NOTIFICATION REQUIREMENTS FOR CASH-FREE TRANSACTIONS:

EBA’s new draft recommendations regarding PSD II

Holger Friedrich
Dr. Waldemar Grudzien

14. Dezember 2016
COREtechmonitor | Blogpost

Key Facts

- EBA publishes a document with “recommendations” for requirements applicable to a cash-free transaction reporting system for payment service providers and bank regulators
- EBA provides a classification scheme based on 7 criteria and thresholds, as well as a detailed report form
- Payment service providers may delegate their reporting obligations to third parties, either alone, or together with other payment service providers

1. Classifying an incident

According to Article 96 of Payment Service Directive (PSD) II, payment service providers have until 13th January 2018 to implement a reporting system for major operational and security incidents relating to cash-free transactions. 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 / infrastructures in question
- reputational impact

For four of the criteria, thresholds (in figures) are stated, with yes/no decision criteria for the other three; the thresholds have two levels. Depending on the number of criteria met and the threshold level, the incident is classified as major or minor. An incident is deemed major if it meets at least one level 2 threshold, or three level 1 thresholds.

2. Reporting procedure

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

- Initial report
  - What happened?
  - Actual/possible effects
  - Max. 2 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

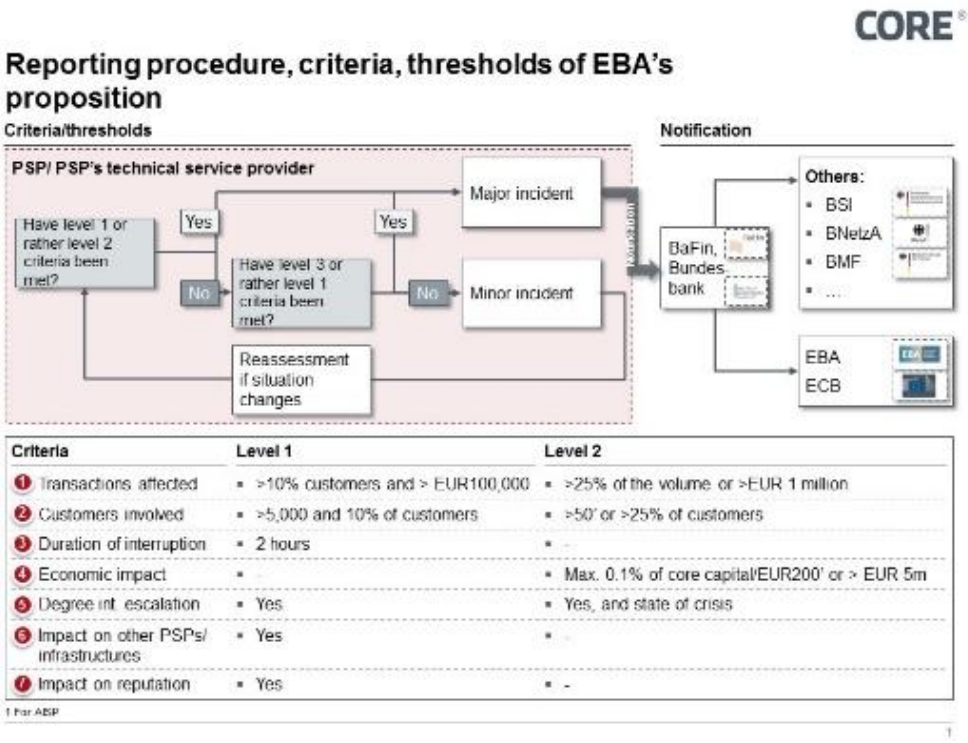

Figure 1: Mechanism for classifying operations and security incidents according to the severity of the effects

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. Such a provider must 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. Besides these detailed requirements as described for the reporting procedure, the draft outlines how information on the major incident is to be shared between the national banking regulator and other competent domestic bodies (Section 5) and information to be shared between national regulators and the EBA and European Central Bank (Section 6). For example, in the first case, if the stability of financial markets is threatened, the Treasury may be involved, or other bodies if the incident has attracted wide media coverage.

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

3. Comparison with MASI

In their final version, these Guidelines will replace the reporting requirements set out in MaSI (German acronym: Minimum requirements for the security of internet payments) on January 13, 2018. An initial comparison shows some common points, as well as differences:

- Report types:
  - Both sets of regulations lay down three types of report – initial, intermediate and end report
  - The EBA sets out concrete deadlines for the three report types, where BaFin's guidelines (the

German Federal Financial Supervisory Authority) are more flexible when it comes to report types

- Reporting deadline:
  - EBA expects the initial report two hours after the incident has been noticed
  - BaFin expects the initial report "immediately, that is, without undue delay, if banking processes are completely or partially interrupted, where it is clear that the downtime will exceed an hour".
  - The BaFin reporting deadline allows more freedom, but in the opinion of the authors, this also means the decision-making process becomes more complex in what may well be seen as a crisis situation
- Criteria for reporting decision:
  - EBA provides a concrete classification scheme with 7 criteria involving thresholds (in figures) and yes/no decisions, and two levels
  - BaFin employs an abstract definition of major payment security incidents that need to be reported – if the availability, integrity, confidentiality or authenticity of IT systems, applications or data with a high or very high protection requirement are compromised or reduced.
  - In this case too, the balance is between more freedom versus lower complexity under circumstances where it may be difficult to make a decision
- Delegation of reporting:
  - EBA and BaFin allow the requirement for reporting to be outsourced to an external IT service provider that handles the PSP's IT services.
  - However, BaFin places no geographical limitations on such IT service providers.
- Reporting form: EBA and BaFin both provide a reporting form.

4. Initial questions and suggestions

EBA's requirements for a reporting system for cash-free transactions will mean that payment service providers will need to adapt their IT and database infrastructure. As shown in Figure 2, there are currently several national and European initiatives on reporting requirements. In the opinion of the authors, 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 procedure for each set of guidelines. In the past, that was often how things turned out.

By allowing reporting requirements to be delegated to the technical service providers responsible for the PSP's IT service, EBA recognizes that external service providers can provide a better quality IT service. They are also able to understand and deal with an incident better than a payment service provider could. It is highly likely that this decision will set the tone for future relations between PSPs and service providers in areas other than those under consideration here. Examples to mention are cloud computing, and identity, authenticity and authorization service providers, with a massive increase in real-time requirements.

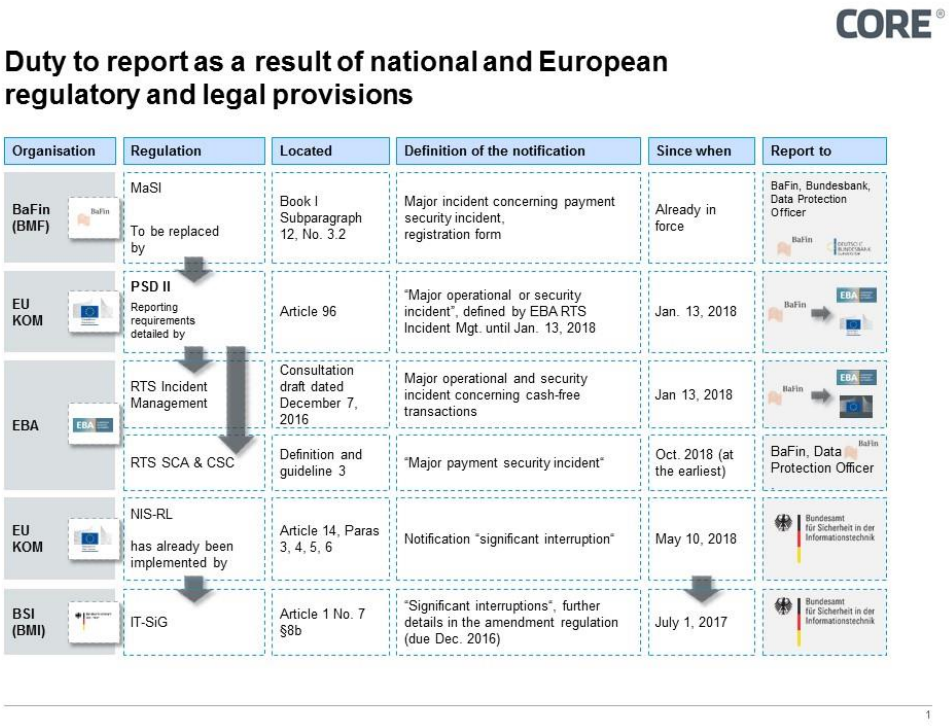

Figure 2: National and international report duties

EBA limits technical service providers to the European Union. Payment service providers are not allowed to choose providers from Norway, Switzerland or the USA. At the very least, it seems like a good idea to extend this to include the European Economic Area (EAR). EBA should also give due consideration to the impending exit of Great Britain. Another point is that EBA only permits providers to submit a single report covering several payment service providers if the latter are based in a single country. The thing to take into account here is that attacks often have international effects and may lead to the same incident affecting payment service providers from more than one country. A report covering the largest possible sphere of influence of an attack would give banking authorities a more comprehensive picture than if they simply received the report covering their own country.

5. Conclusion

Over the past few years, EBA has promised to produce these guidelines at the end of each year. The authors welcome the fact that they have finally been published, though the lengthy delay will lead to more, enormous challenges in the planning process of the German banking industry for the 2017 financial year. Indeed, as time has passed by, the majority of business models have moved towards comprehensive, deep-seated networking, or else the intensity of this trend has increased. It can, therefore, be assumed that the use of technology by both banks and clients will continue to proliferate markedly. In turn, this will lead to a greater number of incidents, and it also seems likely that the severity seen in some incidents will increase.
Consequently, it is reassuring if an industry, where business models are based predominantly on trust, sets a good example and focuses more on the opportunities created by

new regulatory requirements and the underlying technologies than their boards used to do in the past, when there was a greater focus on the risks.

However, the publication of this draft failed to address one aspect: the excessive regulatory burden on the financial sector. It would have had a structurally positive effect to produce a single binding set of reporting regulations, but that would only have been possible following on a national and European harmonization. Now, this harmonization will have to be brought about in the market by the payment service providers as they catch up. Efforts will need to be made to meet the extensive reporting requirements by using a single approach if possible.

An appropriate reporting system will not bring a bank any new customers or increased revenues. However, the reporting system fulfills regulatory requirements – and with in-depth preparation by IT – enables this to be combined with pending consolidation services featuring a higher level of service for technical functions as well as, subsequently, more efficient operating structures.

Sources

INTERNET:

https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

PREVIOUS POSTS IN THIS SERIES

COREinstitute 2016

http://www.coretechmonitor.com/eba-public-hearing-on-strong-customer-authentication-and-secure-communication-under-psd-ii/
http://www.coretechmonitor.com/impact-of-the-new-rts-regulatory-technical-standards-of-psd-ii/
http://www.coretechmonitor.com/it-security-act-new-requirements-for-critical-infrastructure-operators/

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@coretransform.com

Dr. Waldemar Grudzien is a Transformation Engineer at CORE. With a doctorate in electrical engineering and a degree in Business Administration, he has been a manager in a national banking association. A particular focus of Waldemar's is on security regulation and its technological effect on IT infrastructures.

Mail: waldemar.grudzien@coretransform.com

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
www.coreinstitute.org
Phone: +49 30 26344 020
office@coreinstitute.org

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

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

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