European Payment Institutions Federation aisbl

European Payment Institutions Federation

14th December 2020

EPIF's response to EBA Revised Guidelines on major incident reporting

Response to the Consultation:

Q1. Do you agree with the change proposed in Guideline 1.4 to the absolute amount threshold of the criteria 'Transactions affected' in the higher impact level?

Yes, EPIF believes the revised thresholds in Guideline 1.4 are more appropriate. The proposed increase in absolute € value to €15M reflects a more proportionate materiality threshold for larger PSPs. The increased materiality threshold is consistent with the EBA's overall goal of "…to reduce the number of operational incidents that are required to be reported by no longer including those that do not have a significant impact on the operations of PSPs".

EPIF believes that the current impact levels are set quite low given the volume of payment transactions processed on a daily basis, which can result in a relatively minor operational event which impacts a small percentage of users/payment volume under the current threshold becomes reportable. Raising the absolute amount threshold of the criteria 'Transactions affected' in the higher impact level would result in the more accurate reporting of "major incidents".

In terms of "Transactions affected" and "Payment Service Users affected", we would also suggest that the guidance makes it clear that the reporting threshold is only triggered where the absolute threshold AND the percentage threshold is met. We believe that this would lead to the more accurate reporting of major incidents rather, as the revised threshold amounts could still result in the reporting threshold being hit for relatively minor operational and security incidents.

In addition, EPIF would also like to point out the problem with current methodology on calculating the value of 'Payment service users affected' specified in the Guideline 1.3.ii. The current methodology covers only customers that have a contract with the affected PSP that grants them access to the affected payment service. It does not include cases where there is no contract between the customer and the PSP (e.g. payment initiation services, single money remittance services or other services based on the single access or contract). As a result, the provision regarding only the contractual relationship between the PSP and the customer does not reflect the actual nature and scale of the incident (the customer is not always contractually linked to the PSP) and raises significant interpretation difficulties in this area in practice.. In addition, there are also significant difficulties in practice in determining who may suffer the consequences of a given incident, which is why EPIF considers that the methodology should be limited to payment service users who are indeed users and have been affected by the incident.

Therefore, in order to clarify this criterion, EPIF suggests taking into account the change of definition of the methodology used as follows (bold changes):

> [**Paragraph 1 of Guideline 1.3.ii**]
>
> "Payment service providers should understand as 'payment service users affected' all customers (either domestic or from abroad, consumers or corporates) **that the provider has granted**

access to the affected payment service, and that have suffered the consequences of the incident.

In circumstances where the actual number of payment services users who were impacted by the incident cannot be determined, payment service providers should resort to estimations based on past activity and taking into account the type of payment services provided so as to reflect the actual nature and scale of the impact of the incident on the payment services market.

[**Paragraph 3 of Guideline 1.3.ii**]

Furthermore, payment service providers should take as the total number of payment service users the aggregated figure of domestic and cross-border payment service users ~~contractually bound to them at the time of the incident (or, alternatively, the most recent figure available) and~~ availing of payment services ~~and with access to the affected payment service, regardless of their size or whether they are considered active or passive payment service users~~ from the payment service provider at the time of the incident.

Q2. Do you agree with the changes proposed in Guideline 1.4 to the assessment of the criteria 'Transactions affected' and 'Payment service users affected' in the lower impact level, including the introduction of the condition that the operational incidents must have a duration longer than one hour?

Yes, EPIF agrees with the changes proposed in Guideline 1.4 to the assessment of the criteria 'Transactions affected' and 'Payment service users affected' in the lower impact level, including the condition that operational incidents must have a duration longer than one hour. However, EPIF believes that the proposed re-wording of the criterion "high escalation" is not sufficiently clear. The reference to Guideline 60.d of EBA/GL/2019/04 is self-referential, as Guideline 60.d itself refers to "incidents with a potentially high adverse impact". So, the assessment of the severity of an incident for the purpose of major incident reporting cannot be classified by reference to "high adverse impact".

The observation that the criterion "high escalation" is often met in parallel with the criteria of "reputation" and of "economic impact" is explained by the fact that both criteria are not independent from each other. We believe that the classification of the severity of an incident should be based on criteria that are independent from each other. If criteria depend on each other, the match of one criterion in the lower class will always be "amplified" as the dependent criterion will also match.

We propose to withdraw the criterion "high escalation" entirely, because the escalation to senior management is a *consequence* of a severity and not a *condition* to the severity of an incident - such as Guideline 60.d of EBA/GL/2019/04 suggest as well.

Alternatively, we suggest a re-wording as follows:

"Payment service providers should consider whether, as a result of its impact on payment-related services, the management body as defined by EBA Guidelines on ICT and security risk management has been or will likely be informed, ~~in line with Guideline 60(d) of the EBA Guidelines on ICT and security risk management,~~ for exceptional reasons about the incident outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. Furthermore, payment service providers should consider whether, as a result of

the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered."

We also agree with the introduction of the condition that operational incidents must have a minimum duration of at least one hour. This change should reduce the number of reportable operational incidents for PSPs where disruptions are not considered to have a significant impact on the PSP or its users.

For EBA's consideration:

We suggest a change to the proposed lower impact conditions from "AND" to "OR" to the Transactions and Payment Service Users Affected illustrated below which requires PSPs to apply impact levels for each criteria individually as opposed to considering the impact levels as combined thresholds. This results in a loss of materiality for larger PSPs, where €500K and 5000 payment service users would not be considered of material significance when evaluating the impact of an incident relative to the size of larger PSPs (i.e. loss of proportionality).

> Example: *Currently PSPs are required to consider an incident for reporting if the incident impacts 10% of its users AND this equates to at least 5000 users. Under the proposed wording, PSPs will be required to consider the incident if the lesser of 10% OR 5000 users are impacted. Proportionality of the materiality for larger PSPs is lost under the proposed criteria and is contrary to the intention of the proposed guidelines.*

- It is proposed that the EBA reconsider the introduction of the condition "OR" and keep the use of "AND" for both Transactions and Payment Service Users Affected.
- EBA might also consider removing the set €500K and 5000 payment service users impact in entirety which will allow PSPs to report proportionate to their size applying only a % threshold relative to the size of the PSP in all cases.

In addition, further clarification would be beneficial regarding introduction of condition that the operational incidents must have a duration longer than 1 hour is requested, to understand the differentiation between 1 hour for operational incidents impacting payment processing versus 2 hours for service downtime

To minimize conflicting assessment and potentially over-reporting, it would be beneficial to align both periods to the existing service downtime period of 2 hours.

Q3. Do you agree with the inclusion of the new criterion 'Breach of security measures' in Guidelines 1.2, 1.3 and 1.4?

EPIF is strongly concerned about the inclusion of the new criterion "breach of security measures" in Guideline 1.3 on the basis that this broadens the scope and complexity of the process of determining whether a major reportable incident has occurred. The wording of the new criterion is so broad that it seems likely that any kind of security issue would result in this lower impact level always being met, which has the impact of lowering the reporting threshold and will result in non-major incidents being reported.

For sake of clarity, this does *not* mean that EPIF has any objections that security incidents should be reported. EPIF understands that, a breach of security measures must be reported already under the existing guidelines, when the incident is classified as "major". EPIF's concerns are, this new criterion does not appropriately reflect the *severity* of an incident.

First, it is unclear how this new criterion is defined. In para. 18, the EBA refers to Guideline 3.4.1 in EBA/GL/2019/04 to define a “breach of security measures”. However, Guideline 3.4.1 in EBA/GL/2019/04 covers a number of security measures, and it is unclear which of these to focus on, nor how to classify incidents based on their impact to the controls mentioned. EPIF asks for additional clarity in this regard.

Secondly, the EBA suggests in para. 8 that there are security incidents which "would not qualify as major but that are "material". However, the EBA does not provide sound evidence for the existence of such security incidents and does not provide any criteria by which they assess a security incident as "material". It is not clear which of the existing major incident reporting criteria fail to recognise security incidents as “material” or “major”, i.e. what type of severe security incidents would ***not*** be captured by applying the existing reporting criteria. EPIF would welcome additional rationale for how the proposed inclusion will help "capture additional security incidents that the EBA deems material", as stated by the EBA in para. 14. With regard to the individual criteria and thresholds used, the EBA considered that minor amendments in some thresholds may be needed in order to (i) avoid capturing operational incidents without a significant impact and (ii) to capture additional security incidents that the EBA deems material” (page 7, point 14 of the CP). However, EBA does not clarify which of the existing reporting criteria do ***fail*** to capture the “material” security breaches, nor specify what type of security breaches it took into consideration when revising the guidelines.

Moreover, in para. 11, the EBA states that "some of the security incidents appear not to be captured by the current criteria and thresholds", without providing any evidence for any underreporting of security incidents. Particularly the EBA does not provide any evidence about which of the existing criteria fail to classify security incidents as "major", i.e. which sort of security incidents would not be captured by the existing criteria.

In para. 17, the EBA furthermore refers to "relevant security incidents that would be of interest to Competent Authorities". The PSD2 however does not provide a basis for reporting of "relevant" incidents, and the EBA does not provide any rationale for when an incident would be deemed as “relevant”, nor what the "interest to Competent Authorities" would entail (if not severity of the incident).

As regards the proposed criterion, EPIF deems the criterion inappropriate and unsuitable:

- The proposed criterion refers to ***causes*** of an incident as opposed to the other criteria referring to the ***impact*** of an incident. As the EBA states in para. 2, the objective of the Major Incident Report is to "ensure that the damage to users [...] is kept to a minimum". Accordingly, the assessment criteria should be based on the impact rather than on the cause of an incident. The severity of an incident is independent from its cause and the sole fact that an incident is caused by a breach of certain security measures does not make this incident "material" in the meaning of potential damage.
- The criterion is not suitable to make an assessment whether the incident shall be classified as major, as the root cause is regularly not known during the incident and only known after thorough investigations. The classification as "major" will therefore regularly be determined when the Incident is resolved.

On the whole: EPIF fully agrees with EBA’s intention to make enhancements in the criteria, with the objective to ensure “security breaches” will be reported, when payment service users are adversely

affected, damaged or harmed etc.. However, the current drafting given in the Consultation Paper is very broad and does not provide any objective criteria by which EBA assess a security incident - when caused by a breach of security measures - as "material". More general, EPIF does not recognize that the drafted Guideline provides objective criteria to capture security incidents that the EBA deems material, or criteria against which such incidents can be assessed for reporting to competent authorities. Accordingly, EPIF asks

- that EBA provide greater elaboration on what is proposed to be captured by this proposal, providing clear examples for incidents, which fail to meet the current criteria, but are severe .
- that objective criteria be included as part of the guidelines against which security incidents can be assessed.
- that these criteria should be based on the measurement of the adverse ***effect,*** an incident has on payment services users, payment institutions etc.

Q4. Do you agree with the proposed changes to the Guidelines aimed at addressing the deficiencies in the reporting process?

Yes, EPIF agrees with the proposed changes aimed at addressing the deficiencies in the reporting process.

Reporting after the incident has been classified as major and when you know that the reporting channels of the regulatory authority is operational is far more practical than trying to adhere to the previous requirements. However we believe that under requirement 3.6 that major incidents affecting functions outsourced by payment service providers to third parties and that these incidents should also be communicated from PSPs to NCAs, that PSP should legally ask their outsource entities to report incident as opposed to report by PSPs.

Q5. Do you support the introduction of a standardised file for submission of incident reports from payment service providers to national competent authorities? If so, what type of structured file format would you support (e.g. “MS Excel”, “xbrl”, “xml”) and why?

Yes, EPIF supports the introduction of a standardized file for submission of incident reports from payment service providers to national competent authorities. EPIF would support any widely used format, insofar that it is supported by all Competent Authorities across the EU.

We would support a [MS Excel] file format that can be uploaded to the national competent authority. MS Excel is a file format that most people are familiar with and can navigate easily. There should be an option for supporting material to be appended where required given that MS Excel is not conducive to long pieces of text.

An MS Excel template is simple to populate and a standard for other regulatory reporting requirements. We suggest that the Excel template include formattable “free comments sections” for a better user experience when completing the template.

If more complex format is to be introduced, it will reduce simplicity and speed of the reporting process

It would be highly beneficial to reduce restrictions within reporting template and allow a more enriched user experiences for data input into description field which are mainly merged and hard to manipulate.

Q6. Do you agree with the proposed changes to Guidelines 2.4, 2.7, 2.12, 2.14, and 2.18 that are aimed at simplifying the process of reporting major incidents under PSD2?

Yes, EPIF agrees with the proposed changes aimed at simplifying the process of reporting major incidents under PSD2.

We agree with the proposed changes to Guidelines 2.4 (providing additional documents to complement the information in the notification file where requested to do so), 2.7 (timing of submission), 2.12 (intermediate report to be filed within 3 working days of initial report), 2.14 (Updating information in template when they become aware of significant changes since the submission of the previous report and submit an intermediate report when requested to do so) and 2.18 (submission of final report in a max of 20 working days after business is deemed back to normal). We believe this would simplify the process of reporting major incidents under PSD2 due to the following:

- 2.4. A use of standardized reporting template will improve the quality of the reports submitted and will simplify the reporting process for PSPs.
- 2.7. A proposed assignment of the unique incident reference code by the national competent authority will enhance traceability of incidents for competent authorities and reduce misunderstanding between competent authorities and PSPs when dealing with multiple incidents.
- 2.12 and 2.14. The proposed removal of the obligation for PSPs to provide updates to the intermediate reports every 3 working days reduces administration efforts associated with major incident management and shifts the focus appropriately to major developments / updates competent authorities are required to be informed of.
- 2.18. The extension of the final report submission to 20 working days after business is deemed back to normal allows PSPs with more time to conclude investigations and root cause analysis necessary required for final reporting.

Q7. Do you agree with the proposed changes to the templates in the Annex to the Guidelines?

Yes, EPIF agrees with the proposed changes to the templates in the Annex to the Guidelines since the introduced changes will improve the quality of the reports submitted to national competent authorities (e.g. removing fields that have little added value for the reporting and are of limited use for competent authorities).

We do think it will be necessary in some cases to provide supporting documentation, particularly in order to adequately address the “Root Cause Analysis and Follow Up” section in the Final Report as the current checkbox response format is unlikely to provide a full picture of the incident.