CORE®

EBA BEGINS TALKS ON GUIDELINES REGARDING REPORTING INCIDENTS OF PAYMENT FRAUD

Holger Friedrich
Dr. Waldemar Grudzien

August 2017
COREtechmonitor | Blogpost

Key Facts

- The EBA has published draft guidelines on fraud reporting requirements in accordance with Article 96(6) of PSD II – the talks run until November 3, recommendations will come into force as from January 13, 2018
- Account Information Service Providers (AISP) are excluded from regulation
- The EBA prescribes a detailed breakdown of data – payment service providers will need to make extensive changes to their reporting system or set one up
- The EBA redefines “fraud”
- Different scope of the reports, i.e. quarterly or annual report
- Report only on transactions that have actually been carried out, no report on attempted fraudulent transactions
- As regards incidents involving card payments, both the card issuer and the card acceptor are required to submit a report

Report

Key Points

In line with Article 96(6) of PSD II, payment service providers must submit statistical data on fraudulent cases according to different methods of payment to the supervisory authorities at least once each year. The relevant authorities concerned then send a summary of this information to the EBA and European Central Bank.

The EBA prescribes detailed requirements for a total of 10 recommendations for both of the aforementioned notification centers – 7 for payment service providers and 3 for supervisory authorities. AISPs are excluded from this regulation as they do not carry out payment transactions and cannot, therefore, report on fraudulent payment transactions. As far as the breakdown scope of data is concerned, the EBA distinguishes between very detailed annual reports and the less detailed quarterly reports. Furthermore, the used payment service stipulates how much information the data breakdown must contain. Hence, for example, very little basic data is reported concerning financial transfers and direct debits, whereas a lot of information has to be sent regarding card payments and bank transfers.

The EBA formulates its own definition of “fraud” within the context of use for “fraudulent payment transactions”. Accordingly, fraudulent payment transactions comprise all types of payment fraud that take place in the payments market, and include non-authorized transactions, fraud due to manipulation by the payer as well as fraudulent actions by the payer himself. Abstract terms which can neither be allocated clearly nor interpreted closely such as “phishing”, “social engineering” or “Trojans” are not used deliberately; all fraudulent transactions must be notified without any distinction made between one or the other. Instead,

the EBA is introducing a new technological-neutral category, which is based on four attributes:

- The place in the payment chain where the fraud takes place, e.g. payer's/payee's PSP
- The type of authentication which did not prevent fraud, e.g. SCA/non-SCA
- The payment channel which was host to the fraud
- The path used by the fraudster to access secret payment data, e.g. manipulation of the payer

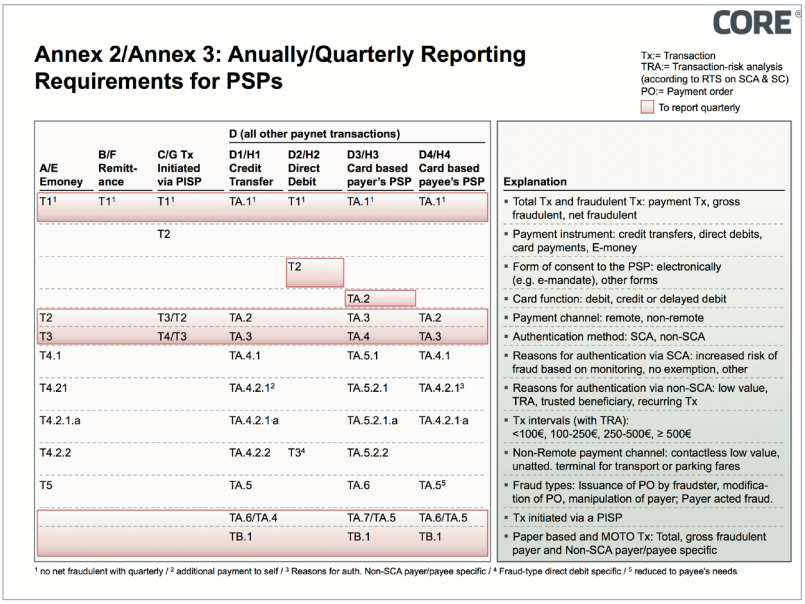
Fraudulent card payments need to be notified by both the payer's PSP and payee's PSP. The EBA thus hopes to gain an extensive understanding of card fraud. On the one hand, types of fraud can differ greatly depending on whether it happens to the card issuer or the card holder. Nevertheless, both end points can learn from the experiences of the other party in preventing new types of fraud.

The EBA intends to counter the risk of the number of fraud cases being counted twice when reported by both parties by not adding up the figures of the same case. The EBA gets around this cleverly as they do not allocate this work explicitly. It can only be hoped that the unit where both of these notifications are received has to install this logic. The national supervisory authorities will have to prepare themselves accordingly for this. The same logic will have to be used for any payment conducted by a payment initiation service provider (PISP) and for payment from an account servicing payment service provider (ASPSP).

The EBA is willing to waive the requirement to report on attempted fraud in order to take the pressure off payment service providers. Only actual cases of fraudulent activity need to be reported. Each case must be recorded during reporting period in which it occurs and not retrospectively (when the case has already been closed). The details pertaining to the reporting on gross (e.g. before insurance reimbursement) and net (final loss remaining with PSP) loss are also interesting, Through these, the EBA hopes to be able to gain further insight into the efficacy of authentication methods, fraud monitoring systems and other measures.

The initial quarterly report must be sent to the national supervisory authority in the second half of 2018 and will comprise incidents which have occurred since the second quarter of 2018. The first annual report is expected in the first half of 2020 and must include incidents regarding strong customer authentication and secure communication (RTS SCA&SC) which have happened ever since the Regulatory Technical Standards came into force. At the moment, it is expected that this RTS will come into force as from February 2019.

The supervisory authorities themselves are able to decide both what format the report shall take as well as the means of communication. Both will also need to be geared towards the necessary interfaces concerning reporting requirements for non-cash payment transactions in the context of PSD II.



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

Figure 1: Breakdown of data for annual and quarterly reports corresponding to the tables in the EBA Draft

The EBA wishes to get an overview, based on quarterly figures on the gross/net ratio of loss transactions, on the payment channel (remote yes/no), on the authentication method (strong yes/no), on the service provider (PISP/APSP), on the percentage of payments initiated electronically/non-electronically, on consent (e-mandate yes/no) and on the card function (debit/div. credit). Based on this data, it will be possible to have an idea over time of the number of losses actually occurring, attack vectors, weaknesses in processes, organizations and systems involving non-cash payment transactions as well as the impact of measures.

Conclusion

The authors believe that the ten recommendations on reporting represent a logical and sound continuation of the reporting of serious payment transaction incidents with non-cash payment transactions in the context of PSD II.

The national supervisory authorities also need to set themselves up to fulfill these electrification requirements. It is ultimately a matter of what the national supervisory authorities, the EBA and the ECB do with this collated data that will determine whether it will be a success along with further obligations. It would certainly be worthwhile if the data were to be made available to community insiders in an appropriate format in order to continue tempering payment systems and to actively assist with the supervisory authority's own objectives in shaping the market and the product.

Banks could have had both categories of requirements (notification and reporting) in place many years ago at a much lower cost, and having involved less organizational effort and less political friction. It is now a matter of also implementing these obligations arising from PSD II in the final remaining months. The requirements will force the payment

service providers to further adapt their IT and database infrastructure. In the best-case scenario, all notification and reporting requirements will be collated in one engine in order to reduce the effort to implement many different but mostly similar systems.

The digitalization of data recording and data transfer forced on banks as a result of regulations and supervisory authorities may serve as a blueprint for the automated collection of all data relevant to the supervisory authorities for the banking authority which is in real-time and risk-adequate.

Sources

Internet:

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

Previous posts in this series:

COREinsitute 2016/2017

https://www.coretechmonitor.com/final-recommendations-of-the-eba-on-notification-requirements-for-non-cash-transactions-in-the-context-of-psd-ii/

https://www.coretechmonitor.com/notification-requirements-for-cash-free-transactions-ebas-new-draft-recommendations-regarding-psd-ii/

https://www.coretechmonitor.com/eba-public-hearing-on-strong-customer-authentication-and-secure-communication-under-psd-ii/

https://www.coretechmonitor.com/impact-of-the-new-rts-regulatory-technical-standards-of-psd-ii/

Authors

Holger Friedrich has been in charge of our consulting unit since 2010. He was one of the founding members of the Institute for Theoretical Computer Science at the University of Potsdam (HPI). Before founding CORE, he set up a technology company and was a partner in a leading international strategic consulting firm.

Mail: holger.friedrich@core.se

Holger Friedrich

Dr. Waldemar Grudzien is a Transformation Engineer at CORE and focused on the security regulations of the nancial industry and their technological effects on IT infrastructures. During his work at a national federation of the nancial industries he was a specialist for retail banking and banking technologies. He graduated in electrical engineering at the TU Berlin.

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