CORE®

EBA STARTET KONSULTATION ZU LEITLINIEN IM BERICHTSWESEN VON BETRUGSVORFÄLLEN IM ZAHLUNGSVERKEHR

Holger Friedrich
Dr. Waldemar Grudzien

August 2017
COREtechmonitor | Blogpost

Key Facts

- EBA veröffentlicht Entwurf mit Leitlinien für ein Berichtswesen von Vorfällen nach Artikel 96(6) der PSD II – Konsultation läuft bis zum 3. November, Empfehlungen gelten ab 13. Januar 2018
- Kontoinformationsdienstleister (AISP) von Regelung ausgenommen
- EBA gibt detaillierte Datenaufschlüsselung vor – Zahlungsdienstleister werden Berichtssystem anpassen oder aufbauen müssen
- EBA definiert „Betrug“ neu
- Unterschiedliche Berichtstiefen in Quartals- und Jahresbericht
- Bericht nur von ausgeführten, nicht von versuchten betrügerischen Transaktionen
- Bei Vorfällen mit Kartenzahlungen müssen Kartenausgeber und Kartenakzeptant berichten

Report

Wesentliche Inhalte

Gemäß Artikel 96(6) der PSD II müssen Zahlungsdienstleister den Aufsichtsbehörden mindestens einmal jährlich statistische Daten zu Betrugsfällen in Verbindung mit den unterschiedlichen Zahlungsmitteln vorlegen. Die betreffenden zuständigen Behörden stellen der EBA und der EZB diese Daten in aggregierter Form zur Verfügung.

Für beide benannte Meldeziele gibt die EBA in insgesamt 10 Empfehlungen – 7 für Zahlungsdienstleister und 3 für Aufsichtsbehörden – detaillierte Anforderungen vor. Kontoinformationsdienstleister sind von der Regulierung ausgenommen, da sie keine Zahlungstransaktionen ausführen und somit nicht zu betrügerischen Zahlungstransaktionen berichten können. Bezüglich der Tiefe der Datenaufschlüsselung unterscheidet die EBA zwischen sehr detaillierten jährlichen und weniger detaillierten vierteljährlichen Berichten. Darüber hinaus richtet sich die Tiefe der Datenaufschlüsselung nach dem angebotenen Zahlungsinstrument, so müssen zum Beispiel bei Finanztransfers und Lastschriften nur wenige grunsätzliche Daten berichtet werden, während bei Kartenzahlungen und Überweisungen sehr viele Informationen übermittelt werden müssen.

Die EBA stellt eine eigene Definition von „Betrug“ (Fraud) im Sinne der Verwendung in „betrügerischen Zahungstransaktionen“ auf. Demnach umfassen betrügerische Zahlungstransaktionen alle Arten von Zahlungsbetrug im Zahlungsmarkt. Hierzu zählt die EBA neben nicht autorisierten Transaktionen auch Betrug durch Manipulation des Zahlers sowie betrügerisches Handeln des Zahlers selbst. Abstrakte, frei interpretierbare und nicht eindeutig zurechenbare Begriffe wie „Phishing“, „Social Engineering“ oder „Trojaner“ werden bewusst nicht gebraucht; alle betrügerischen Transaktionen müssen unterschiedslos gemeldet werden. Stattdessen bietet die EBA eine neue, Technologie-

neutrale Kategorisierung an, die auf vier Attributen aufbaut:

- Ort in der Zahlungskette, an dem der Betrug stattfindet, z.B. der Zahlungsdienstleister von Zahler oder Zahlungsempfänger
- Authentifikationsart, die Betrug nicht verhindert hat, z.B. starke/nicht starke Authentifizierung
- Zahlungskanal, in dem der Betrug stattfand
- Weg, über den Betrüger sich Zugang zu geheimen Zahlungsdaten verschafft haben, z.B. Manipulation des Zahlers

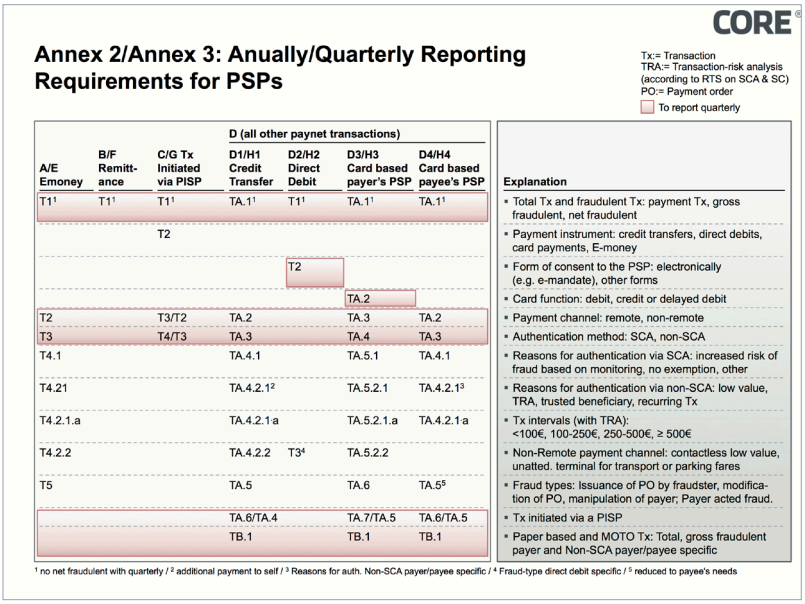
Betrügerische Kartenzahlungen müssen sowohl vom Zahlungsdienstleister des Zahlers als auch vom Zahlungsdienstleister des Empfängers gemeldet werden. So hofft die EBA, ein umfängliches Bild des Kartenbetrugs zu erhalten. Die Betrugsarten beim Kartenausgeber und beim Kartenakzeptanten können sich einerseits stark unterscheiden, andererseits können beide Endpunkte von den Erfahrungen des jeweiligen Anderen bei der Verhinderung neuer Betrugsarten lernen.

Dem Risiko des doppelten Zählens beim doppelten Bericht eines Vorfalls will die EBA Rechnung tragen, indem die Zahlen des gleichen Vorfalls nicht aufaddiert werden. Dabei formuliert sich die EBA geschickt um die Zuschreibung der Rechenarbeit herum. Zu hoffen ist, dass die Stelle, bei der beide Meldungen auflaufen, diese Logik installieren muss. Hierzu müssen sich die nationalen Aufsichten entsprechend aufstellen. Die gleiche Logik muss bei eine Zahlung initiierenden Zahlungsauslösediensten (PISP) und eine Zahlung ausführenden Zahlungsdiensten (ASPSP) angewendet werden.

Zur Entlastung der Zahlungsdienstleister verzichtet die EBA auf Berichte zum versuchten Betrug, nur tatsächlich ausgeführter Betrug muss berichtet werden. Hierbei muss jeder Vorfall in dem Berichtzeitraum erfasst werden, in dem er aufgetreten ist und nicht erst in dem Zeitraum, in dem der Vorfall geschlossen wurde. Interessant ist auch die Vorgabe zum Bericht von Bruttoverlust (vor z.B. Erstattung aus einer Versicherung) und Nettoverlust (der finale Verlust der beim Zahlungsdienstleister verbleibt). So erhofft die EBA weitere Erkenntnisse über die Effektivität von Authentifiezirungsmethoden, Betrugsüberwachungssystemen und weiteren Maßnahmen gewinnen zu können.

Der erste Quartalsbericht muss im zweiten Halbjahr 2018 an die nationale Aufsichtsbehörde übermittelt werden und Vorfälle ab dem 2. Quartal 2018 umfassen. Der erste Jahresbericht wird im ersten Halbjahr 2020 erwartet, er muss Vorfälle ab dem Gültigkeitszeitpunkt des technischen Regulierungsstandards zu starker Kundenauthentifizierung und -sicherer Kommunikation (RTS SCA&SC) enthalten. Nach heutiger Erwartung sollte dieses RTS ab Februar 2019 gültig sein.

Über das Berichtsformat und die Kommunikationsmittel können die Aufsichtsbehörden selbst entscheiden. Beides wird sich an den ebenfalls notwendigen Schittstellen zu Meldepflichten im bargeldlosen Zahlungsverkehr im Kontext PSD II orientieren müssen.



Annex 2/Annex 3: Anually/Quarterly Reporting Requirements for PSPs

Tx:= Transaction
TRA:= Transaction-risk analysis (according to RTS on SCA & SC)
PO:= Payment order
To report quarterly

			D (all other paynet transactions)				
A/E Emoney	B/F Remitt-ance	C/G Tx Initiated via PISP	D1/H1 Credit Transfer	D2/H2 Direct Debit	D3/H3 Card based payer's PSP	D4/H4 Card based payee's PSP	Explanation
T1[1]	T1[1]	T1[1]	TA.1[1]	T1[1]	TA.1[1]	TA.1[1]	• Total Tx and fraudulent Tx: payment Tx, gross fraudulent, net fraudulent
		T2					• Payment instrument: credit transfers, direct debits, card payments, E-money
				T2			• Form of consent to the PSP: electronically (e.g. e-mandate), other forms
					TA.2		• Card function: debit, credit or delayed debit
T2		T3/T2	TA.2		TA.3	TA.2	• Payment channel: remote, non-remote
T3		T4/T3	TA.3		TA.4	TA.3	• Authentication method: SCA, non-SCA
T4.1			TA.4.1		TA.5.1	TA.4.1	• Reasons for authentication via SCA: increased risk of fraud based on monitoring, no exemption, other
T4.21			TA.4.2.1[2]		TA.5.2.1	TA.4.2.1[3]	• Reasons for authentication via non-SCA: low value, TRA, trusted beneficiary, recurring Tx
T4.2.1.a			TA.4.2.1.a		TA.5.2.1.a	TA.4.2.1.a	• Tx intervals (with TRA): <100€, 100-250€, 250-500€, ≥ 500€
T4.2.2			TA.4.2.2	T3[4]	TA.5.2.2		• Non-Remote payment channel: contactless low value, unatted. terminal for transport or parking fares
T5			TA.5		TA.6	TA.5[5]	• Fraud types: Issuance of PO by fraudster, modification of PO, manipulation of payer; Payer acted fraud.
			TA.6/TA.4		TA.7/TA.5	TA.6/TA.5	• Tx initiated via a PISP
			TB.1		TB.1	TB.1	• Paper based and MOTO Tx: Total, gross fraudulent payer and Non-SCA payer/payee specific

[1] no net fraudulent with quarterly / [2] additional payment to self / [3] Reasons for auth. Non-SCA payer/payee specific / [4] Fraud-type direct debit specific / [5] reduced to payee's needs

Abbildung 1: Aufschlüsselung der Daten für jährliche und Quartalsberichte korrespondierend zu den Tabellen des EBA-Entwurfs

Vierteljährlich will sich die EBA einen statistisch unterlegten Überblick verschaffen zum Brutto/Netto-Verhältnis der Schadenstransaktionen, zum Zahlungskanal (fern ja/nein), zur Authentifizierungsmethode (stark ja/nein), zum Dienstleister (Zahlungsauslösedienst/Zahlungsdienst), zum Verhältnis elektronisch/nicht elektronisch initiierter Zahlungen, zum Einverständnis (E-Mandat ja/nein) und zur Kartenfunktion (Debit/div. Credit). Auf Basis dieser Daten wird über die Zeit ein Überblick über die tatsächlich auftretenden Schäden, Angriffsvektoren, Schwächen von Verfahren, Organisationen und Systemen des bargeldlosen Zahlungsverkehrs und die Wirkung von Maßnahmen möglich.

Fazit

Nach Auffassung der Autoren stellen die 10 Empfehlungen zum Berichtswesen eine logische und gute Fortführung zum Meldewesen von schwerwiegenden Zahlungsverkehrsvorfällen im bargeldlosen Zahlungsverkehr im Kontext der PSD II dar.

Auch die nationalen Aufsichtsbehörden müssen sich entsprechend dieser Elektrifizierungsbedarfe aufstellen. Für den Erfolg dieser und weiterer Pflichten kommt es maßgeblich darauf an, wie die nationalen Aufsichten, EBA und EZB die gesammelten Informationen der weiteren Auswertung und Operationalisierung zuführen. Sinnvoll wäre die Zurverfügungstellung der Daten an die Fachcommunity in geeigneter Form, um die Zahlungssysteme weiter zu härten und den eigenen Aufsichtsobjekten aktiv bei der Markt- und Produktgestaltung zu helfen.

Beide Anforderungsklassen (Meldung und Bericht) hätten Banken vor Jahren zu geringeren Kosten, zu geringeren organisatorischen Aufwänden und zu geringeren politischen Friktionen haben können. Nun gilt es, auch diese aus der PSD II entstandenen Pflichten in kurzer verbliebener Zeit umzusetzen. Die Anforderungen werden die Zahlungsdiensteanbieter zwingen, ihre IT- und Datenbanken-Infrastruktur weiter anzupassen. Im besten Fall sollten

alle Melde- und Berichtsanforderungen in einer Engine zusammengeführt werden, um den Aufwand für die verschiedenen, jedoch zumeist ähnlichen Melde- und Berichtsbedarfe möglichst gering zu halten.

Die durch Regulierung und Aufsicht forcierte Digitalisierung der Datengewinnung und Datenübermittlung bei Banken kann als Blaupause für die automatisierte Erhebung aller aufsichtsrelevanten Daten zur echtzeitfähigen, risikoadäquaten Bankenaufsicht dienen.

Quellen

Internet:

https://www.eba.europa.eu/news-press/calendar?p_p_id=8&_8_struts_action=%2Fcalendar%2Fview_event&_8_eventId=1917556

Vorausgehende Posts der Serie:

COREinsitute 2016/2017

https://www.coretechmonitor.com/de/finale-empfehlungen-der-eba-zu-meldepflichten-im-bargeldlosen-zahlungsverkehr-im-kontext-psd-ii/

https://www.coretechmonitor.com/de/meldepflichten-im-bargeldlosen-zahlungsverkehr-entwurf-neuer-empfehlungen-der-eba-im-kontext-psd-ii/

http://www.coretechmonitor.com/de/public-hearing-der-eba-zu-starker-authentifizierung-und-sicherer-kommunikation-im-rahmen-der-psd-ii/

http://www.coretechmonitor.com/de/auswirkungen-rts-psd-ii/

Autoren

Holger Friedrich verantwortet seit 2010 die Beratungseinheit von CORE. Er ist seit über 25 Jahren in der Softwareindustrie tätig. Vor der Gründung von CORE hat er ein Technologieunternehmen aufgebaut, wirkte in leitender Position bei marktführenden Technologieanbietern und war u.a. Partner in einer führenden internationalen Strategieberatung.

Mail: holger.friedrich@core.se

Holger Friedrich

Dr. Waldemar Grudzien setzt sich als Transformation Engineer mit den aktuellen regulatorischen Anforderungen und deren technischer Realisierung auseinander. Als promovierter Elektrotechniker war er als Leiter in einem nationalen Bankenverband für die Bereiche Retailbanking und Banktechnologien zuständig.

Mail: waldemar.grudzien@core.se

Dr. Waldemar Grudzien

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
https://institute.core.se
Phone: +49 30 26344 020
office@coreinstitute.org

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://www.core.se
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
https://www.core.se
Phone: +44 203 319 0356
office@coretransform.co.uk

COREtransform MEA LLC
DIFC – 105, Currency House, Tower 1
Dubai P.O. Box 506656 I UAE
https://www.core.se
Phone: +971 4 3230633
office@coretransform.ae