

2017-03-07

European Banking Authority

Consultation Paper on draft Guidelines on major incidents reporting under the Payment Services Directive 2

The Swedish Bankers' Association (SBA) appreciates the opportunity to comment upon the draft guidelines on major incidents reporting under the Payment Services Directive 2, the "Draft Guidelines". We have divided the answer into two parts: first, key comments we believe the European Banking Authority (EBA) should consider when developing the guidelines on incident reporting and second, answers to the EBA questions.

Key comments

1. It would be valuable for the European financial industry to receive feedback on the filed reports on some level. An idea could be to anonymize received reports and present an aggregated view regarding the outcome on major incidents. This could provide insights, lessons learned and knowledge sharing for the European financial industry without disclosing sensitive information. The benefits for the European financial industry are many and there are also benefits for European consumers in terms of enhanced consumer protection, while the expected additional workload for EBA or the local FSA is limited.
2. The SBA urges European authorities to harmonise all guidelines and definitions from the European ecosystem of regulatory authorities regarding incident reporting.

Answers to the EBA questions

Q1. Do you consider the definitions included in the draft Guidelines to be sufficiently clear?

The SBA supports the answer and view provided by the European Banking Federation (EBF) in their response to the Draft Guidelines, i. e. "we would propose to align them as much as possible with definitions already proposed by International bodies such as the ones proposed by the Bank for International Settlement, ENISA or ISO (information security definitions)". If there are reasons to choose other definitions we would like to understand the rational behind doing so.

The SBA suggests that the defintion of continuity should be amended the way the EBF proposes and thus read: "The property of an organisation being capable of delivering its payment-related services at acceptable predefined levels even if one or more components of the system fail or it it is affected by an abnormal external event. It includes both preventative measures and arrangements to deal with contingencies".

It is valuable if the term "designated third party" could be defined since it is used in many articles throughout the Draft Guidelines.

Q2. Do you consider the criteria and methodology applicable for the assessment and classification of an incident as major to be sufficiently clear? If not, what should be further clarified?

The SBA supports the answer provided by EBF.

Q3. Do you consider that the methodology will capture all of / more than / less than those incidents that are currently considered major? Please explain your reasoning.

We believe the methodology will capture all major incidents.

However, it remains unclear in the Draft Guidelines how financial institutions should reason when deciding if an incident is major or not.

For clarification purposes the text in subparagraph n 1.5 should be included in 1.3. The Diagram 1 (page 10) should also be included in the Draft Guidelines, near 1.3.

Q4. In particular, do you propose to add, amend and/or remove any of the thresholds referred to in Guideline 1.3? If so, please explain your reasoning.

The institutions covered by the reporting obligations in PSD2 are very different in nature and it is complex to build a framework relevant for all. As a consequence, thresholds are probably better reflected through percentages (%) and thus more appropriate than fixed numbers (euro). A percentage of clients, accounts etc. better reflects the magnitude of an impact on any financial institution regardless of size and nature while fixed numbers do not reflect the proportion. Percentages are better connected to the potential impact of an institution's operation while numbers are more theoretical in nature and less connected to a Payment Service Provider's business operations.

Q5. Do you think that the information depicted in the template in Annex 1 is sufficient to provide competent authorities in the home Member State with a suitable picture of the incident? If not, which changes would you introduce? Please explain your reasoning.

The SBA assumes that the purpose with the reporting is to identify and map potential problems and enhance security of the entire payment value chain. In that context the MS Excel-template will provide challenges for Payment Service Providers to identify which information should be included in the "initial", "intermediate" and "final" report and respond accordingly. Specifically, the MS Excel-template is too complex and may require the Payment Service Providers spending resources on correct reporting instead of correcting the problem. It is important not to create an administrative burden which runs the risk of shifting focus from fixing potential problems customers may be experiencing to compliance-activities driven by authorities' perceived need for insight. The more detailed the initial reporting requirements are the larger the risk for an unfocused response to the incident.

For the above reasons, the requirements on the format and content of the initial report should be limited to the absolute minimum. To get an appropriate picture of an incident the SBA suggests a more flexible report template. The SBA proposes that the initial report should include these records:

1. Payment Service Providers name and address.
2. Payment Service Providers contact details.
3. Describe the incident and the circumstances of how the incident was detected.
4. Describe what measures the Payment Service Providers is taking in response to the incident.
5. If possible, specify which thresholds were triggered.
6. Date and signature.

The advantage with this approach is obvious: it is quick, provides a heads up for competent authorities and thus fulfills the initial reporting objectives.

The intermediate report and final report can be more thorough for all Payment Service Providers and include the ideas and concepts proposed in the template Major Incident Report.

Q6. Are the instructions provided along with the template sufficiently clear and helpful to remove any doubts that could arise when completing the required fields? If not, please explain your reasoning.

Please also see answers for question 5.

The MS Excel-template is too complex and will require many hours to fill out correctly.

All categories should therefore be removed, e.g. the "Types of Incident" definitions should be changed and/or removed.

An idea could be to include the Security type of incident in the Operational part.

Furthermore, EBA should consider whether to change the expression "Acts of God", what is intended? Perhaps this could be changed to "external event" or "force majeure".

If any category should be included, it should preferably be in line with other guidelines.

We support the comment from the EBF that on the template itself, the wording "unique identification number" should be clarified and be replaced by commonly used terminology such as BIC.

Q7. As a general rule, do you consider the deadlines and circumstances that should trigger the submission of each type of report (i.e. initial, intermediate and final) feasible? If not, please provide a reasoning and justify any alternative proposal.

We would like to focus our comments on the initial report since the deadline requires a detailed notification immediately after the incident has been detected. It is likely that the required information to fully classify an incident may take a longer time to identify and establish depending on the internal organization at the Payment Service Provider and the fact that many people may be involved in addressing the issue. This implies that it can take some time before some critical parameters in the threshold table are known.

Therefore, the SBA proposes a more realistic alternative in which an initial report (see also Q5) is submitted as fast as possible and by the latest 24 hours after detection.

In order to clarify the paragraphs in the draft guidelines both 2.7 and 2.8 should have the wording “major incident” instead of “incident”.

The SBA also supports additional answers and views provided by the EBF in their response to question 7.

Q8. Do you consider that the delegated reporting procedure proposed in the draft Guidelines will provide added value to the market? Please explain your reasoning.

The SBA has no comments.

Q9. Do you consider that the consolidated reporting procedure proposed in the draft Guidelines will provide added value to the market? Please explain your reasoning.

The consolidated reporting procedure can add value if all participants in the payment value chain are included and covered.

SWEDISH BANKERS' ASSOCIATION

Hans Lindberg

Peter Göransson