Brussels, 14 December 2020

EACB Answer

to EBA's Consultation paper on the draft revised Guidelines on major incident reporting under PSD2 (EBA/CP/2020/22)

December 2020

About the EACB:
The **European Association of Co-operative Banks** (EACB) is the voice of the co-operative banks in Europe. It represents, promotes and defends the common interests of its 27 member institutions and of co-operative banks in general. Co-operative banks form decentralised networks which are subject to banking as well as co-operative legislation. Democracy, transparency and proximity are the three key characteristics of the co-operative banks' business model. With 2,700 locally operating banks and 52,000 outlets co-operative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 214 million customers, mainly consumers, retailers and communities. The co-operative banks in Europe represent 85 million members and 705,000 employees and have a total average market share of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

General comments

The EACB welcomes the opportunity to participate in the public consultation on revised Draft Guidelines on major incidents reporting under the Payment Services Directive 2. Already in 2017, in relation to the first edition of the Guidelines, the EACB stressed its concern about the volume and the extreme sensitivity of data and information to be gathered by the authorities. The Guidelines should achieve a balance between what is essential to notify and a realistic timeframe to do so. This principle is particularly relevant for smaller organisations (e.g. many co-operative banks) whose resources are limited. In practice, in smaller organisations, the employees that are investigating the incident are the same ones who fill in the reports relating to the incident. Therefore, oversize reporting and notification requirements mean less time for investigating the problem and preventing its harmful consequences. The current Guidelines require very detailed notification of incidents within a very short timeframe.

In addition, for some co-operative banks the reporting is made by the central body which needs to verify the information with regional cooperative banks (qualification of the incident, quantification of the impacts: number of customers, number of transactions and amounts, …). In this context, reporting obligations should consider the existing diversity within the European banking sector. Emphasis should be given at any time on investigating and repairing the incident rather than in following complex notification procedures.

We welcome the proposed changes which aim at reducing the number of incidents that are required to be reported. For reporting to be meaningful, the reporting obligation should relate to truly major incidents and exclude less significant, more "business as usual" incidents that fall under the current criteria.

In particular, we welcome the reduction of the number of reports that PSPs have to submit. Nevertheless, we believe that even further reduction is warranted. An initial and a final report would be sufficient to attain the goals of the Guidelines whilst the lack of need to submit an intermediary report would save PSPs' resources.

Having said that, we are aware that the draft Regulation on Cyber-resilience (DORA) and the expected implementing regulations will affect the reporting processes covered by the EBA Guidelines on major incident reporting under PSD2. The need to modify the same reporting process twice in a relatively short period of time would consume significant financial and human resources. We would therefore prefer that the revision of the EBA Guidelines is aligned with the DORA legislative and implementation process.

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 EACB welcomes the increase of the absolute amount threshold of the criterion 'Transactions affected' in the higher impact level as this would be helpful to cover only significant incidents. This would not only decrease reporting costs, but also overhead expenses.

We are not in position to confirm whether the change would result in the projected reduction of reported incidents by 30%.

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 EACB agrees with the proposal to raise the criteria for transactions affected in the lower impact level. This will help covering only major incidents.

Having said that, we consider that the percentage of transactions affected and the absolute threshold for the value of affected transactions should be cumulative and not alternative conditions (thus "and" instead of "or"), even when the time factor that the incidents lasts longer than 1 hour is added. A purely percentage-based approach without an absolute threshold for transactions value would increase the number of reports with minor relevance.

An incident affecting more than 10% of transactions of very low value during off-peak hours would become subject to reporting. Likewise, the conditions for the number of payment service users affected expressed as a percentage and an absolute lower threshold should be cumulative and not alternative ("and" and not "or").

The change to a include time factor to lower impact level criteria is a positive development even though it might cause slight confusion with the "service downtime" criteria (regardless of the clarification in the Guidelines). To avoid the confusion, we consider that "service downtime" is a more appropriate term than "duration of the incident". From the customer perspective, it is not the operational down time that is important, but the service down time. The separation between operational incident and service down time is therefore not or not equally defined in many institutions.

Further, we would like to note that if the time factor applies only to "lower" impact categories, it will not affect the level of reporting obligations of large banks. The requirement that payment service providers should report only those operational incidents affecting the ability to initiate and/or process transactions that affect payment service users with a duration longer than one hour should apply also to the "higher impact level" category. If an online banking system is down for one second, probably 100% of users are affected, however, we do not consider such an operational incident to be major.

In general, however, this change is positive and supports the goal of providing information of the incidents that are material by excluding less significant incidents that fall under the current criteria.

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

We acknowledge the need to gather more information about security incidents. However, adding the criterion "breach of security measures" to the lower level impact category needs more clarification. There may be situations when the criteria "breach of security measures", "high level of internal escalation" and "reputational impact" can be simultaneously fulfilled without there being any immediate impact on users or services. However, because in such a situation three lower impact criteria would be fulfilled, a PSP would be obliged to report the incident. Especially, that as the EBA itself noted the criteria 'High level of internal escalation' and 'Reputational impact'

are often being met and subsequently reported together. Whilst the EBA has proposed minor amendments to the description of these criteria in Guideline 1.3 and the examples provided in the Annex to the Guidelines, we doubt whether these amendments are sufficient to prevent the situation whereby incidents without an immediate impact on users or services would have to be reported. We do not consider such a reporting obligation desirable.

By contrast, we consider that a breach of payment security data is highly relevant and hence the new criterion "Breach of security measures" should also be relevant in the context of the higher impact level. However, in a scenario where singular person's data could be compromised either due to intentional malicious actions or unintentional actions (human error), this would still most likely trigger the earlier mentioned two other lower impact criteria. This kind of scenario would be out of proportion in comparison with other incidents reported.

We appreciate that the EBA seeks to provide more clarity to distinguish the criteria 'High level of internal escalation' and 'Reputational impact'. Nevertheless, we believe that both criteria would benefit from even further clarification.

- High level of internal escalation:

Using this criterion for the identification of a major incident may cause misleading internal behaviours when there is no clear evidence of a major incident state. The quantitative (objective) criteria most often already trigger internal escalation procedures, so there is no need for subjective criteria and mix of internal and external communication procedures.

In addition, we suggest not to use the "crisis mode" in Guideline 1.4 (Table 1) for the initial classification of the incident because it is not necessarily known whether an incident triggers a "crisis mode" until more than four hours have gone by.

- Reputational impact:

Reputational impact is an unquantifiable factor and it is difficult to implement it. In particular, almost every incident will involve "some" reputational impact but its scope may vary considerably. A simple "yes/no" answer does not allow to measure it and prompts responding "yes" even if the reputational risk is low.

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

In general, the EACB agrees with the proposed changes but would like to make the following comments.

23a: See our comment to Question 5.

23b: It seems to us that initial report details have not been updated.

23c: The EACB appreciates that the number of reports is reduced and only one intermediate report will be now required. Nevertheless, we would still like to ask the EBA that only 2 reports are compulsory for the notification of major incidents: an initial report and a final report. The EACB believes that intermediary reports do not bring any added value regarding the management of the incident itself while they create substantial administrative burdens for PSPs, in particular smaller PSPs like some co-operative banks.

The EACB also appreciates that the suggested changes will enable more time to provide detailed information for the initial, intermediate and final reports. The clarification that the 4-hour deadline for submission of the initial report applies from the moment of classification of the incident and not the detection of the incident is welcome, however, the time available is still too short. We believe that the initial report should be provided within the 12-24 hours from the moment when the incident is first classified as "major" using a simplified version of the template in Annex 1. In the first hours from the incident, it is crucial for a PSP to concentrate resources on containing the incident and its effects rather than spend them on fulfilling reporting obligations.

The EACB very much welcomes the extension of the deadline to submit the final report to 20 business days. In general, we consider it sufficient most of the times except for the new field introduced in the revised template's Section C "Assessment of the effectiveness of the actions taken". The time required for the "Assessment of the effectiveness of the actions taken" will depend on expectations and clarifications provided by the EBA (see Question 7).

23d: In certain situations, it is difficult to provide specific information, for instance, economic impact. By extending the reporting time, it may become more feasible to provide such information. All fields can be filled if best estimate is an acceptable value.

23ef: These additions are welcome.

23g: Several issues are still unclear. What is the right way to deliver the information? Should a final report be filed with the updated information? Is there a need to submit complete final report if incident is reclassified?

23hi: These clarifications are helpful.
We have certain doubts concerning the reports, though. If payment service provider is able to submit initial, intermediate AND end report within one report (as for example the volume of transactions was reached by the incident) but it could be resolved within one hour, would this mean that initial and end report must be reported after receiving the unique reference number of the local authorities?

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?

As an association, the EACB cannot answer this question because of the divergence of views of its members.

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?

The EACB agrees with changes to these guidelines. Simplifying the process and extending submission timeframes enable more extensive and complete reports. It should be clarified well in advance how the national CA will communicate the individual reference code to PSPs.

Guideline 2.12: See our comment to point 23c under Question 4.

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

In general, the EACB agrees with the changes and supports the proposal.

The fields suggested to be removed provide very little relevant information and can be deleted from the template. However, some comments concerning the fields to be added:

- "fields seeking information on whether the incident has been reported to other authorities and what their decisions/recommendations for said incident may be;"

This provides very little added value. For instance, in Finland, in addition to FIN-FSA there are very limited number of cases to be reported to Finnish Transport and Communications Agency. In a rare occasion, a report would be sent to the CA of Baltic countries as well.

- "assessment of the actions taken during the duration of the incident; and"

The inclusion of this field is not clear. Does this mean objective assessment whether the actions during the incident were adequate or effective? The actions and lessons learnt are already covered by the current template and we see little added value concerning this field.

Having said that, as we indicated in the general comments, we would prefer that the changes to templates are introduced in a manner aligned with the legislative processes for DORA.