon über einen Kanal ohne Fernzugang erworben | X | X |
| | *davon nach Kartenfunktion aufgeschlüsselt:* | | |
| **4.2.2.1.1** | Zahlungen mit Karten mit Debitfunktion | X | X |
| **4.2.2.1.2** | Zahlungen mit Karten mit einer Kredit- oder einer „verzögerten“ Debitfunktion | X | X |
| **4.2.2.2** | **davon durch eine starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Kartenzahlungen nach Betrugsarten:* | | |
| **4.2.2.2.1** | Ausstellung eines Zahlungsauftrags durch einen Betrüger | | X |
| **4.2.2.2.1.1** | Verlorene oder gestohlene Karte | | X |
| **4.2.2.2.1.2** | Karte nicht erhalten | | X |
| **4.2.2.2.1.3** | Gefälschte Karte | | X |
| **4.2.2.2.1.4** | Sonstiges | | X |
| **4.2.2.2.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **4.2.2.2.3** | Manipulation des Zahlers zur Leistung einer Kartenzahlung | | X |
| **4.2.2.3** | **davon durch nicht starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische Kartenzahlungen nach Betrugsarten:* | | |
| **4.2.2.3.1** | Ausstellung eines Zahlungsauftrags durch einen Betrüger | | X |
| **4.2.2.3.1.1** | Verlorene oder gestohlene Karte | | X |
| **4.2.2.3.1.2** | Karte nicht erhalten | | X |
| **4.2.2.3.1.3** | Gefälschte Karte | | X |

[3] **►A1** Siehe Fußnote 4.

| | | | |
|---|---|---|---|
| **4.2.2.3.1.4** | Sonstiges | | X |
| **4.2.2.3.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **4.2.2.3.3** | Manipulation des Zahlers zur Leistung einer Kartenzahlung | | X |
| | *davon aufgeschlüsselt nach Gründen für die nicht starke Kundenauthentifizierung* | | |
| **4.2.2.3.4** | Wiederkehrende Zahlungsvorgänge (Art. 14 RTS) | X | X |
| **4.2.2.3.5** | Kontaktlose Kleinbetragszahlungen (Art. 11 RTS) | X | X |
| **4.2.2.3.6** | Unbesetztes Terminal für Beförderungs- und Parkgebühren (Art. 12 RTS) | X | X |
| **►A1 4.2.2.3.7** | Sonstiges | X | X |

| **Verluste aufgrund von Betrug je Haftungsträger:** | Gesamtverlust |
|---|---|
| Der meldende Zahlungsdienstleister | X |
| Der Zahlungsdienstnutzer (Zahlungsempfänger) | X |
| Sonstige | X |

## Validierung

| |
|---|
| 4.1 + 4.2 = 4 |
| 4.2.1 + 4.2.2 = 4.2 |
| 4.2.1.1.1 + 4.2.1.1.2 = 4.2.1; 4.2.2.1.1 + 4.2.2.1.2 = 4.2.2 |
| 4.2.1.2 + 4.2.1.3 = 4.2.1; 4.2.2.2 + 4.2.2.3 = 4.2.2 |
| 4.2.1.2.1 + 4.2.1.2.2 + 4.2.1.2.3 = Zahl der in betrügerischer Absicht gemeldeten Zahlungsvorgänge 4.2.1.2; 4.2.1.3.1 + 4.2.1.3.2 + 4.2.1.3.3 = Zahl der in betrügerischer Absicht gemeldeten Zahlungsvorgänge 4.2.1.3; 4.2.2.2.1 + 4.2.2.2.2 + 4.2.2.2.3 =Zahl der in betrügerischer Absicht gemeldeten Zahlungsvorgänge 4.2.2.2; 4.2.2.3.1 + 4.2.2.3.2 + 4.2.2.3.3 = 4.2.2.3 |
| 4.2.1.2.1.1 + 4.2.1.2.1.2 + 4.2.1.2.1.3 + 4.2.1.2.1.4 + 4.2.1.2.1.5 = Zahl der in betrügerischer Absicht gemeldeten Zahlungsvorgänge 4.2.1.2.1;<br>4.2.1.3.1.1 + 4.2.1.3.1.2 + 4.2.1.3.1.3 + 4.2.1.3.1.4 + 4.2.1.3.1.5 = Zahl der in betrügerischer Absicht gemeldeten Zahlungsvorgänge 4.2.1.3.1;<br>4.2.2.2.1.1 + 4.2.2.2.1.2 + 4.2.2.2.1.3 + 4.2.2.2.1.4 = Zahl der in betrügerischer Absicht gemeldeten Zahlungsvorgänge 4.2.2.2.1; 4.2.2.3.1.1 + 4.2.2.3.1.2 + 4.2.2.3.1.3 + 4.2.2.3.1.4 = 4.2.2.3.1 |
| **►A1**4.2.1.3.4 + 4.2.1.3.5 + 4.2.1.3.6 + 4.2.1.3.7 + 4.2.1.3.8 = 4.2.1.3; 4.2.2.3.4 + 4.2.2.3.5+ 4.2.2.3.6 + 4.2.2.3.7 = 4.2.2.3 |

## E- Datenaufschlüsselung der Barabhebungen mit Karten, die vom Karten ►A1ausstellenden Zahlungsdienstleister zu melden sind

**▼A1**

| | Posten | Zahlungs-vorgänge | Betrügerische Zahlungs-vorgänge |
|---|---|---|---|
| **5** | **Barabhebungen** | X | X |
| | *davon nach Kartenfunktion aufgeschlüsselt* | | |
| 5.1 | davon Barabhebungen mit Karten mit Debitfunktion | X | X |
| 5.2 | davon Barabhebungen mit Karten mit einer Kredit- oder einer „verzögerten“ Debitfunktion | X | X |
| | *davon betrügerische Barabhebungen nach Betrugsarten:* | | |
| 5.2.1 | Erteilung eines Zahlungsauftrags (Barabhebung) durch den Betrüger | | X |
| 5.2.1.1 | Verlorene oder gestohlene Karte | | X |
| 5.2.1.2 | Karte nicht erhalten | | X |
| 5.2.1.3 | Gefälschte Karte | | X |
| 5.2.1.4 | Sonstiges | | X |
| 5.2.2 | Manipulation des Zahlers zur Vornahme einer Barabhebung | | X |

| **Verluste aufgrund von Betrug je Haftungsträger:** | Gesamtverlust |
|---|---|
| Der meldende Zahlungsdienstleister | X |
| Der Zahlungsdienstnutzer (Kontoinhaber) | X |
| Sonstige | X |

**Validierung**

**▼A1**

| |
|---|
| 5.1 + 5.2 = 5 |
| 5.3.1 + 5.3.2 = 5 |
| 5.3.1.1 + 5.3.1.2 + 5.3.1.3 + 5.3.1.4 = 5.3.1 |

## F- Datenaufschlüsselung für E-Geld-Zahlungsvorgänge

| | Posten | Zahlungs-vorgänge | Betrügerische Zahlungsvorgänge |
|---|---|---|---|
| **6** | **E-Geld-Zahlungsvorgänge** | **X** | **X** |
| **6.1** | **davon als Fernzahlungsvorgang ausgelöst** | X | X |
| **6.1.1** | **davon durch starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische E-Geld-Zahlungsvorgänge nach Betrugsarten:* | | |
| **6.1.1.1** | Ausstellung eines Zahlungsauftrags durch den Betrüger | | X |
| **6.1.1.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **6.1.1.3** | Manipulation des Zahlers durch den Betrüger zur Ausstellung eines Zahlungsauftrags | | X |
| **6.1.2** | **davon durch nicht starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische E-Geld-Zahlungsvorgänge nach Betrugsarten:* | | |
| **6.1.2.1** | Ausstellung eines Zahlungsauftrags durch den Betrüger | | X |
| **6.1.2.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **6.1.2.3** | Manipulation des Zahlers durch den Betrüger zur Ausstellung eines Zahlungsauftrags | | X |
| | *davon aufgeschlüsselt nach Gründen für die nicht starke Kundenauthentifizierung* | | |
| **6.1.2.4** | Geringer Wert (Art. 16 RTS) | X | X |
| **6.1.2.5** | Vertrauenswürdiger Begünstigter (Art. 13 RTS) | X | X |
| **6.1.2.6** | Wiederkehrende Zahlungsvorgänge(Art. 14 RTS) | X | X |
| **6.1.2.7** | Zahlung an sich selbst (Artikel 15 RTS) | X | X |
| **6.1.2.8** | Verwendung sicherer Unternehmenszahlungsverfahren oder -protokolle (Art. 17 RTS) | X | X |
| **6.1.2.9** | Vorgangsrisikoanalyse (Art. 18 RTS) | X | X |
| **►A1 6.1.2.10** | Vom Händler ausgelöste Zahlungsvorgänge[4] | X | X |
| **►A1 6.1.2.11** | Sonstiges | X | X |

[4] **►A1** Siehe Fußnote 4.

| | Posten | Zahlungs-vorgänge | Betrügerische Zahlungsvorgänge |
|---|---|---|---|
| **6.2** | **davon ohne Fernzugang ausgelöst** | X | X |
| **6.2.1** | **davon durch starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische E-Geld-Zahlungsvorgänge nach Betrugsarten:* | | |
| **6.2.1.1** | Ausstellung eines Zahlungsauftrags durch den Betrüger | - | X |
| **6.2.1.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **6.2.1.3** | Manipulation des Zahlers durch den Betrüger zur Ausstellung eines Zahlungsauftrags | | X |
| **6.2.2** | **davon durch nicht starke Kundenauthentifizierung authentifiziert** | X | X |
| | *davon betrügerische E-Geld-Zahlungsvorgänge nach Betrugsarten:* | | |
| **6.2.2.1** | Ausstellung eines Zahlungsauftrags durch den Betrüger | | X |
| **6.2.2.2** | Änderung eines Zahlungsauftrags durch den Betrüger | | X |
| **6.2.2.3** | Manipulation des Zahlers durch den Betrüger zur Ausstellung eines Zahlungsauftrags | | X |
| | *davon aufgeschlüsselt nach Gründen für die nicht starke Kundenauthentifizierung* | | |
| **6.2.2.4** | Vertrauenswürdiger Begünstigter (Art. 13 RTS) | X | X |
| **6.2.2.5** | Wiederkehrender Zahlungsvorgang (Art. 14 RTS) | X | X |
| **6.2.2.6** | Kontaktlose Kleinbetragszahlungen (Art. 11 RTS) | X | X |
| **6.2.2.7** | Unbesetztes Terminal für Beförderungs- und Parkgebühren (Art. 12 RTS) | X | X |
| **►A1 6.2.2.8** | Sonstiges | X | X |

| **Verluste aufgrund von Betrug je Haftungsträger:** | Gesamtverlust |
|---|---|
| Der meldende Zahlungsdienstleister | X |
| Der Zahlungsdienstnutzer | X |
| Sonstige | X |

## Validierung

| |
|---|
| 6.1 + 6.2 = 6 |
| 6.1.1 + 6.1.2 = 6.1; 6.2.1 + 6.2.2 = 6.2 |
| 6.1.1.1 + 6.1.1.2 + 6.1.1.3 = Zahl der in betrügerischer Absicht gemeldeten Zahlungsvorgänge 6.1.1; 6.1.2.1 + 6.1.2.2 + 6.1.2.3 = Zahl der in betrügerischer Absicht gemeldeten Zahlungsvorgänge 6.1.2; 6.2.1.1 + 6.2.1.2 + 6.2.1.3 =Zahl der in betrügerischer Absicht gemeldeten Zahlungsvorgänge 6.2.1; 6.2.2.1 + 6.2.2.2 + 6.2.2.3 = 6.2.2 |
| ►**A1** 6.1.2.4 + 6.1.2.5 + 6.1.2.6 + 6.1.2.7 + 6.1.2.8 + 6.1.2.9 + 6.1.2.10 + 6.1.2.11 = 6.1.2; 6.2.2.4 + 6.2.2.5 + 6.2.2.6 + 6.2.2.7 + 6.2.2.8 = 6.2.2 |

## G- Datenaufschlüsselung für Finanztransferzahlungsvorgänge

| | Posten | Zahlungsvorgänge | Betrügerische Zahlungsvorgänge |
|---|---|---|---|
| 7 | **Finanztransfers** | X | X |
| | | | |

## H- Datenaufschlüsselung für Zahlungsvorgänge, die von Zahlungsauslösedienstleistern ausgelöst wurden

| | Posten | Zahlungsvorgänge | Betrügerische Zahlungsvorgänge |
|---|---|---|---|
| **8** | **Zahlungsvorgänge, die von Zahlungsauslösedienstleistern ausgelöst wurden** | **X** | **X** |
| **8.1** | davon über Fernzahlungswege ausgelöst | X | X |
| **8.1.1** | davon durch starke Kundenauthentifizierung authentifiziert | X | X |
| **8.1.2** | davon durch nicht starke Kundenauthentifizierung authentifiziert | X | X |
| **8.2** | davon über Zahlungsweg ohne Fernzugang ausgelöst | X | X |
| **8.2.1** | davon durch starke Kundenauthentifizierung authentifiziert | X | X |
| **8.2.2** | davon durch nicht starke Kundenauthentifizierung authentifiziert | X | X |
| | davon nach Zahlungsinstrument aufgeschlüsselt | | |
| **8.3.1** | Überweisungen | X | X |
| **8.3.2** | Sonstiges | X | X |

**Validierung**

| |
|---|
| 8.1 + 8.2 = 8 |
| 8.3.1 + 8.3.2 = 8 |
| 8.1.1 + 8.1.2 = 8.1 |
| 8.2.1 + 8.2.2 = 8.2 |