

ABTEILUNG FÜR STATISTIK –
INFORMATIONSSYSTEME UND DATENMANAGEMENT

Ausweisrichtlinie zum Beleg B5

Versionsinfo:

Version Mai 2021:

- Die zu meldenden Geldwerte sind in **EINER** mit zwei Kommastellen (auf den Cent genau) anzuführen.
- Betreffend SWIFT-Zahlungen wurde betreffend des NON-SEPA-Schemas ergänzt: (wir würden eine „NA“-Klassifizierung bei SWIFT-Transaktionen erwarten).

Version Juli 2021:

- Debit MasterCard steht als Systemkennung ab 2022 zur Verfügung.
- Nähere Definition von Transaktionen via „Mobile payment solution“ bzw. „P2P-Lösung für mobile Zahlungen“
- Nähere Ausführungen, ab wann und für welchen Zeitraum betrügerische Zahlungen zu melden sind.
- Unterscheidung der Meldepflichten von P2P-Lösung für mobile Zahlungen im B1 und im B4/B5
- Nähere Ausführungen zu Non-SEPA-Lastschriftverfahren („ONUS“ bzw. „nicht anwendbar“).
- Nähere Definition zu den EWR-Ländern

Version September 2021:

- Genauere Beschreibung betreffend betrügerische Zahlungen am ATM.
- Weitere Präzisierung zu den EWR-Ländern
- Ein Beispiel bezüglich des Meldezeitpunktes bzw. der Meldeperiode von betrügerischen Transaktionen wurde eingefügt.
- Betrügerische Transaktionen via nicht kartengebundener Zahlungsdienste sind weiterhin von Issuern und Acquirern meldepflichtig. Statt im B1 (bis Ende 2021 meldepflichtig) müssen diese Daten (zu Bluecode, Paybox, Daopay, Dimoco, ...) mit den gleichen Details wie bisher ab Anfang 2022 im B5 gemeldet werden.
- Ergänzung zu Apple Pay unter Begriffe und Erklärungen.
- Nochmalige Klarstellung des Zusammenhangs der Meldekonzpte die Transaktion ohne starke Kundenauthentifizierung ausweisen und jener, in denen die Gründe für die Durchführung von Transaktionen ohne starke Kundenauthentifizierung (Ausnahmen) anzugeben sind.

Version November 2021:

- Nähere Erläuterungen zu sonstigen Zahlungsdiensten (gesendet) wurde hinzugefügt

- Die in der Dimension SYSTS wurde Ausprägung NA auf NOTA (Nicht anwendbar) für Überweisungen umgestellt.

Version März 2022:

- Konkretisierung bezüglich der Meldung von abgebrochenen, zurückgewiesenen stornierten und rückgebuchten Transaktionen

Version Juni 2022:

- Konkretisierung bezüglich der Meldung von in Papierform eingereichten Daueraufträgen
- Konkretisierung bezüglich der bezüglich der Meldung betrügerischer Bargeldüberweisungen/Finanztransfers

Version November 2022:

- Es wurde klargestellt, dass die „Acquirer-Positionen“ „am physischen EFTPOS initiiert“ (ACQ0400BETRUG), „am Geldautomaten (ATM) initiiert“ (ACQ0500BETRUG) und „anders initiiert“ (ACQ0600BETRUG) alle unter die Kategorie „elektronisch initiiert“ bzw. „nicht über einen Fernzugang“ fallen.
- NONSEPA1-n Zahlungen (abseits von ONUS und NOTA) sind nur nach Rücksprache mit der OeNB zu melden (dies wurde im Schaubild entsprechend gekennzeichnet)

Version Oktober 2023:

- Konkretisierung bezüglich der bezüglich der Meldung betrügerischer Bargeldüberweisungen/Finanztransfers
- Konkretisierung bezüglich Überweisungen initiiert als Datei/ Sammelüberweisung (mit CD/Diskette)

Version April 2024:

- Ergänzung der neuen Rechtsgrundlage zur Einleitung eines Sanktionsverfahrens bei Übertretungen der in den Ausweisrichtlinien definierten statistischen Berichtspflichten

Version Mai 2026:

- Ergänzung **SEPA sofort/instant One-Leg Out** (SEPAOI) als Systemstandard 1.

Inhalt

1.	ALLGEMEINES.....	5
2.	GESETZLICHE GRUNDLAGE.....	6
3.	MELDEPFLICHT	7
4.	BEGRIFFE UND ERKLÄRUNGEN.....	8
4.1	BETRUGSARTEN	14
	<i>Änderung eines Zahlungsauftrags durch den Betrüger</i>	14
	<i>Erteilung eines Zahlungsauftrags durch den Betrüger</i>	14
	<i>Manipulation des Zahlers durch den Betrüger</i>	16
4.2	STARKE KUNDENAUTHENTIFIZIERUNG UND GRÜNDE FÜR DIE DURCHFÜHRUNG VON TRANSAKTIONEN OHNE STARKE KUNDENAUTHENTIFIZIERUNG	16
4.3	LÄNDERGLIEDERUNG	19
4.4	BETRÜGERISCHE ÜBERWEISUNGEN, LASTSCHRIFTEN UND SCHECKS.....	19
	<i>Betrügerische Überweisungen.....</i>	20
	<i>Betrügerische Lastschriften</i>	25
	<i>Betrügerische Scheck-Zahlungen.....</i>	26
	<i>Sonstige Zahlungsdienste (gesendet).....</i>	26
	<i>Bargeldüberweisungen/Finanztransfers</i>	26
	<i>Transaktionen, die von Zahlungsauslösedienstleistern ausgelöst wurden.....</i>	27
4.5	BETRUG ATM BARGELDBEBEHUNG - ISSUERMELDUNG	27
4.6	BETRUG POS - ISSUERMELDUNG	27
4.7	BETRUG POS UND ATM - ISSUERMELDUNG DETAILS	28
4.8	BETRUG POS – ACQUIRERMELDUNG.....	30
4.9	BETRUG POS - ACQUIRERMELDUNG DETAILS	31
4.10	BETRUG HAFTUNGSTRÄGER	31
4.11	BETRUG VIA NICHT KARTENGEBUNDENER ZAHLUNGSDIENSTE.....	31
5.	MELDEDIMENSIONEN	33

1. Allgemeines

Die zu meldenden Geldwerte sind in **EINER** mit zwei Kommastellen (auf den Cent genau) anzuführen. Die Anzahl ist in **EINER** zu melden. Zahlungstransaktionen in Fremdwährungen sind enthalten. Daten werden unter Verwendung des Referenzwechsellkurses der EZB oder der für diese Transaktionen zugrunde gelegten Wechselkurse in Euro umgerechnet. Für den Fall, dass es keinen "Kurs der Transaktion" gibt (z.B. USD-Überweisung auf ein USD-Konto) sollte daher, wenn möglich, zu dem jeweiligen Tagesreferenzkurs, sonst (wenn z.B. keiner vorhanden) zum Monatsreferenzkurs umgerechnet werden.

Bestandsdaten beziehen sich auf Positionen zum Ende des Berichtszeitraums, d. h. Positionen am letzten Arbeitstag des betreffenden Kalenderjahres. Stromgrößen beziehen sich auf im Berichtszeitraum aufgelaufene Zahlungstransaktionen, d. h. die Gesamtsumme für das betreffende Kalenderhalbjahr.

Bitte beachten Sie, dass gemäß Leitlinie 6.1 der EBA-Leitlinien "das Datum, das von Zahlungsdienstleistern für die Erfassung von Zahlungsvorgängen und betrügerischen Zahlungsvorgängen für die Zwecke dieser statistischen Meldung zu berücksichtigen ist, der Tag ist, an dem die Transaktion in Übereinstimmung mit der PSD2 ausgeführt wurde."

Anhang 1 der EZB-Änderungsverordnung legt dann in Übereinstimmung mit Leitlinie 6.2 der EBA-Leitlinien fest: "Der Zahlungsdienstleister sollte alle betrügerischen Zahlungsvorgänge ab dem Zeitpunkt melden, zu dem der Betrug durch eine Kundenbeschwerde oder auf andere Weise aufgedeckt wurde, unabhängig davon, ob der mit dem betrügerischen Zahlungsvorgang zusammenhängende Fall zum Zeitpunkt der Meldung der Daten gelöst ist oder nicht."

Dies bezieht sich auf den Zeitpunkt, ab dem betrügerische Transaktionen gemeldet werden sollten, nicht auf den Bezugszeitraum, für den sie gelten. Sobald eine Transaktion als betrügerisch erkannt wurde, sollte sie folglich sowohl unter Zahlungen als auch unter betrügerischen Transaktionen für den Referenzzeitraum, in dem der ursprüngliche Zahlungsvorgang ausgeführt wurde, gemeldet werden. Dies gilt unbeschadet des Prozesses der Bestätigung des Betrugs.

Die Daten sind unkonsolidiert pro Institut zu melden. Zahlungsdienstleister haben die Daten unverzüglich nach Ablauf eines jeden Kalenderhalbjahres, spätestens aber zwei Monate nach dem Meldestichtag bzw. dem letzten Tag der Meldeperiode an die Oesterreichische Nationalbank zu erstatten. Die Meldung ist mittels elektronischer Übermittlung an die Oesterreichische Nationalbank zu erstatten. Die erste Meldung zur Meldeperiode 1. Halbjahr 2022 hat mit dem Stichtag 30. 6. 2022 zu erfolgen.

Beispiel:

Die Transaktion passierte im Jänner und im Februar wurde sie als betrügerisch eingestuft. Die Meldung erfolgt somit für die Meldeperiode 1. Halbjahr bis Ende August.

Wir empfehlen, dass gleichzeitig mit der aktuellen B5-Meldung auch nochmals komplette Ersatzmeldung für die vorangegangenen Perioden (mit revidierten Daten) gemeldet werden. Es muss lediglich technisch eine neue Versionsnummer (ergo diese hochsetzen) für die bereits gesendeten Meldungen in den Datensatz eingetragen werden.

In dieser Meldung sind ausschließlich betrügerische Transaktionen zu melden, die eine Teilmenge der in den anderen Erhebungen der Zahlungsverkehrsstatistik gemeldeten Transaktionen darstellen.

Weitergabe vertraulicher statistischer Daten

Vertrauliche Daten werden, wie in der Verordnung (EU) 2020/2011 der Europäischen Zentralbank der Europäischen Zentralbank vom 1. Dezember 2020 zur Zahlungsverkehrsstatistik (EZB/2020/59) vorgesehen an die EZB übermittelt. Eine Weitergabe von Daten der EZB an die EBA erfolgt in aggregierter Form (die Daten unterliegen somit keiner Vertraulichkeit).

Die Daten werden auch an die FMA weitergegeben, da gemäß § 86 Abs 3 Zahlungsdienstleister der FMA statistische Daten zu Betrugsfällen in Verbindung mit den unterschiedlichen Zahlungsmitteln vorzulegen haben.

Gemäß Verordnung des Rates Nr. 2533/98 dürfen vertrauliche statistische Daten auch an die nach dem Unionsrecht oder dem nationalen Recht für die Beaufsichtigung von Finanzinstituten, -märkten und -infrastrukturen oder für die Stabilität des Finanzsystems zuständigen Behörden oder Einrichtungen der Mitgliedstaaten und der Union und an den Europäischen Stabilitätsmechanismus (ESM) nur in dem zur Erfüllung der jeweiligen Aufgaben erforderlichen Maße und Detaillierungsgrad übermittelt werden.

2. Gesetzliche Grundlage

Verordnung (EU) 2020/2011 der Europäischen Zentralbank vom 1. Dezember 2020 zur Zahlungsverkehrsstatistik (EZB/2020/59) iVm § 44 und 44a Nationalbankgesetz, die EBA-Leitlinie zur Meldung von Betrugsfällen nach der Zahlungsdiensterichtlinie (PSD2) in ihrer aktuellen Fassung sowie das Devisengesetz 2004¹.

Zahlungsdienstleister haben gemäß § 86 Abs 3 ZaDiG der FMA statistische Daten zu Betrugsfällen in Verbindung mit den unterschiedlichen Zahlungsmitteln vorzulegen. Diese Meldepflicht gilt mit der Übermittlung der Meldungen B1 (für Acquirer und Issuer), B4 (sonstige Zahlungen) und B5 (Betrugsdaten) als erfüllt.

¹ Devisengesetz 2004, BoP Manual 5, ESVG 95 Verordnung (EC) 2223/96; Guideline ECB/2004/15, Guideline ECB/2007/3; Verordnung (EC) 184/2005

Rechtsgrundlage zur Aufzeichnung von Nichteinhaltungen statistischer Berichtspflichten (z.B. Spätmelder oder schwerwiegendes Fehlverhalten im Zusammenhang mit den Meldepflichten).

Auf Grund

- der Verordnung (EU) 2022/1917 der EZB zu Übertretungsverfahren bei Nichteinhaltung statistischer Berichtspflichten (EZB/2022/31)

kann bei Übertretungen der in den Ausweisrichtlinien definierten statistischen Berichtspflichten ein Sanktionsverfahren eingeleitet werden.

3. Meldepflicht

Meldepflichtig für diese Erhebung sind alle Zahlungsdienstleister (Kreditinstitute gemäß EU-Gemeinschaftsrecht², Zahlungsinstitute³, E-Geld-Institute⁴) und bzw. oder Betreiber von Zahlungsverkehrssystemen.

Zahlungsdienstleister sind Institute, die in Österreich als Gesellschaft eingetragen und ansässig sind, einschließlich Tochterunternehmen (eigenständige Kapitalgesellschaften, an denen ein anderes Rechtssubjekt die Mehrheit der Anteilsrechte oder alle Anteilsrechte besitzt) von außerhalb dieses Staatsgebiets ansässigen Mutterunternehmen, und Zweigstellen von Instituten (nicht als Kapitalgesellschaften geführte, rechtlich unselbstständige Rechtssubjekte, die vollständig im Eigentum ihres Mutterunternehmens stehen), deren Hauptverwaltung sich außerhalb dieses Staatsgebiets befindet. Eine Konsolidierung von Daten über Landesgrenzen hinweg ist für statistische Zwecke nicht erlaubt (d. h.: Transaktionen die z.B. über eine Zweigstelle/Filiale in Österreich abgewickelt werden, müssen in Österreich gemeldet werden und dürfen nicht bei der ausländischen Mutter gemeldet werden).

² im Sinne von Artikel 4 Nummer 1 Buchstabe a der Richtlinie 2006/48/EG

³ im Sinne von Artikel 4 Nummer 4 der Richtlinie 2007/64/EG

⁴ im Sinne von Artikel 1 Absatz 3 Buchstabe a der Richtlinie 2000/46/EG

4. Begriffe und Erklärungen

betrügerische
Zahlungsvorgänge

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

- 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
- 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“).

"Freundlicher Betrug"
bzw. "first party fraud"

"First party fraud" sollte nicht in die Meldung betrügerischer Transaktionen einbezogen werden. Ein Beispiel für einen solchen "freundlichen Betrug" ist ein Händler, der absichtlich Rückerstattungen auf seiner eigenen Karte beantragt. Die Rückerstattungen werden vom Aussteller bearbeitet, der dann vom Acquirer eine Rückbelastung verlangt. Letztendlich kann der Acquirer die Gelder beim Händler nicht einziehen.

Nicht-MFIs (Non-MFI)

Jede natürliche oder juristische Person, die nicht zum MFI-Sektor gehört. Für die Zwecke der Zahlungsverkehrsstatistik sind alle Zahlungsdienstleister aus dem „Nicht-MFI“-Sektor ausgeschlossen.

Monetäre Finanzinstitute, MFIs (Monetary Financial Institutions)	MFIs sind alle institutionellen Einheiten der Teilsektoren Zentralbank (ESVG-Sektor S.121), Kreditinstitute (ohne die Zentralbank) (ESVG-Sektor S.122) und Geldmarktfonds (ESVG-Sektor S.123) gemäß dem überarbeiteten Europäischen System Volkswirtschaftlicher Gesamtrechnungen nach der Verordnung (EU) Nr. 549/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 zum Europäischen System Volkswirtschaftlicher Gesamtrechnungen auf nationaler und regionaler Ebene in der Europäischen Union.
Debitkarte (Card with a debit function)	Eine Karte, die Karteninhabern ermöglicht, dass ihre Konten direkt und unmittelbar mit Käufen oder Bargeldbehebungen belastet werden, unabhängig davon, ob diese Konten beim Kartenemittenten gehalten werden oder nicht. Eine Karte mit Debitfunktion kann mit einem Konto, das Überziehungskredite als eine zusätzliche Eigenschaft anbietet, verbunden sein.
Kreditkarte <u>ohne</u> Kreditfunktion (Card with a delayed debit function)	Eine Karte, die Karteninhabern ermöglicht, dass ein Konto beim Kartenemittenten mit Käufen oder Bargeldbehebungen bis zu einer genehmigten Grenze belastet wird. Der Saldo auf diesem Konto wird <u>regelmäßig</u> am Ende eines im Voraus festgelegten Zeitraums (zumeist monatlich) vollständig beglichen (verzögerte Abbuchung). Für den Zeitraum zwischen Bezahlung einer Ware und der Fälligkeit der Kreditkartenabrechnung (z.B. jedes Monatsende) wird dem Kreditkarteninhaber ein zinsenloser Kredit gewährt (convenience credit).
Kreditkarte <u>mit</u> Kreditfunktion (Card with a credit function)	Eine Karte, die Karteninhabern ermöglicht, dass ein Konto beim Kartenemittenten mit Käufen oder Bargeldbehebungen bis zu einer genehmigten Grenze belastet wird. Bei der Rückzahlung des Saldos auf diesem Konto kann dabei der Karteninhaber zwischen der vollständigen Rückzahlung zu den standardmäßig vorgesehenen Terminen und der Rückzahlung per Ratenzahlung innerhalb eines festzulegenden Zeitraumes wählen. Allerdings werden für diese Form der Ratenkreditgewährung in der Regel Zinsen seitens des Kartenemittenten verrechnet (credit card credit).

Überweisung
(credit transfer)

Ein Zahlungsdienst, mit dem der Zahlende sein kontoführendes Institut anweisen kann, dem Begünstigten Geldmittel zu überweisen. Es handelt sich um eine Zahlungsanweisung oder eine Reihe von Zahlungsanweisungen, deren Zweck darin liegt, dem Begünstigten Geldmittel verfügbar zu machen. Sowohl die Zahlungsanweisung als auch die in ihr beschriebenen Geldmittel werden vom Zahlungsdienstleister des Zahlenden zum Zahlungsdienstleister des Zahlungsempfängers, d. h. Begünstigten, transferiert, möglicherweise über mehrere zwischengeschaltete Kreditinstitute und/oder ein oder mehrere Zahlungsverkehrs- und Verrechnungssysteme.

Transaktionen mit Bargeld an einem oder beiden Enden der Zahlungstransaktion, und unter Verwendung eines Überweisungsdienstes, sind als Überweisungen enthalten.

Überweisungen an einem Geldautomat mit Überweisungsfunktion sind auch enthalten. Überweisungen zur Verrechnung ausstehender Forderungen aus Transaktionen unter Verwendung von Kreditkarten mit oder ohne Kreditfunktion sind auch enthalten. Bareinzahlungen auf ein Konto unter Verwendung eines Bankformulars sind nicht unter Überweisungen enthalten.

Überweisungen
beleglos initiiert
(credit transfers – non
paper based)

Jede Überweisung, die der Zahlungspflichtige nicht in Papierform einreicht, d. h. elektronisch. Enthält Einreichungen per Telefax oder sonstiger Kommunikationsmittel (wie automatisiertes Telefon-Banking), sofern sie ohne manuellen Eingriff in elektronische Zahlungen umgewandelt werden.

~~Enthält Daueraufträge, die anfangs zwar in Papierform eingereicht wurden, in der Folge aber regelmäßig elektronisch ausgeführt werden.~~

Enthält Überweisungen, die durch einen Zahlungsdienstleister auf der Basis eines Finanzdienstes ausgeführt werden, wenn der Finanzdienst beleglos initiiert ist, oder die Form der Einreichung des Dienstes unbekannt ist, und der Zahlungsdienstleister die Überweisung elektronisch ausgeführt hat.

Enthält an einem Geldautomat mit Überweisungsfunktion initiierte Überweisungen.

Beleginitiierte Überweisungen (credit transfers – paper based)	<p>Eine Überweisung, die vom Zahler</p> <ul style="list-style-type: none"> • in Papierform veranlasst wird • oder durch die Anweisung an das Personal einer Filiale am Schalter veranlasst wird • oder eine Überweisung, die eine manuelle Bearbeitung erfordert. <p>In Papierform eingereichten Daueraufträge werden als "Beleginitiierte Überweisungen" gemeldet.</p>
Überweisungen initiiert als Datei/ Sammelüberweisung (credit transfers – initiated in a file/batch)	<p>Eine beleglos initiierte Überweisung, die Teil einer Gruppe von Überweisungen ist, die vom Zahlungspflichtigen gemeinsam initiiert werden. Jede Überweisung, die Teil einer Sammelüberweisung ist, wird als separate Überweisung gezählt, wenn die Anzahl der Transaktionen gemeldet wird.</p> <p>Im Fall einer Überweisung über eine CD/Diskette, bei der nur eine Transaktion auf dem Medium gespeichert ist, gibt die EZB vor, dass dies auch unter Datei/Sammelabwicklung gemeldet werden soll.</p>
Geldautomat (ATM – automated teller machine)	<p>Elektromechanische Vorrichtung, mit der autorisierte Nutzer, die typischerweise maschinenlesbare physische Karten verwenden, Bargeld von ihren Konten abheben können und/oder Zugang zu sonstigen Diensten erhalten, zum Beispiel Kontostandsabfragen, Überweisungen oder Bargeldeinzahlungen.</p> <p>Eine Vorrichtung, mit der ausschließlich Kontostandsabfragen getätigt werden können, gilt nicht als ATM.</p> <p>Der Geldautomat kann im Online-Modus, mit einer Echtzeit-Autorisierungsanfrage oder im Offline-Modus betrieben werden.</p>
Geldautomat mit Überweisungsfunktion (ATM with a credit transfer function)	Geldautomat, der es autorisierten Nutzern ermöglicht, Überweisungen unter Verwendung einer Zahlungskarte vorzunehmen.
Bargeldabhebung am Geldautomat (cash withdrawals at ATMs)	Bargeldabhebung an einem Geldautomaten unter Verwendung einer Karte zur Bargeldabhebung.
Bargeldeinzahlung am Geldautomaten	Bargeldeinzahlung an einem Geldautomaten unter Verwendung einer Karte zur Bargeldabhebung. Enthält alle

(cash deposits at ATMs)	Transaktionen, bei denen Bargeld ohne manuellen Eingriff an einem Terminal eingezahlt wird, und der Zahlungspflichtige mit einer Zahlungskarte identifiziert wird.
Scheck (Cheque)	Eine schriftliche Anweisung einer Partei, d. h. des Ausstellers, an eine andere Partei, d. h. den Bezogenen, der normalerweise ein Kreditinstitut ist, die den Bezogenen verpflichtet, dem Aussteller oder einem vom Aussteller benannten Dritten auf Sicht einen bestimmten Betrag zu zahlen. Bargeldabhebungen mit Schecks sind enthalten. Bargeldabhebungen unter Verwendung von Bankformularen sind nicht enthalten. Ausgegebene Schecks, die nicht zur Verrechnung eingereicht wurden, sind nicht enthalten.
Erhaltene Transaktion (Transaction received)	<p>Eine von Zahlungsdienstleistern empfangene Transaktion, an der Nicht-MFIs beteiligt sind.</p> <p>Für verschiedene Zahlungsinstrumente gilt folgende Erhebungslogik:</p> <p>Erhaltene Überweisungen werden auf der Seite des Zahlungsempfängers gezählt;</p> <p>Erhaltene Lastschriften werden auf der Seite des Zahlungspflichtigen gezählt (d.h. es werden die eingehenden Anweisungen/Aufträge zu Lastschriften erfasst);</p> <p>Erhaltene Schecks werden auf der Seite des Zahlungspflichtigen gezählt (Kunde stellt den Scheck aus; Schecklastschrift)</p>
Gesendete Transaktion (Transaction sent)	<p>Eine von Zahlungsdienstleistern gesendete Transaktion, an der Nicht-MFIs beteiligt sind.</p> <p>Für verschiedene Zahlungsinstrumente gilt folgende Erhebungslogik:</p> <p>Gesendete Überweisungen werden auf der Seite des Zahlungspflichtigen gezählt;</p> <p>Gesendete Lastschriften werden auf der Seite des Zahlungsempfängers gezählt (d.h. es werden die ausgehenden/gesendeten Aufträge zu Lastschriften erfasst);</p> <p>Gesendete Schecks werden auf der Seite des Zahlungsempfängers gezählt (Zahlungsempfänger reicht den Scheck zur Gutschrift ein)</p>
EWR-Länder	Die verschiedenen Länder-Sektoren sind unter https://www.oenb.at/meldewesen/meldebestimmungen/aufsichtsstatistik/zahlungsverkehrsstatistik.html

zu finden. Im Sektor BSPAYEWR finden sich alle ERW-Länder sowie unter dem Code X42 die Nicht-ERW-Länder in Summe.

Alle in den Sektoren nicht angeführten „Gebiete/Länder mit einer besonderen verfassungsrechtlichen Beziehung zwischen dem betreffenden Gebiet und dem betreffenden Mitgliedstaat“ mit eigenem Länder-ISO-Code zählen nicht zu den EWR-Ländern (z.B. Französisch Polynesien (PF) nicht zu Frankreich, San Marino (SM) und Vatikan (VA) nicht zu Italien, Faeroer Inseln Dän.Verwaltung (FO) and Grönland (Dän.Verwaltung) (GL) nicht zu Dänemark, Andorra (AD) nicht zu Spanien, Aruba (AW), Bonaire, St. Eustatius und Saba (BQ), Curaçao (CW) and St. Martin (SX) nicht zu den Niederlanden, etc.)

Z.B. ist Grönland nicht bei Dänemark einzurechnen, sondern bei Summe EWR-extern. Monaco kann bei der EWR-Gliederung gleich in Summe bei Frankreich gemeldet werden. Wenn weltweit alle Einzelländer gefordert sind, sind alle ISO-Codes und somit auch Grönland und Monaco einzeln anzuführen.

Apple Pay-
Zahlungstransaktionen

Wir gehen davon aus, dass Apple Pay mit einer Zahlungskarte verknüpft ist. Daher sind diese betrügerischen Transaktionen unter B5 Betrug Acq POS bzw. B5 Betrug Iss POS zu melden.

stornierte
Transaktionen und
abgelehnte
Transaktionen

Im Allgemeinen werden stornierte Transaktionen (cancelled transactions) nicht gezahlt, während abgelehnte Transaktionen (rejected transactions) gezahlt werden. Im Sonderfall der mangelnden Deckung des Kundenkontos sollten abgewiesene Überweisungen nicht gezahlt werden, da sie in der Sphäre der Kundenbank auf der Absenderseite abgewiesen werden (was nicht zu einer tatsächlichen Transaktion führt). Abgelehnte Lastschriften hingegen sind im gleichen Fall der mangelnden Deckung zu zählen, da sie in der Interbankensphäre auf der Empfängerseite abgelehnt werden (in diesem Fall wird eine tatsächliche Transaktion durchgeführt und später abgelehnt).

Rückabwicklung

Eine Rückabwicklung (reversal) ist eine technische Annullierung einer Transaktion. Vor der Abrechnung der ursprünglichen Transaktion wird die Stornierung von der ursprünglichen Transaktion abgezogen und nicht als separate Transaktion gemeldet.

Rückerstattung /
Rücktransaktion

Eine Rückerstattung (refund) ist eine separate Transaktion. Die Rückerstattung wurde separat und unabhängig von der ursprünglichen Zahlungstransaktion abgewickelt; sie sollte separat gemeldet werden.

4.1 Betrugsarten

Änderung eines Zahlungsauftrags durch den Betrüger

„Änderung eines Zahlungsauftrags durch den Betrüger“ ist eine Art nicht autorisierter Zahlungsvorgang im Sinne der Leitlinie 1.6 c) der EBA-Leitlinien zu den Meldeanforderungen für Betrugsdaten nach Artikel 96 Absatz 6 PSD2 (EBA/GL/2018/05) 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.

Diese Betrugsart ist für Überweisungen, kartengestützte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen relevant.

Ein Beispiel ist die Situation, in der der Betrüger den Betrag auf einem Zahlungsauftrag vor dessen Ausführung ändert. Ein weiteres Beispiel ist die Änderung des Begünstigten: Ein Betrüger könnte auf das Konto eines Opfers zugreifen, um eine Reihe von Zahlungsdetails so zu ändern, dass bei der Ausführung von Zahlungstransaktionen durch den Zahlungsverkehrsdienstleister des Opfers die Gelder unbeabsichtigt an einen oder mehrere Begünstigte, die vom Betrüger ausgewählt wurden, und nicht an den vorgesehenen Begünstigten überwiesen werden.

Erteilung eines Zahlungsauftrags durch den Betrüger

„Erteilung eines Zahlungsauftrags durch den Betrüger“ ist eine Art nicht autorisierter Zahlungsvorgang im Sinne der Leitlinie 1.6 d) der EBA-Leitlinien zu den Meldeanforderungen für Betrugsdaten nach Artikel 96 Absatz 6 PSD2 (EBA-GL-2018-05) 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.

Diese Betrugsart ist für Überweisungen, kartengestützte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen relevant. Ein Beispiel ist die Situation in der ein Händler einen betrügerischen Zahlungsauftrag mit - aus einer früheren Transaktion gespeicherten - Anmeldedaten erstellt.

- Verlust oder Diebstahl einer (E-Geld-)Karte

Eine Betrugsart, die bei der Verwendung eines verlorenen oder gestohlenen kartenbasierten Zahlungsinstruments (Debit-, verzögerte Debit- oder Kreditkarte) ohne die tatsächliche, implizite oder scheinbare Berechtigung des Karteninhabers auftritt. Diese Betrugsart ist für kartenbasierte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen relevant.

- (E-Geld-)Karte nicht erhalten

Eine Betrugsart die ein kartengestütztes Zahlungsinstrument beschreibt, von dem der Zahler behauptete, dass es nicht empfangen wurde, obwohl der Zahlungsdienstleister (Emittent) des Zahlers bestätigt, dass es an den Zahler gesendet wurde (mit einer beliebigen Zustellungsmethode). Diese Betrugsart ist für kartengestützte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen relevant.

- Kartenfälschung bzw. gefälschte E-Geld-Karte

Eine Betrugsart, die die Verwendung eines veränderten oder illegal reproduzierten kartengestützten Zahlungsinstruments, einschließlich der Replikation oder Veränderung des Magnetstreifens oder der Prägung, beschreibt. Diese Betrugsart ist für kartengestützte Zahlungstransaktionen/E-Geld-Zahlungstransaktionen relevant. Typisch für solche Betrugsarten sind Situationen, in denen die Karteninformationen kopiert werden, indem ein Kartenlesegerät verwendet wird, das in betrügerischer Weise an einen Geldautomaten angeschlossen ist. Diese gestohlenen Informationen werden dann zur Herstellung einer gefälschten Karte verwendet.

- Diebstahl von Kartendaten

Diebstahl sensibler Zahlungsdaten gemäß der Definition in Artikel 4(32) der Richtlinie (EU) 2015/2366. Die sensiblen Zahlungsdaten beziehen sich in diesem Fall auf Daten über ein kartengestütztes Zahlungsinstrument. Diese Betrugsart ist für kartengestützte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen relevant. Ein Beispiel ist die Situation in der ein Händler einen betrügerischen Zahlungsauftrag mit Kartendaten erstellt, die aus einer früheren Transaktion gespeichert wurden. Bei E-Geld-Zahlungstransaktionen mit einer Karte ist dieser Betrugsfall als Diebstahl von E-Geld-Kartendaten zu verstehen, auch wenn eine gesonderte Definition dieses Betrugsfalls für E-Geld-Karten nicht in Anhang II der Verordnung enthalten ist. Im Falle des Diebstahls von E-Geldkartendaten beziehen sich die sensiblen Zahlungsdaten auf Daten auf der E-Geldkarte.

- Sonstige

Diese Betrugsart ist für kartengestützte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen relevant.

- Nicht autorisierter Zahlungsvorgang / Nicht autorisierte E-Geld-Kontotransaktion

Diese Betrugsart entspricht der Definition in Leitlinie 1.1. a. der EBA-Leitlinien zu den Meldeanforderungen für Betrugsdaten nach Artikel 96 Absatz 6 PSD2 (EBA-GL-2018-05). Diese Betrugsart ist für Lastschriften und E-Geld-Kontotransaktionen relevant. Bei Lastschriftbetrug ist dies eine nicht autorisierte Zahlungstransaktion, d.h. beispielsweise eine Zahlungstransaktion, bei der sich der Betrüger die IBAN des Zahlungsdienste-Nutzers verschafft und diese benutzt, um eine betrügerische Einzugsermächtigung zu erteilen, um seine eigene Stromrechnung über eine Lastschrift zu begleichen.

Manipulation des Zahlers durch den Betrüger

Darunter ist die "Manipulation des Zahlers" im Sinne der Leitlinie 1.1 b) der EBA-Leitlinien zu den Meldepflichten für Betrugsdaten nach Artikel 96 Absatz 6 der Richtlinie (EU) 2015/2366 zu verstehen.

Diese Betrugsart ist für Überweisungen, Lastschriften, kartengestützte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen relevant.

Betrüger gewinnen in der Regel das Vertrauen der Opfer und überzeugen sie, Gelder auf ein "sicheres" Konto zu überweisen, das sie kontrollieren. Ein Beispiel ist die Situation in der sich ein Betrüger als Geschäftsführer ausgibt und einen Sachbearbeiter überzeugt, einen Zahlungsauftrag zu erteilen.

Fälle, in denen der Zahlungsempfänger betrügerisch ist, z.B. weil er fiktive Waren oder Dienstleistungen verkauft, aber nicht direkt in den Zahlungsvorgang eingreift, fallen nicht in den Bereich der betrügerischen Transaktionen, die nach der Verordnung gemeldet werden müssen.

Ein Beispiel für betrügerische, kartengestützte Zahlungstransaktionen ist die Situation, in der ein Betrüger vorgibt, ein Vertreter eines Online-Autovermieters zu sein. Das Opfer wendet sich mit der Zahlungstransaktion an den Betrüger.

4.2 Starke Kundenauthentifizierung und Gründe für die Durchführung von Transaktionen ohne starke Kundenauthentifizierung

Authentifizierung

Starke Kundenauthentifizierung (SCA) bedeutet "starke Kundenauthentifizierung" gemäß der Definition in Artikel 4(30) der Richtlinie (EU) 2015/2366.

Nicht-starke Kundenauthentifizierung (NOSCA) bezieht sich auf Transaktionen, die gemäß Kapitel III der von der Kommission delegierten Verordnung (EU) 2018/389 von der starken Kundenauthentifizierung ausgenommen sind, sowie auf Transaktionen, für die die Bestimmungen in Artikel 97 Absatz 1 der Richtlinie (EU) 2015/2366 nicht gelten. Vom

Händler initiierte Transaktionen sowie andere Transaktionen, auf die SCA nicht anwendbar ist, sind eingeschlossen.

Grund für die Durchführung von Transaktionen ohne starke Kundenauthentifizierung

Kleinbetragszahlungen

Zahlungstransaktionen, für die die Ausnahme in Artikel 16 der delegierten Verordnung (EU) 2018/389 der Kommission gilt.

„Kleinbetragszahlungen“ gelten für Überweisungen, Kartenzahlungen und E-Geld-Zahlungstransaktionen.

Zahlungen an die eigene Person

Zahlungstransaktionen, für die die Ausnahme in Artikel 15 der delegierten Verordnung (EU) 2018/389 der Kommission gilt.

„Zahlungen an die eigene Person“ gelten für Überweisungen und E-Geld-Zahlungstransaktionen.

vertrauenswürdige Empfänger

Zahlungstransaktionen, für die die Ausnahme in Artikel 13 der delegierten Verordnung (EU) 2018/389 der Kommission gilt.

„Vertrauenswürdige Empfänger“ gelten für Überweisungen, kartenbasierte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen.

wiederkehrende Zahlungsvorgänge

Zahlungstransaktionen, für die die Ausnahme in Artikel 14 der delegierten Verordnung (EU) 2018/389 der Kommission gilt.

„Wiederkehrende Zahlungsvorgänge“ gelten für Überweisungen, kartenbasierte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen.

von Unternehmen genutzte sichere Zahlungsprozesse und -protokolle

Zahlungstransaktionen, für die die Ausnahme in Artikel 17 der delegierten Verordnung (EU) 2018/389 der Kommission gilt.

„Von Unternehmen genutzte sichere Zahlungsprozesse und -protokolle“ gelten für Überweisungen, kartengestützte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen.

Transaktionsrisikoanalyse

Zahlungstransaktionen, für die die Ausnahme in Artikel 18 der delegierten Verordnung (EU) 2018/389 der Kommission gilt.

„Transaktionsrisikoanalyse“ gilt für Überweisungen, kartengestützte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen.

kontaktlose Kleinbetragszahlungen

Kontaktlose Zahlungen, für die die Ausnahme in Artikel 11 der delegierten Verordnung (EU) 2018/389 der Kommission gilt.

„Kontaktlose Kleinbetragszahlungen“ gelten für Überweisungen, kartengestützte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen.

unbeaufsichtigte Terminals für Verkehrsnutzungsentgelte und Parkgebühren

Zahlungsvorgänge, für die die Ausnahme in Artikel 12 der delegierten Verordnung (EU) 2018/389 der Kommission gilt.

„Unbeaufsichtigte Terminals für Verkehrsnutzungsentgelte und Parkgebühren“ gilt für Überweisungen, kartenbasierte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen.

Andere Gründe für keine starke Kundenauthentifizierung

„Andere Gründe für keine starke Kundenauthentifizierung“ gilt für kartengestützte Zahlungstransaktionen und E-Geld-Zahlungstransaktionen, für die keiner der verbleibenden Gründe zutrifft. Ein Beispiel für solche Transaktionen ist eine kartenbasierte Zahlungstransaktion, die grenzüberschreitend außerhalb des EWR getätigt wurde, und bei der die betroffene Nicht-EWR-Gegenpartei SCA nicht unterstützt und nicht den PSD2-Anforderungen unterliegt (so genannte "One-Leg-In-Transaktionen").

Für Zahlungsdienstleister ist zusätzliche Zeit vorgesehen, um zu SCA-konformen Verfahren zu migrieren.

Beispiel betrügerische Überweisung ohne starke Kundenauthentifizierung

Wird daher bei den **betrügerischen gesendeten elektronischen Überweisungen** (unter CRTR0100BETRUG) angegeben, dass betrügerische Transaktionen ohne starke Kundenauthentifizierung durchgeführt wurden, ist gleichzeitig bei CRTR0101BETRUG anzugeben welche Gründe (Ausnahmen) es für die Durchführung von Transaktionen ohne starke Kundenauthentifizierung gegeben hat.

Beispiel betrügerische Kartenzahlung ohne starke Kundenauthentifizierung

Wird daher auf der **Issuing-Seite eine betrügerische Kartenzahlung ohne E-Geld** (unter POSISS0100BETRUG, POSISS0200BETRUG, POSISS0300BETRUG) ohne starke Kundenauthentifizierung gemeldet, ist unter POSISS0600BETRUG der Grund für die Durchführung von Transaktionen ohne starke Kundenauthentifizierung anzugeben. Im Fall von **betrügerischen E-Geld-Zahlungen** ohne starke Kundenauthentifizierung ist unter POSISS0400BETRUG oder POSISS0500BETRUG der Grund für die Durchführung von Transaktionen ohne starke Kundenauthentifizierung anzugeben.

Wird daher auf der **Acquiring-Seite eine betrügerische Kartenzahlung ohne E-Geld** (unter POSACQ0500BETRUG, POSACQ0600BETRUG, POSACQ0700BETRUG) ohne starke Kundenauthentifizierung gemeldet, ist unter POSACQ0800BETRUG der Grund für die Durchführung von Transaktionen ohne starke Kundenauthentifizierung anzugeben.

4.3 Ländergliederung

In der gesamten Meldung B5 ist folgende Ländergliederung anzugeben:

- Österreich
- Einzelländeraufschlüsselung für alle Länder des EWR
- „grenzüberschreitend außerhalb des EWR“ (X42)

4.4 Betrügerische Überweisungen, Lastschriften und Schecks

Grundsätzlich sind (betrügerische) Transaktionen von der Meldepflicht betroffen, die nicht den reinen Zwischenbankverkehr betreffen, d. h. es muss zumindest der ursprüngliche Auftraggeber einer Zahlungstransaktion oder der finale Empfänger der Transaktion ein Nicht-MFI sein. Sollte ein Institut ein Konto für ein anderes Institut führen (Nostro- bzw. Lorokonto), ist immer der Empfänger einer Überweisung meldepflichtig und nicht der Begünstigte.

Es sind sowohl (betrügerische) Zahlungstransaktionen für die Meldung relevant,

- die zwischen zwei bei verschiedenen Zahlungsdienstleistern geführten Konten erfolgen
- als auch solche Zahlungstransaktionen, die zwischen zwei bei demselben Zahlungsdienstleister geführten Konten abgewickelt werden.

(Betrügerische) Überweisungen, die zwischen verschiedenen Konten, die auf denselben Namen lauten und beim selben Zahlungsdienstleister geführt werden, sind ebenfalls zu erfassen. Der reine Bargeldtransfer ist für diese Meldung nicht relevant. Cash Pooling, sofern es keinen ausdrücklichen Auftrag des Kunden gibt und die Bank das Cash Pooling selbst vornimmt, ist auch nicht zu melden.

Im Fall von (betrügerischen) Überweisungen und ähnlichen Transaktionen, bei denen der Zahlungspflichtige die Transaktion einleitet, ist der (die Zahlungsanweisung) sendende Teilnehmer auch der Absender der Geldmittel und der empfangende Teilnehmer der Empfänger der Geldmittel (und der Zahlungsanweisung).

Im Fall von (betrügerischen) Lastschriften, Schecks, E-Geld-Zahlungen (serverbasierte E-Geldzahlungen) und ähnlichen Transaktionen, bei denen der Zahlungsempfänger die Transaktion einleitet, ist der (die Zahlungsanweisung) sendende Teilnehmer der Empfänger der Geldmittel und der (die Zahlungsanweisung) empfangende Teilnehmer der Absender der Geldmittel.

Gebühren auf Konten, Zins- und Dividendenzahlung der Bank sowie Auszahlung des Kreditbetrags auf das Girokonto des Kunden werden nicht als Überweisungen bzw. Lastschriften gezählt.

Stornierte Zahlungstransaktionen sind ausgeschlossen. Es sind nur Zahlungsvorgänge zu melden, die ausgelöst und ausgeführt (gegebenenfalls auch angenommen und abgerechnet) worden sind.

Zurückgewiesene (betrügerische) Überweisungen (im Falle einer Unterdeckung des Kontos) werden ebenfalls nicht gezählt, da sie auf der Sender-Seite zurückgewiesen werden. Zurückgewiesene (betrügerische) Lastschriften werden gezählt, da sie auf der Empfänger-Seite zurückgewiesen wurden (Auftrag wurde durchgeführt und erst dann zurückgewiesen). Die Zurückweisung der Lastschrift wird als solche nicht gemeldet.

Als ausgehende (betrügerische) Transaktionen bei den einzelnen Zahlungsarten wird folgendes verstanden:

- Ausgehende (betrügerische) Transaktionen zu Überweisungen werden auf der Seite des Zahlungspflichtigen gezählt;
- Ausgehende (betrügerische) Transaktionen zu Lastschriften werden auf der Seite des Zahlungsempfängers gezählt, d. h. es werden die ausgehenden Anweisungen (Aufträge) zu Lastschriften statistisch erfasst;
- Ausgehende (betrügerische) Transaktionen zu Schecks werden ebenfalls auf der Seite des Zahlungsempfängers gezählt;

Als eingehende (betrügerische) Transaktionen bei den diversen Zahlungsarten wird folgendes verstanden:

- Eingehende (betrügerische) Transaktionen zu Überweisungen werden auf der Seite des Zahlungsempfängers gezählt;
- Eingehende (betrügerische) Transaktionen zu Lastschriften werden auf der Seite des Zahlungspflichtigen gezählt, d. h. es werden die eingehenden Anweisungen (Aufträge) zu Lastschriften statistisch erfasst;
- Eingehende (betrügerische) Transaktionen zu Schecks werden ebenfalls auf der Seite des Zahlungspflichtigen gezählt;

Betrügerische Überweisungen

Überweisungen in Papierform (in Belegform) bzw. elektronisch (beleglos)

Beleglos (elektronisch) initiierte Überweisungen sind Überweisungen, die der Zahlungspflichtige nicht in Papierform einreicht, d. h. elektronisch. Enthalten sind:

- Einreichungen per Telefax oder sonstiger Kommunikationsmittel (wie automatisiertes Telefon-Banking), sofern sie ohne manuellen Eingriff in elektronische Zahlungen umgewandelt werden

- ~~Daueraufträge, die anfangs zwar in Papierform eingereicht wurden, in der Folge aber regelmäßig elektronisch ausgeführt werden~~
- Überweisungen, die durch einen Zahlungsdienstleister auf der Basis eines Finanzdienstes ausgeführt werden, wenn der Finanzdienst beleglos initiiert ist, oder die Form der Einreichung des Dienstes unbekannt ist, und der Zahlungsdienstleister die Überweisung elektronisch ausgeführt hat
- an einem Geldautomaten mit Überweisungsfunktion initiierte Überweisungen

Überweisungen in Papierform werden vom Zahler in Papierform oder durch die Anweisung an das Personal einer Filiale am Schalter veranlasst, und erfordern eine manuelle Bearbeitung. In Papierform eingereichten Daueraufträge werden als "Beleginitiierte Überweisungen" gemeldet.

gesendete Überweisungen (weder beleg- noch elektronisch initiiert)

Diese Aufschlüsselung umfasst alle Fälle von Überweisungen, die nicht elektronisch und nicht in Papierform veranlasst werden, z.B. MOTO-Transaktionen (Auftrag via Brief oder Telefon).

Mit und ohne Fernzahlung

Eine **Fernzahlungstransaktion** wird in Artikel 4 Absatz 6 der Richtlinie (EU) 2015/2366 definiert.

Nicht-Fernzahlungstransaktionen umfassen Zahlungstransaktionen an Terminals einschließlich solcher, die kontaktlose Technologie, Geldautomaten, POS-Terminals, unbeaufsichtigte Terminals und automatisierte Zahlungszentren verwenden.

Auf Online-Banking basierende Überweisung

Dazu gehören Transaktionen, bei denen der Zugriff auf die Online-Banking-Plattform über Webbrowser oder die mobile Online-Banking-App eines Zahlungsdiensteanbieters erfolgt. Überweisungen, die von Zahlungsauslösedienstleistern über die Online-Banking-Plattform der Anbieter von Kontodienstleistungen für Zahlungsdienste initiiert werden, sind hier ebenfalls eingeschlossen und werden zusätzlich in einer eigenen Untergliederung "von Zahlungsauslösedienstleister initiierte Überweisungen" gemeldet. Daher schließen sich diese Aufgliederungen nicht gegenseitig aus.

Zahlungen im E-Commerce

E-Commerce-Zahlungen beziehen sich auf alle auf Online-Banking basierenden Überweisungen, die im Zusammenhang mit einem "Verkauf oder Kauf von Waren oder Dienstleistungen, sei es zwischen Unternehmen, Haushalten, Einzelpersonen oder privaten Organisationen, durch elektronische Transaktionen über das Internet oder andere computervermittelte (Online-Kommunikations-)Netzwerke" initiiert wurden. Der Begriff umfasst die Bestellung von Waren und Dienstleistungen, die über Computernetzwerke versandt werden, wobei die Zahlung und die letztendliche Lieferung der Waren oder Dienstleistungen entweder online oder offline erfolgen kann".

E-Commerce-Zahlungen umfassen nur solche, die über Online-Banking initiiert werden, da E-Commerce eine Unterposition der auf Online-Banking basierenden Überweisung ist. Diese Aufgliederung umfasst nicht diejenigen E-Commerce-Transaktionen, die über andere Mittel als die in der Definition der auf Online-Banking basierenden Überweisung beschriebenen Wege eingeleitet werden. Da jedoch die von den Zahlungsauslösedienstleistern initiierten Überweisungen im Zusammenhang mit E-Commerce-Transaktionen sowohl über eine Online-Banking-Plattform initiiert werden als auch mit einem Kauf auf der Website eines Händlers verbunden sind, sind sie ebenfalls eingeschlossen. Transaktionen, bei denen Anbieter von Kontodienstleistungen für Zahlungsdienste als Zahlungsauslösedienstleister fungieren, um eine einfache Überweisung für ein Konto bei einer anderen ASPSP zu initiieren, sind nicht eingeschlossen.

gesendete Überweisungen (elektronisch/beleglos ausgelöst) - via ATM oder anderem Terminal

Diese Aufschlüsselung umfasst nur Überweisungen an physischen Terminals (keine Ferntransaktionen).

Mobile payment solution

Eine Lösung zur Initiierung von Zahlungen, bei der die Zahlungsdaten und die Zahlungsanweisungen mittels mobiler Kommunikations- und Datenübertragungstechnologie über ein mobiles Gerät übertragen und/oder bestätigt werden. Zu dieser Kategorie gehören digitale Brieftaschen und andere mobile Zahlungslösungen, die zur Initiierung von P2P- (Person-zu-Person) und/oder C2B- (Consumer-to-Business) Transaktionen, d.h. Überweisungen, Kartenzahlungen und/oder E-Geld-Transaktionen, verwendet werden.

Mobile Zahlungslösungen umfassen nur Ferntransaktionen über digitale Brieftaschen, C2B- und P2P-Mobilzahlungslösungen, während nur Transaktionen über P2P-Mobilzahlungslösungen separat ausgewiesen werden.

Eine digitale Brieftasche wird definiert als "eine Lösung, bei der Benutzer Daten registrieren können, die sich auf ein oder mehrere Zahlungsinstrumente oder Zahlungskonten beziehen, um die Initiierung von Zahlungstransaktionen zu ermöglichen".

Ausgeschlossen sind

- Transaktionen, die nicht aus der Ferne initiiert werden, z. B. an einem Geldautomaten oder einem anderen PSP-Terminal
- Überweisungen auf Basis von Online-Banking.

Überweisungen, die in der Mobile-Banking-App des Zahlungsdienstleisters ausgelöst werden, sind nur in der Untergliederung "Online-Banking-basierte Überweisungen" enthalten, da die Mobile-Banking-App lediglich eine alternative Schnittstelle ist, die die Auslösung von Online-Banking-basierten Zahlungen ermöglicht.

P2P-Lösung für mobile Zahlungen

Eine Lösung, bei der Zahlungen von einer Person an eine andere Person (P2P) über ein mobiles Gerät initiiert, bestätigt und/oder empfangen werden. Die Zahlungsanweisung und andere Zahlungsdaten werden mit einem mobilen Gerät übertragen und/oder bestätigt. Eine unverwechselbare mobile Zahlungskennung, wie z.B. Mobiltelefonnummer oder E-Mail-Adresse, kann als Proxy verwendet werden, um den Zahler und/oder Zahlungsempfänger zu identifizieren. Mobile P2P-Zahlungslösungen können verwendet werden, um Überweisungen, Kartenzahlungen und/oder E-Geld-Transaktionen zu veranlassen.

Nicht unter dieser Kategorie zu melden sind überweisungsbasierte P2P-Zahlungen

- die über die Mobile-Banking-App initiiert werden
- die über Online-Banking initiiert werden
- die an Geldautomaten oder anderen PSP-Terminals initiiert werden.

Unterscheidung der Meldung von P2P-Lösung für mobile Zahlungen im B4 bzw. im B1:

Im **B5** geht es wie im **B4** nur um gesendete Überweisungen. Die EZB konkretisiert: Überweisungsbasierte P2P-Zahlungen, die aus der Ferne über eine mobile Zahlungslösung initiiert werden, sollten in dieser Kategorie gemeldet werden. Eine mobile P2P-Zahlungslösung ermöglicht den Geldtransfer von Person zu Person unter Verwendung ihrer Zahlungskonten.

Im Gegensatz dazu sollten im **B1** kartenbasierte, aus der Ferne initiierte P2P-Zahlungstransaktionen, wie z.B. ZOIN, separat (unter POSIS6700 und POSIS6800) unter kartenbasierten Zahlungstransaktionen in der Unterkategorie "Mobile P2P-Zahlungslösung" gemeldet werden. Diese Transaktionen werden nach wie vor von der PSA gemeldet.

SEPA- und Nicht-SEPA-Verfahren

Die Meldung von Überweisungen ist zwischen SEPA- und Nicht-SEPA-Verfahren aufgeteilt und ist für jedes Verfahren gesondert zu melden. Internationale Verfahren für Überweisungen sind das **SEPA-CT-Verfahren** und das **SEPA-Sofort-CT-Verfahren**.

Unter „**Non SEPA Zahlungen**“ versteht man alle Zahlungen, die nicht den SEPA-Regularien unterliegen, das sind zum Beispiel Zahlungen in Nicht-SEPA-Länder (Auslandsüberweisung) und Fremdwährungsaufträge in Nicht-EUR-Währungen. Wenn hier ein eigenes Verfahren verwendet wird ist dieses Verfahren (im Schaubild als **NONSEPA1-n** gekennzeichnet) zu melden (bitte diesbezüglich um Rücksprache mit der OeNB).

Das SEPA sofort/instant One-Leg Out-Verfahren⁵ ermöglicht es Zahlungsdienstleistern für Sofortüberweisung im Euro-Leg, die bestehenden SEPA-Zahlungsinfrastrukturen zu nutzen.

⁵ [https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2023-03/EPC158-22%20v1.0%202023%20One-Leg%20Out%20Instant%20Credit%20Transfer%20\(OCT%20Inst\)%20Scheme%20Rulebook_0.pdf](https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2023-03/EPC158-22%20v1.0%202023%20One-Leg%20Out%20Instant%20Credit%20Transfer%20(OCT%20Inst)%20Scheme%20Rulebook_0.pdf)

Voraussetzung für eine One-Leg-Out-Transaktion:

- eine Transaktion in einer beliebigen Währung, sofern mindestens einer der beiden Teile auf Euro (Euro-Teil) lautet;
- es eine eingehende oder ausgehende Überweisung von Konto zu Konto ist;
- im Euro-Teil sofort rund um die Uhr an 365 Tagen im Jahr abgewickelt wird.

Die EZB erläutert, dass für den Spezialfall, wenn bei Transaktionen auf einer oder beiden Seiten Bargeld im Spiel ist und die Transaktion trotzdem als SEPA-Transaktion abgewickelt wird, diese Transaktion trotzdem als SEPA-Transaktion zu melden ist (SEPA end-date regulation 260/2012 und VERORDNUNG (EU) Nr. 1409/2013 der EZB zur Zahlungsverkehrsstatistik widersprechen sich hier geringfügig).

An **TARGET2**-Transaktionen sind in der Regel MFIs an beiden Enden der Transaktionen beteiligt (daher hier nicht meldepflichtig). Wenn es sich bei TARGET2-Transaktionen um Einzelhandelstransaktionen (von Nicht-MFIs) handelt, die über TARGET2 "gepusht" werden, sollten sie nach dem **jeweiligen Schema** (wenn ein Schema verwendet wird) oder als "**nicht anwendbar**" gemeldet werden.

Bei "On Us"-Transaktionen sollte das Dimensionsschema als "**Onus**" erfasst werden, wenn kein Clearing- und Settlement-System an der Verarbeitung der Transaktion beteiligt ist. Dies gilt unabhängig von dem für die Verarbeitung dieser Transaktionen angewandten Standard. Für andere Transaktionen, die nicht über ein Schema verarbeitet werden, sollte die Dimension des Schemas als "**nicht anwendbar**" gemeldet werden, unabhängig vom angewandten Standard.

Auch in Fällen, in denen das zur Verarbeitung der Transaktion verwendete Schema nicht bekannt ist, was z.B. bei Zahlungen über eine Korrespondenzbank der Fall sein könnte, sollte die Schemadimension als "**nicht anwendbar**" gemeldet werden. Für Transaktionen, die von Zahlungsauslösedienstleistern initiiert werden, sollte der gleiche Ansatz angewandt werden wie für Transaktionen, die von einer PSU initiiert werden.

STEP1 oder RT1 sind keine Non-SEPA-Verfahren, sondern Zahlungssysteme die SEPA-Verfahren nutzen. SWIFT gilt als technischer Standard (wir würden eine „NA“-Klassifizierung bei SWIFT-Transaktionen erwarten).

Initiierungsinstitut

~~Hier ist anzugeben welches Institut die Überweisung initiiert hat. Das kann ein Zahlungsauslösedienstleister (PISP) oder ein „herkömmlicher“ Zahlungsdienstleister (PSP) sein.~~

Abwicklung

Eine Überweisung kann als Einzel- oder Datei/Sammelabwicklung initiiert sein. Eine Datei/Sammelabwicklung ist eine beleglos initiierte Überweisung, die Teil einer Gruppe von

Überweisungen ist, die vom Zahlungspflichtigen gemeinsam initiiert werden. Jede Überweisung, die Teil einer Sammelüberweisung ist, wird als separate Überweisung gezählt, wenn die Anzahl der Transaktionen gemeldet wird.

Im Fall einer Überweisung über eine CD/Diskette, bei der nur eine Transaktion auf dem Medium gespeichert ist, gibt die EZB vor, dass dies auch unter Datei/Sammelabwicklung gemeldet werden soll.

Betrügerische Lastschriften

Sowohl wiederkehrende als auch "einmalige" Lastschriften sind eingeschlossen. Bei wiederkehrenden Lastschriften wird jede einzelne Lastschrift als ein Zahlungsvorgang gezählt. Lastschriften, die zur Begleichung ausstehender Salden aus Zahlungstransaktionen mit einer Kredit- oder verzögerten Debitkarte verwendet werden, sind ebenfalls eingeschlossen.

Einzel-/Sammelabwicklung

Eine **Sammelabwicklung** ist eine elektronisch initiierte Lastschrift, die Teil einer Gruppe von Lastschriften ist, die gemeinsam vom Zahlungsempfänger initiiert wurden. Jede in einer Sammelabwicklung enthaltene Lastschrift wird bei der Meldung der Anzahl der Transaktionen als separate Lastschrift gezählt.

Genehmigung zum Einzug

Es ist anzugeben, ob die Genehmigung zum Einzug über ein elektronisches Mandat erteilt wurde oder in einer anderen Form als einem elektronischen Mandat.

SEPA- und Nicht-SEPA-Verfahren

Die Meldung von Lastschriften ist zwischen SEPA- und Nicht-SEPA-Verfahren aufgeteilt und ist für jedes Verfahren gesondert zu melden. Internationale Verfahren für Lastschriften sind das SEPA-DD-Core-Verfahren und das SEPA-DD-B2B-Verfahren.

„**SEPA-B2B-Lastschriftverfahren**“ bedeutet "SEPA Business-to-Business-Lastschriftverfahren". Es handelt sich dabei um ein Zahlungsinstrument für Geschäftskunden, das dem Regelwerk für die Durchführung von Einzügen in Euro im gesamten SEPA-Raum von Konten, die für die Annahme von Einzügen bestimmt sind, unterliegt.

Das „**SEPA-Lastschrift Kernverfahren**“ ist das Zahlungsverfahren für SEPA-weite Lastschriften, wie es im Regelwerk für das SEPA-Kernlastschriftverfahren (SEPA Core Direct Debit Scheme Rulebook) festgelegt ist.

Nicht SEPA-Lastschriften

Bei On-Us-Transaktionen sollte das Dimensionsschema als "**Onus**" erfasst werden – wenn kein Geldtransfer zwischen Institutionen erfolgt. Dies gilt unabhängig von dem für die Verarbeitung dieser Transaktionen angewandten Standard. Für andere Transaktionen, die

nicht über ein Schema verarbeitet werden, sollte die Dimension des Schemas als "**nicht anwendbar**" gemeldet werden, unabhängig vom angewandten Standard. Auch in Fällen, in denen das zur Verarbeitung der Transaktion verwendete Schema nicht bekannt ist, sollte die Schemadimension als "nicht anwendbar" gemeldet werden.

Betrügerische Scheck-Zahlungen

Es ist immer das Land entscheidend, in dem der Kunde sein Bankkonto hat und nicht das Land, in dem der Kunde seinen Hauptwohnsitz hat.

Sonstige Zahlungsdienste (gesendet)

Jeder Zahlungsdienst, der in den Anwendungsbereich der Richtlinie (EU) 2015/2366 fällt, aber nicht in eine der anderen Kategorien von Zahlungsdiensten in Anhang III der EZB-Verordnung ECB/2013/43 in der Fassung vom 28 November 2013 aufgenommen werden kann. Andere Zahlungsdienste sind zum Beispiel Bargeldauszahlungen am Schalter.

Transaktionen über Telekommunikations-, Digital- oder IT-Geräte sind von diesem Punkt ausgenommen, da sie nicht als Zahlungsdienste gemäß PSD2 gelten. Die Rechnungsstellung durch den Carrier ist ebenfalls nicht in den sonstigen Zahlungsdiensten enthalten.

Bargeldüberweisungen/Finanztransfers

Dabei sind "Finanztransfers" im Sinne von Artikel 4(22) der Richtlinie (EU) 2015/2366 gemeint. Das bestimmende Merkmal einer Finanztransfers ist die Tatsache, dass Gelder von einem Zahler eingehen, ohne dass Zahlungskonten auf den Namen des Zahlers oder des Zahlungsempfängers eingerichtet werden. Bargeldüberweisungen werden nicht als Überweisungen gemeldet, da sie separat ausgewiesen werden.

Weitere Informationen finden sich auch in Erwägungsgrund (9) der Richtlinie (EU) 2015/2366 (PSD2): "Der Finanztransfer ist ein einfacher Zahlungsdienst, der in der Regel auf Bargeld beruht, das ein Zahler einem Zahlungsdienstleister zur Verfügung stellt, der den entsprechenden Betrag z.B. über ein Kommunikationsnetz an einen Zahlungsempfänger oder an einen anderen im Namen des Zahlungsempfängers handelnden Zahlungsdienstleister überweist. In einigen Mitgliedstaaten bieten Supermärkte, Händler und andere Einzelhändler der Öffentlichkeit eine entsprechende Dienstleistung an, die es ihnen ermöglicht, Versorgungsunternehmen und andere regelmäßige Haushaltsrechnungen zu bezahlen. Diese rechnungsbezahlenden Dienstleistungen sollten als Geldüberweisung behandelt werden, es sei denn, die zuständigen Behörden sind der Auffassung, dass die Tätigkeit unter einen anderen Zahlungsdienst fällt".

Das sowohl die Meldeposition „Finanztransfers“ im B1 wie auch die Meldeposition „Bargeldüberweisungen“ im B4 auf die Definition in Artikel 4(22) der Richtlinie (EU) 2015/2366 verweist sind die dazugehörigen Betrugsfälle im B5 zu melden. Die Unterschiede der Meldepositionen im B1 bzw. B4 werden in den jeweiligen Ausweisrichtlinien erklärt.

Transaktionen, die von Zahlungsauslösedienstleistern ausgelöst wurden

Vom Zahlungsauslösedienstleister sind über ihn ausgelöste Zahlungsvorgänge zu melden (CRRPISPBETRUGSCA und CRRPISPBETRUGNSCA).

Es ist auch anzugeben welche Zahlungsinstrumente verwendet werden. Die Dimension „andere“ kann „leer“ bleiben, wenn Zahlungsauslösedienstleister nur Überweisungen initiieren dürfen. Die Kategorie "andere" wäre nur zu befüllen, wenn es den Zahlungsauslösedienstleistern in Zukunft erlaubt wäre, andere Transaktionen als Überweisungen zu veranlassen.

Auch der Initiierungskanal (über Fernzahlungswege ausgelöst bzw. über Zahlungsweg ohne Fernzugang ausgelöst) ist anzugeben.

Die geografische Aufschlüsselung erfolgt auf der Grundlage des Landes, in dem das Konto liegt von dem aus die Zahlung veranlasst wird, um zu zeigen, in welchem Umfang diese Dienstleistung grenzüberschreitend erbracht wird.

4.5 Betrug ATM Bargeldbehebung - Issuermeldung

Hier sind aus Issuer-Sicht betrügerische Bargeldabhebungen mit kartengebundenen Zahlungsinstrumenten (ohne E-Geld-Transaktionen) anzugeben.

Einerseits erfolgt eine Aufgliederung in betrügerische Bargeldabhebungen mit Debitkarten, Kreditkarten ohne Kreditfunktion und Kreditkarten mit Kreditfunktion. Weiters ist das Land anzugeben, in dem sich die betrügerische Bargeldabhebung ereignet hat (Land des Terminals).

Andererseits ist über alle vorher angeführten Zahlungskarten (ohne E-Geld) anzugeben welche Betrugsart vorlag (ebenfalls unter Angabe des Landes, in dem sich der Betrug ereignet hat).

4.6 Betrug POS - Issuermeldung

Hier sind alle betrügerischen, kartengebundenen Zahlungsvorgänge mit, von inländischen Zahlungsdienstleistern ausgegebenen, kartengebundenen Zahlungsinstrumenten welche elektronisch initiiert sind zu melden, unterteilt in

- Debitkarte
- Kreditkarte ohne Kreditfunktion
- Kreditkarte mit Kreditfunktion

Sowohl in der EZB-Verordnung als auch in den EBA-Leitlinien ist festgelegt, dass betrügerischen, kartengebundenen Zahlungsvorgänge sowohl vom Issuer als auch vom Acquirer gemeldet werden sollten.

Hierfür ist auch eine Angabe der Systemkennung unter gleichzeitiger Angabe des Landes des Terminals und des Landes des Acquirers sowie ob es sich um eine Transaktion mit oder ohne starke Kundenauthentifizierung handelt sowie ob die Transaktion über Fernzahlungswege ausgelöst wurde oder nicht, erforderlich. Außerdem sind die unterschiedlichen Betrugsarten, anzugeben.

Aus welchen Gründen keine starke Kundenauthentifizierung durchgeführt wurde ist nicht nach Kartenfunktion (Debitkarte, Kreditkarte mit bzw. ohne Kreditfunktion) anzugeben, sondern gesammelt über alle Zahlungskarten (ohne E-Geld).

Betrügerische E-Geld-Zahlungsvorgänge mit, von inländischen Zahlungsdienstleistern ausgegebenem, E-Geld sind unterteilt in Transaktionen mit Karten, auf denen E-Geld direkt gespeichert werden kann (Betrag auf Chip) sowie Transaktionen mit E-Geld-Konten (serverbasiert). Hier ist die Angabe des Landes des Terminals und des Landes des Acquirers sowie ob es sich um eine Transaktion mit oder ohne starke Kundenauthentifizierung bzw. die Gründe für keine starke Kundenauthentifizierung sowie ob die Transaktion über Fernzahlungswege ausgelöst wurde oder nicht, erforderlich. Außerdem sind die unterschiedlichen Betrugsarten, anzugeben.

4.7 Betrug POS und ATM - Issuermeldung Details

Zusätzlich sind hier Details zu Betrug mit Zahlungskarten und E-Geld-Karten unter gleichzeitiger Angabe des Land des Terminals und des Landes des Acquirers zu melden. Folgende Definitionen sind anzuwenden:

Mobile Zahlungslösung

Eine Lösung zur Initiierung von Zahlungen, bei der die Zahlungsdaten und die Zahlungsanweisungen mittels mobiler Kommunikations- und Datenübertragungstechnologie über ein mobiles Gerät übertragen und/oder bestätigt werden. Zu dieser Kategorie gehören digitale Brieftaschen und andere mobile Zahlungslösungen, die zur Initiierung von P2P- (Person-zu-Person) und/oder C2B- (Consumer-to-Business) Transaktionen, d. h. Überweisungen, Kartenzahlungen und/oder E-Geld-Transaktionen, verwendet werden.

Mobile P2P Zahlungslösung

Eine Lösung, bei der Zahlungen von einer Person an eine andere Person (P2P) über ein mobiles Gerät initiiert, bestätigt und/oder empfangen werden. Die Zahlungsanweisung und andere Zahlungsdaten werden mit einem mobilen Gerät übertragen und/oder bestätigt. Eine unverwechselbare mobile Zahlungskennung, wie z.B. Mobiltelefonnummer oder E-Mail-Adresse, kann als Proxy verwendet werden, um den Zahler und/oder Zahlungsempfänger zu identifizieren. Mobile P2P-Zahlungslösungen können verwendet werden, um Überweisungen, Kartenzahlungen und/oder E-Geld-Transaktionen zu veranlassen.

Elektronische Initiierung von Kartentransaktionen

Kartenbasierte Zahlungstransaktionen, die an einem EFTPOS, einem Geldautomaten oder einem anderen physischen Terminal, das die elektronische Zahlungsinitiierung ermöglicht, oder aus der Ferne durch elektronische Mittel der Informationsübertragung initiiert werden.

Mit einem Imprinter (sog. „Ritsch-Ratsch-Geräte“) werden keine elektronischen Zahlungen ausgeführt, da es sich hierbei um papierbasierte Zahlungen handelt.

In Deutschland wird die Ansicht vertreten, dass auch Kreditkartenzahlungen mit Unterschrift ebenfalls nicht als elektronische Zahlungen anzusehen sind. Dieser Ansicht hat sich Österreich nicht angeschlossen. Somit gelten Kartenzahlungen, die via elektronischen Terminals initiiert wurden und nicht mit PIN, sondern mit Unterschrift „bestätigt“ wurden, im österreichischen Meldewesen auch als elektronische Zahlungen.

Fernzahlungstransaktion

Eine Fernzahlungstransaktion wird in Artikel 4 Absatz 6 der Richtlinie (EU) 2015/2366 definiert.

Nicht-Fernzahlungstransaktion

Nicht-Fernzahlungstransaktionen umfassen Zahlungstransaktionen an Terminals einschließlich solcher, die kontaktlose Technologie, Geldautomaten, POS-Terminals, unbeaufsichtigte Terminals und automatisierte Zahlungszentren verwenden.

Kontaktloses Zahlen/NFC

Grundsätzlich gilt: Bei der Bezahlungsfunktion wird unterschieden in „Kontaktloses Zahlen“ (NFC), „nicht kontaktloses Zahlen“ (NONFC) und das „kontaktlose Zahlen mit sonstigen Contactless-Funktionen“ wie Quick Response Codes und Bluetooth Low Energy (PROX)), bei denen der NFC-Chip in einem Gerät (Smartphone oder Smartwatch, etc.) eingebunden ist. Wenn die Karten beide Bezahlungsfunktionen unterstützen, dann werden diese Karten einmal mit dem Dimensionskürzel NFC und einmal mit NONFC gemeldet.

Im vorliegenden Fall sind unter „kontaktlose Zahlungen“ (ISS0401BETRUG) jene betrügerischen Transaktionen zu melden die mit NFC und sonstigen Contactless-Funktionen (Quick Response Codes und Bluetooth Low Energy, etc.) durchgeführt wurden. Unter der Hievon-Position NFC (ISS0402BETRUG) sind ausschließlich NFC-Zahlungen zu melden.

Zahlungen am ATM initiiert

Hier sind nur elektronisch initiierte Zahlungen am ATM mit Zahlungskarten (nicht über einen Fernzugang; ohne E-Geld) zu melden, nicht Ein- und Auszahlungen.

E-Geld-Zahlungstransaktionen

Eine E-Geld-Zahlungstransaktion ist ein Zahlungsvorgang unter Verwendung von "elektronischem Geld" gemäß der Definition in Artikel 2 Absatz 2 der Richtlinie 2009/110/EG.

nicht elektronisch initiiert (mit Fernzugriff)

Hier können MOTO-Transaktionen (Auftrag via Brief oder Telefon) gemeldet werden.

anders initiiert

Hier sind alle elektronisch initiierten Zahlungskartentransaktionen (mit / ohne Fernzugriff) zu melden, die weder am ATM noch am physischen EFTPOS initiiert wurden.

Sonstige

Unter Sonstige sind alle betrügerischen E-Geld-Zahlungsvorgänge mit, von inländischen Zahlungsdienstleistern ausgegebenem, E-Geld mit E-Geld-Konten gemeint, deren Verfügung nicht über Karten bzw. nicht über einen mobilen Zahlungsvorgang erfolgt.

4.8 Betrug POS – Acquirermeldung

Hier sind aus Acquirer-Sicht betrügerische Zahlungen mit kartengebundenen Zahlungsinstrumenten (ohne E-Geld-Transaktionen) anzugeben.

Sowohl in der EZB-Verordnung als auch in den EBA-Leitlinien ist festgelegt, dass betrügerischen, kartengebundenen Zahlungsvorgänge sowohl vom Issuer als auch vom Acquirer gemeldet werden sollten.

Einerseits erfolgt eine Aufgliederung in betrügerische Zahlungen mit Debitkarten, Kreditkarten ohne Kreditfunktion und Kreditkarten mit Kreditfunktion. Andererseits ist über alle Zahlungskarten (ohne E-Geld) hinweg anzugeben wie viele betrügerische Transaktionen elektronisch initiiert sowie ohne starker Kundenauthentifizierung registriert wurden. Ebenso ist über alle Zahlungskarten (ohne E-Geld) hinweg anzugeben wie viele betrügerische Zahlungen nicht elektronisch initiiert wurden.

Für alle diese Konzepte ist

- das Land anzugeben, in dem sich die betrügerische Zahlung ereignet hat (Land des Terminals) sowie aus welchem Land der Karten-Issuer stammt und
- ob die betrügerische Zahlung über Fernzahlungswege ausgelöst wurde oder nicht.

Für betrügerische Zahlungen mit Debitkarten, Kreditkarten ohne Kreditfunktion und Kreditkarten mit Kreditfunktion ist weiters anzugeben:

- die Systemerkennung der Karte
- ob die Zahlung mit oder ohne starke Kundenauthentifizierung initiiert wurde
- um welche Betrugsart es sich handelte

Für das Konzepte „Zahlungskarte (ohne E-Geld) elektronisch initiiert, ohne starker Kundenauthentifizierung“ ist der Grund für die Durchführung von Transaktionen ohne starke Kundenauthentifizierung anzugeben.

4.9 Betrug POS - Acquirermeldung Details

Hier sind aus Acquirer-Sicht über alle elektronischen Zahlungskarten (ohne E-Geld) hinweg die betrügerischen Transaktionen anzugeben inkl. der Information aus welchem Land der Karten-Issuer stammt bzw. in welchem Land der Terminal stand. Weiters ist anzugeben welche betrügerischen Zahlungen davon an einem

- physischen EFTPOS initiiert (non-remote)
- am ATM initiiert (non-remote)
- anders initiiert (non-remote)

wurden.

Die Kategorie „anders initiiert (non-remote)“ ist als Restgröße der Kartenzahlungen ohne Fernzugriff (nicht am EFTPOS bzw. am ATM initiiert) zu sehen.

4.10 Betrug Haftungsträger

„Verluste aufgrund von Betrug je Haftungsträger“ bezieht sich auf die Verluste des meldenden Zahlungsdienstleisters (PSP), seiner Zahlungsdienstnutzer (PSU) oder Dritten (THIRD), 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.

Diese Verluste müssen aufgegliedert werden in:

- gesendete Überweisungen Betrug
- gesendete Lastschriften Betrug
- Kartenzahlungen (ohne E-Geld) Issuer Betrug
- Kartenzahlungen (ohne E-Geld) Acquirer Betrug
- Behebung am ATM Betrug
- E-Geld-Zahlung Betrug

Hier ist keine Ländergliederung anzugeben. Es gilt immer „Inland und grenzüberschreitend kombiniert“.

4.11 Betrug via nicht kartengebundener Zahlungsdienste

Für die betrügerischen Transaktionen via nicht kartengebundener Zahlungsdienste haben Isser und Acquirer die Dimensionsausprägungen „Transaktionsart“ und „Systemerkennung“, sowie die Messgröße „Anzahl“ und „Betrag“ zu melden. Bei der Transaktionsart sind die

betrügerischen Transaktionen nach Issuer- und Acquirersicht ATM, POS und E-money zu melden. Dies gilt z.B. für die Systemerkennung Bluecode, Paybox, Daopay und Dimoco, für die die anderen Melde-Schaubilder im B5 nicht zutreffen.

5. Meldedimensionen

technische Dimensionskürzel und Dimensionsausprägungen

Langtext

WA

ANZ

BETR

Wertart

Anzahl

Betrag

SYSTS

SEPA

SEPAINST

NONSEPA1

NONSEPA2

NONSEPA3

ONUS

NOTA

Systemstandard

SEPA Zahlung

SEPA instant

Non SEPA Zahlungen

Non SEPA Zahlungen

Non SEPA Zahlungen

Non SEPA Zahlungen (on-us)

Non SEPA Zahlungen (nicht anwendbar)

SYSTS2

SEPADIDECS

SEPADIDEB2B

ONUS

NOTA

NONSEPADIDE

Systemstandard 2

SEPA Direct Debit Core scheme

SEPA Direct Debit B2B scheme

Non SEPA Direct Debit (on-us)

Non SEPA Direct Debit (nicht anwendbar)

~~Non SEPA direct debits~~

LD

AT

DE

BE

X42

etc.

Land Sender/Empfänger

Isocode Einzelland

Isocode Einzelland

Isocode Einzelland

grenzüberschreitend außerhalb des EWR

LDC

AT

DE

BE

X42

etc.

Land Sender/Empfänger

Isocode Einzelland

Isocode Einzelland

Isocode Einzelland

grenzüberschreitend außerhalb des EWR

AUTENT

NOSCA

SCA

Authentifikation

ohne starke Kundenauthentifizierung

mit starker Kundenauthentifizierung

INSTR

Zahlungsinstrument

CRTR
OTHER

Überweisung
andere

CHANNEL

REMOTE
NONREMOTE

Initiierungskanal

über Fernzahlungswege ausgelöst
über Zahlungsweg ohne Fernzugang ausgelöst

SYSTE

VISA
MASTERCARD
AMEXCO
DINERS
MAESTRO
PAYBOX
CUP
JCB
VPAY

ECCSH

EUFIS
EDEKA
DEBITMASTERC

Systemerkennung

Visa
MasterCard
American Express
Diners Club
Maestro
Paybox Credit Card - mobiles Zahlungsservice
China UnionPay
Japan Credit Bureau
Visa V Pay
Electronic Cash Karte der Deutschen
Kreditwirtschaft
EUFISERV Karte der European Savings Banks
Financial Services
EDEKA Gutscheinkarte
Debit MasterCard

EINZUG

ELEINZUG

Genehmigung zum Einzug

über elektronisches Mandat erteilte
Zustimmung
in einer anderen Form als einem
elektronischen Mandat
erteilte Zustimmung

OTHEREINZUG

Ausnahmen für eine starke

Kundenauthentifizierung

Kleinbetragszahlungen
Überweisungen zwischen Konten, die von
derselben natürlichen oder juristischen Person
gehalten werden
Vertrauenswürdige Empfänger
Wiederkehrende Zahlungsvorgänge
von Unternehmen genutzte sichere
Zahlungsprozesse und -protokolle
Transaktionsrisikoanalyse
Kontaktlose Zahlungen an der Verkaufsstelle
Unbeaufsichtigte Terminals für
Nutzungsentgelte und Parkgebühren
vom Händler ausgelöste Zahlungsvorgänge

NONSCA

LW

PTS

TB

RT

SCP

TRA

CLW

UTTPF

MIT

OTHER	Sonstige
ORIGINCT	Betrugsarten / Betrugsquelle Überweisungen
ISS	Erteilung eines Zahlungsauftrags durch den Betrüger
PMOD	Änderung eines Zahlungsauftrags durch den Betrüger
PMAN	Manipulation des Zahlers durch den Betrüger zur Erteilung eines Zahlungsauftrags
ORIGINDD	Betrugsarten / Betrugsquelle Lastschrift
UAP	Nicht autorisierte Zahlungstransaktion
PMAN	Manipulation des Zahlers
FRAUDTYP	Betrugsarten / Betrugsquelle
LOS	Verlust oder Diebstahl einer Karte
CNR	Karte nicht erhalten
CC	Kartenfälschung
OTHER	Sonstige
PMAN	Manipulation des Zahlers zur Bargeldabhebung
CDT	Diebstahl von Kartendaten
PMOD	Änderung eines Zahlungsauftrags durch den Betrüger
UAT	nicht autorisierte E-Geld-Kontotransaktion
POSTP	POS Typ
FACETOFACE	Face to Face = nicht über Fernzahlungswege ausgelöst
CARDNOTPRES	Card not present = über Fernzahlungswege ausgelöst
HAFTTRAEG	Verluste aufgrund von Betrug je Haftungsträger
PSP	der meldende Zahlungsdienstleister
PSU	der Zahlungsdienstnutzer (Zahler)
THIRD	Andere/Dritte