CORE®

FINAL RECOMMENDATIONS OF THE EBA ON NOTIFICATION REQUIREMENTS FOR NON-CASH TRANSACTIONS IN THE CONTEXT OF PSD II

Christian Everts
Holger Friedrich
Dr. Waldemar Grudzien

July 2017
COREtechmonitor | Blogpost

Key Facts

- EBA publishes final document with recommendations for requirements applicable to a non-cash transaction reporting system for payment service providers and bank regulatory authority
- Final recommendations virtually unchanged from the draft recommendations published in December 2016
- EBA receives 43 comments on the draft recommendations
- Significant amendments relate to an extension of the notification deadline, an increase in the loss threshold, a new breakdown of the three reporting types and the delegation of notification requirements
- Further amendments were made in order to clarify definitions and specify terms that has previously only been outlined in brief

Report

1. Amendments to the draft

The deadline for initial notification has been significantly extended from 2 to 4 hours following identification of the incident. Due to reorganization of the three notification types, it is no longer necessary to provide as much information in the initial and interim notifications. This is due to the newly introduced "completion" of the notification forms, meaning that only the final report needs to contain all information pertaining to the incident. The criteria previously referred to as "Level 1" and "Level 2" proved insufficiently self-explanatory and have been replaced by the terms "Lower Impact Level" and "Higher Impact Level." For the Higher Impact Level criterion, the number of transactions concerned has been increased from one million to five million euros.

Also noteworthy is the decision of the EBA to lift the geographical restriction affecting the delegation of notification requirements to technical service providers, thus allowing the requirements to be delegated to such service providers outside the European Union. At the same time, the EBA is making it clear that the payment service provider is responsible for giving notification to regulatory authorities and that they should inform the regulator in advance of who is submitting notification on their behalf.

Clarifications and specifications that have a greater effect on the reporting burden relate to the scope of incidents subject to reporting requirements. Consequently, incidents that could have developed into a major incident – but that were resolved before this happened – no longer need to be reported. On the other hand, the EBA is making it clear that an incident already classed as "major" still needs to be reported even if it has been resolved within the first 4 hours. In this instance, the initial report may also include the interim and final reports.

In light of the changes, the final reporting regime of the EBA is as follows:

2. Classification of an incident

The EBA proposes a classification scheme with four quantitative criteria and three qualitative ones to decide whether an incident needs to be reported. These criteria are

- number of transactions in question
- number of clients involved
- service downtime
- economic impact
- level of internal escalation
- impact on other PSPs[1] / infrastructures?
- damage to reputation?

For the first four of these criteria, thresholds (in figures) are stated, with yes/no decision criteria for the other three – with the thresholds split into two levels. Depending on the number of criteria met and the threshold level, the incident is classified as either major or minor. An incident is deemed major if it meets at least one "Higher Impact Level" threshold, or at least three "Lower Impact Level" thresholds.

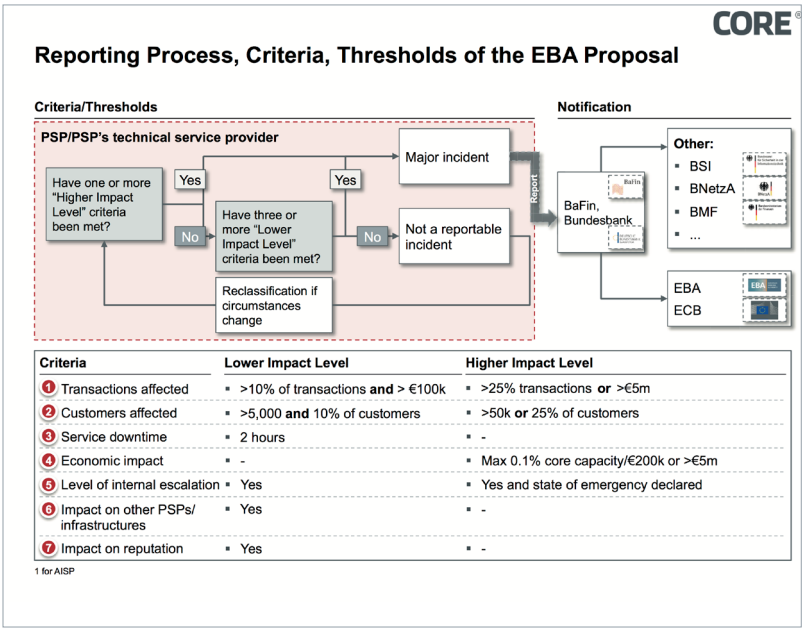

Figure 1: Mechanism for classifying operational and security incidents according to the severity of the effects

3. Reporting process

The EBA expects three types of report over the course of an incident:

Initial report
- What happened?
- Actual/possible effects
- Max. 4 hours after the incident has come to light

Intermediate report(s)
- If there is a significant change in the situation
- Max. 3 working days after initial report
- Last intermediate report when normal operations have been resumed

End report
- Full information about the incident that occurred
- Effects and resolution of the incident
- Max. 2 weeks after the incident has been dealt with

What is new is that the three notification types can now be combined, meaning that only the final report has to contain all information on the incident.

[1] PSP: Payment Service Provider according to PSD II

Furthermore, in the event that an incident could be resolved within 4 hours of coming to light, a final report should be submitted that also contains the information in the first and interim reports. A final report must also be submitted in the event that an incident initially classed as “major” has since been downgraded so that a report is no longer deemed necessary.

The payment service provider can delegate its reporting obligations to a technical service provider, either alone or in association with other payment service providers. However, the PSP is still responsible for ensuring major incidents are reported. The technical provider must no longer be based in the European Union. If several of its clients are affected by an incident, the provider may send the competent authority a single report for these payment service providers.

In line with guideline number 4, the EBA requires payment service providers to ensure that their operational and security policies specify all the responsibilities and processes for dealing with major incidents.

Besides these detailed requirements described for the reporting process from the payment service provider to the banking regulatory authority, the draft outlines how information on the major incident is to be shared between the national banking regulatory authority and other competent domestic bodies (Section 5) as well as the EBA and European Central Bank (Section 6).

For example, in the first case, if the stability of financial markets is threatened, the national banking regulatory authority may involve the treasury department or other bodies if the incident has already attracted wide media coverage. For both types of information sharing, more requirements are being imposed in terms of the confidentiality and integrity of the information shared.

Conclusion

The EBA’s requirements for a reporting system for non-cash transactions will mean that payment service providers will need to further adapt their IT and database infrastructure. As shown in Figure 2, there are currently several national and European initiatives on reporting requirements. The main challenge will be to bring together the various requirements within a unified reporting engine rather than, in the worst case, implementing a specific reporting process for each set of guidelines. In the past, that was often how things turned out.

With the help of effective fraud management systems, the decision to increase the loss threshold for the “Higher Impact Level” from one million to five million euros should reduce the number of major incidents.

Banks and payment service providers will now be more aware of the need to classify and report incidents as “major”, as all report types need to be submitted for incidents of this kind, even when the incident has been downgraded so that a report is no longer deemed necessary.

The lack of harmony between different reporting regimes should still be regarded as disadvantageous for the European banking industry.

In the view of the authors, the banks and their regulators should examine whether – as part of ongoing digitalization – the

reporting requirements could be converted to automated data-sharing models to facilitate continuous data collection on the part of the regulators. As demonstrated by account screening for more than a decade, it is not a question of technology, but rather of political and administrative will. The regulated bodies would therefore no longer need to set up a costly reporting and monitoring system and the regulators would no longer feel that they have to ask for information. The identifiable potential benefits lie in the huge cost savings and the quality improvements relating to all the risks quantifiable as part of bank governance.

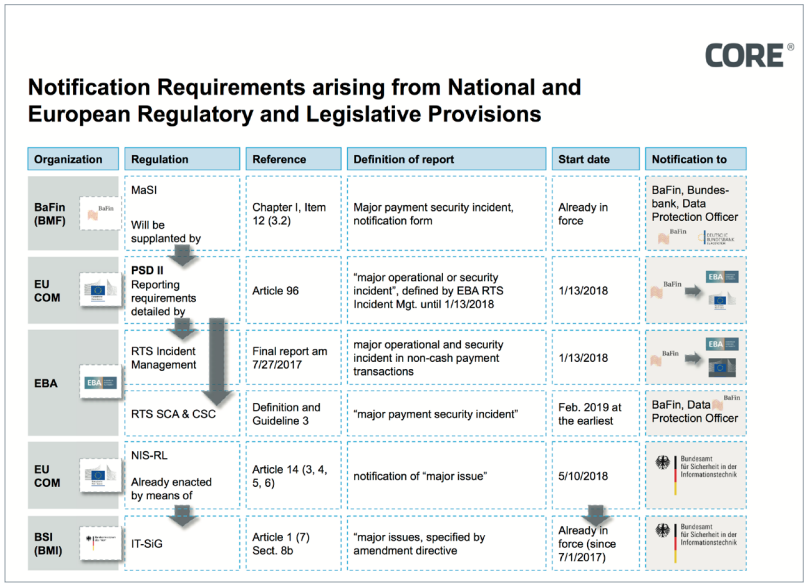

Figure 2: National and European reporting requirements

Sources

Internet:

https://www.eba.europa.eu/-/eba-publishes-final-guidelines-on-major-incident-reporting-under-psd2

Previous posts in this series:
COREinsitute 2016/2017

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/

https://www.coretechmonitor.com/it-security-act-new-requirements-for-critical-infrastructure-operators/

Authors

Christian Everts is a Transformation Manager at CORE and is particularly experienced in the field of regulation. Prior to joining CORE, Christian worked for several banks as a compliance manager, where he primarily implemented regulatory requirements in German and international investment and universal banks.

Mail: christian.everts@core.se

Christian Everts

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 financial industry and their technological effects on IT infrastructures. During his work at a national federation of the financial 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