ASOCIACIÓN ESPAÑOLA DE BANCA

Response to EBA revised GL on major incident reporting under PSD2

11th December 2020

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?

The rise up of the threshold from 5M to 15M € in the higher impact level is a step in the right direction in order to report the real critical operational/technical incidents. Still there is margin to increase this threshold of 15M to 20-30M, thinking of gross settlement payments examples, and having into account that there is no discrimination for the transactions affected whether they are only delayed beyond the SLAs or they are not executed (which is clearly a more critical incident).

Given the heterogeneity of entities that report information to the CA, one single and static criteria for all PSPs might not be equally representative of the criticality. In this regard, alternative references such as a percentage of the entity's average daily transactions value (for example, 5% for lower impact level and 10% for higher impact level) should be considered. If this solution is not to be adopted, at least the threshold amount for a single transaction should not be an isolated trigger.

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?

The rise up of the threshold in 'Transactions affected' from 100k to 500k € in the lower impact level is a step in the right direction, in order to report the real critical operational/technical incidents. Still there is margin to increase this threshold up to 1M€, thinking on gross settlement payments examples, and having into account that there is no discrimination for the transactions affected whether they are only delayed beyond the SLAs or they are not executed (which is clearly a more critical incident).

As pointed in Q1, given the heterogeneity of entities that report information to the CA, one single and static criteria for all PSPs might not be equally representative of the criticality. In this regard, alternative references such as a percentage of the entity's average daily transactions value (for example, 5% for lower impact level and 10% for higher impact level) should be considered.

Additionally, the added condition of incident duration longer than one hour for both 'Transactions affected' and 'Payment service users affected' is quite rational. As EBA guidelines states, this is just specifically for operational incidents (that affect the ability of the payment service provider to initiate and/or process transactions). Those solved in less than 1 hour, are not significant enough to be reported to NCAs.

Yet, references such as a percentage of the PSP's average daily transaction volume should be considered as an alternative to further threshold increase, in order to avoid a number of less significant incidents either for banks or customers to be reported.

Q3. Do you agree with the inclusion of the new criterion 'Breach of security measures' in Guidelines 1.2, 1.3 and 1.4? (Breach of security measures' to be included in the Guidelines. This criterion is suggested to have a lower impact level only. In order to trigger a major incident report, this criterion would need to be used in combination with two other criteria from the lower impact level)

The proposed criterion seems a quite rational complementary condition to report critical security incidents in payments. Nevertheless, it would mean that more critical security incidents triggered to be reported to CAs that could be shared among different authorities according to the EU countries in the framework of EBA/GL/2018/05 and NIS Directive 2016/1148. Having said that, it would add complexity to the major incident reporting obligations under the PSD2 and could result in double reporting obligations whenever they are also to be reported under the mentioned regulations.

If such criterion is kept, clarification from EBA would be welcomed concerning the limited responsibilities of PSPs to report their own incidents when the security breach is suffered, not by the PSP itself (PSP systems are not compromised in any way) but by the customers, either retail or corporations, that might represent a potential fraud to the customers. This would not provide additional information since it is already reported under other PSD2 obligations EBA/GL/2018/05. The same is valid for incidents suffered by other third parties such as market infrastructures. Those will have direct reporting obligation.

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

All the changes to achieve clarity, simplification, and standardization among EU countries are highly appreciated. Additionally, more alignment with other EU incident reporting regulations is expected for the new modifications.

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?

MS Excel or XBRL/XML formats are supported although MS Excel allows manual feeding of information and facilitate timely reports in due form. It allows all PSPs size to easily implement the standardised form.

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?

All the changes to achieve more simplification and standardization among EU countries are highly appreciated, and the suggested changes will certainly contribute to it. Still, more alignment with other EU incident reporting regulations is expected in the new modifications.

Also, the simplification of a unique intermediate report (not a report to be sent every 3 days) and the extended of the deadlines to send the final report are appreciated (from 2 weeks to 20 days). For this final report extending up to 30 working days would help the PSP to optimise the investigation and provide the detailed root cause of the incident.

Additionally, related to guidelines 2.8 that foresee the PSP to submit the initial report after an operational or security incident "within 4 hours from the moment the operational or security incident has been classified as major, or if the reporting channels of the competent authority are known not to be available or operated at that time, as soon as they become available/operational again." More clarity would be welcomed whenever the incident occurs during a weekend or bank-holiday. For those, the report could be submitted the first working day, when the competent authority would access the information, and it should not be led to the availability of the CA's channels that might not be known by the PSP. The contrary does not add any value and might harm the PSP's activity held under limited capabilities in those periods.

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

The proposed changes seem adequate, though the format is still too complex. There should be a clear distinction if it is just an operational/technical incident or a security incident.

Cybersecurity related changes should be kept aside as previously mentioned since they do not add much information and are already subject to other reporting obligations.