Date: 7 March 2017
EBF_025776

EBF response to the EBA Consultation Paper on the draft Guidelines on major incidents reporting under the Payment Services Directive 2 (EBA/CP/2016/23)

Question 1: Do you consider the definitions in the draft Guidelines to be sufficiently clear?

In order for these definitions to be applied in a consistent way, 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) or clarify them in line with the Rationale as follows:

1. "**Major operational or security incident**": we would suggest adding the following terms to the definition proposed*:* "A major incident must be understood as an incident that reaches any of the four criteria in level 2 or three of more criteria in level 1."

   Equally, the concept of "**event**" in the definition itself should be clarified as being "occurrence of a particular set of circumstances" (see ENISA definition).

   On the definition of major incident itself, we have some reservations on the need to retain events that "**may have**" a material adverse impact as its rather subjective nature may lead PSPs to report any potential fraud case, defeating the very purpose of reporting. We would therefore propose to delete the reference to events that may have an impact.

   Operational incidents are defined in Annex 1 (page 42) and include failures in processes, people and systems impacting payment systems. This definition is very similar to the definition of Operational Risk events according to Basel rules. It would therefore be very useful to clarify the boundaries between operational incidents and security incidents.

2. Under "availability", we would suggest restricting the definition of **payment-related services** to the ones provided by the PSP.

3. Some confusing interpretation may arise between the definitions proposed for "availability" and for "**continuity**". The definition of continuity should be amended as follows:
   "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 if it is affected by an abnormal external event. It includes both preventative measures and arrangements to deal with contingencies and delete: **after a disruptive incident occurs**".
In order to clarify the definitions even further, we would suggest adding a definition of "crisis mode or equivalent" as used in Table 1 on page 26.

4. We would suggest adding a clear reference to Annex 1 of PSD2 in the definition of "**Payment-related services**" in order to make sure that the business activity referred to is understood being as the PSP services directly required for the provision of the payment services.

Question 2: Do you consider the criteria and methodology applicable to the assessment and classification of an incident as major to be sufficiently clear? If not, what should be further clarified?

We fully support the introduction of a harmonised reporting framework and a common template for the notification of incidents but some clarifications are needed in order for it to be effective:

- As suggested under question 1, it would be appropriate to include some clarifications from the rationale into the Guidelines (notably rationale 19 and 20).

- In order to bring the guidelines in line with PSD2, we would suggest replacing the word "client" by "Payment Service User".

- Table 1 mentions "other Payment service providers or relevant infrastructure potentially affected" as one of the criteria to be retained. This concept should be clarified as, indeed, major breakdowns in energy supply or a payment network operators will inevitably have an impact on the capacity for PSPs to ensure business continuity.

- Equally, reporting channels should gradually be harmonised with the European Union to allow for a pan-European approach in the reporting of major incidents. This harmonised approach should lead to the introduction of one single reporting mechanism to avoid duplication in reporting requirements, notably at local level.

- National Competent Authorities (NCA) should also harmonise the actions they envisage to take vis à vis PSPs in response to the reporting of a major incident. The same is valid for supporting measures they take to help PSPs solve an incident more quickly or mitigate its impact. We would propose that major incidents reported be anonymised and shared back with PSPs. This would provide them with very useful data on the incident itself and the modus operandi and, in turn, allow them to prevent such incidents to occur again.

- Last but not least, sharing post factum information between all parties would support a more efficient fight against fraud and allow non affected entities to adopt preventative measures. The sharing of information between PSPs should further extend in case TPPs have acted as intermediaries, be it AISPSPs, PISPSPs or Card Issuing PSPs. In order for AS PSPs to have a complete view on major incident potentially affecting their clients, we would therefore suggest that the supervisory Authority, when receiving notifications from TPPs, inform at the same time AS PSPs

they are working with. It is of particular importance to AS PSPs to receive real-time information on the very nature of the incident (compromission of credentials or fraudulent behaviour on the part of the client,…).

Question 3: Do you consider that the methodology will capture all of/more than/less than those incidents that are currently considered major? Please explain your reasonning.

As explained above under question 2, incidents are major when they affect a given percentage (amount, PSUs affected, nature of the PSU affected –corporate versus individuals, down-time,…) within a particular context (large of small PSP), failing which a much larger number of incidents will be reported as compared to today's practice. The proposed methodology will indeed not capture more incidents than those currently considered major but it will increase the number of events PSPs will have to report. The reason is that the proposed indicators and thresholds are not aligned with the Cyber Incident reporting criteria and the thresholds defined by the Single Supervisory Mechanism (SSM).

We would therefore strongly support a more granular percentage-based approach as suggested above.

Question 4: 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.

In order to be meaningful, the criteria should both be expressed as percentages of transactions and PSUs affected and amount lost.

Regarding the indicator **Number of payment transactions affected** (and/or total value compromised):

- We suggest defining its Level 1 and 2 consistently, in both cases as a percentage of the number of transactions AND a minimum amount of the transactions compromised.

Regarding the indicator **Clients affected**:

- It should be clarified whether the percentage refers to: (a) All clients of the PSP, or (b) All clients potentially using the affected payment service or (c) All clients usually using the affected payment service at the time of the incident.
- We suggest defining its Level 1 and 2 consistently, in both cases as a percentage of the number of clients OR the total amount of clients affected.

Regarding the indicator **Economic impact**, we suggest aligning the Level 2 threshold to those for major cyber incidents set by the Single Supervisory Mechanism (ECB), >25,000,000 Euro.

Regarding the indicator **Other PSPs or relevant infrastructures potentially affected**, we think that the definition of this indicator is too broad; we suggest further defining it, or else removing it:

- At the moment when an incident happens, the PSP may not be in a position to fully assess its further impacts on other PSPs. If the incident affects a relevant infrastructure, the PSP may take remedial action to reduce its impact on the infrastructure and avoid it becoming a major incident.

- Major breakdowns in energy supply or at other payment network operators will inevitably have an impact on the capacity for PSPs to ensure business continuity. The EBA should clarify whether they should be reported under this indicator and which should be the trigger to do so.

Regarding the indicator **Reputational impact**, we think that the definition of this indicator is too broad. We suggest retaining incidents that receive coverage more than once in mass media that may be influential, and may have a business impact on the PSP.

Regarding **Guideline 1.5**:
- We think that the main Level 2 criteria should be the economic impact. Therefore, an incident should be classified as major "when one or more criteria at Level 2" are fulfilled, adding "provided that the Economic impact indicator is one of them".
- We believe that the proposal to classify as major any incident that fulfils "three or more criteria at Level 1" introduces more complexity than other methodologies on incident classification.

Question 5: 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 template proposed is quite clear and close to current practices but we would nevertheless propose adding a box "estimates" to allow for more accurate reporting once the impact of the incident has been clearly identified.

In order to make the reporting process more efficient, we would suggest introducing different templates depending on the timing of the notification (initial, intermediate and final). The final report should be more specific and could be modelled along the lines of the proposed template.

As rightly stated in the consultation paper, data breaches may have a serious impact on payment service users and their PSPs. For that reason, they should be reported in the same way under PSD2 and the GDPR. We would therefore propose aligning reporting requirements as it was done for the NIS Directive to avoid duplication and loss of meaningful intelligence.

Data breaches may equally be due to reporting channels that are not sufficiently secured. We would therefore urge competent authorities to agree on security protocols for both reporting and recording the data submitted by PSPs.

Question 6: 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.

The reference to "relevant infrastructures potentially affected" in Table 1 should be reflected in the template as the criteria will not be the same because their field of intervention is mostly at inter-PSP level. We would therefore suggest a different template for these entities.

It would also be necessary to clarify whether an incident consisting of different intermittent interruptions of several systems would be considered as a service downtime (page 41).

On page 42:

- The taxonomy of Type of incident should be aligned with those applied in the SSM Cyber Incident Reporting
- In the cause of the incident, the definition of the type of incident targeted intrusion is very similar to infection of internal systems and it would be beneficial to clarify them.

On the template itself, the wording "unique identification number" should be clarified and be replaced by commonly used terminology such as BIC or the legal identification number of the PSP in the country where it is registered.

As suggested above, the initial report should be limited to general details as data on the service downtown can only be provided once business continuity has been restored (at best in the interim report).

Question 7: 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.

As a general comment, we wish to point out that, especially in smaller organisations, resources are limited and, in practice, the same employees are investigating the incident itself and, at the same time, filling in the report relating to the incident. This means that an extended reporting will be done at the expense of the investigation and the resolution of the incident. We would therefore advocate for a balanced approach and find the right balance between what is to be notified and at what time. The proposed guidelines require a very detailed notification already immediately after the incident has been detected when the emphasis should be on investigating and solving the incident.

Numeric criteria and indicators are not necessarily known at the time the incident is detected, even though they are basically clear and easily identifiable. Criteria e, f and g may, to the contrary, lead to more interpretation and may defer depending on the organisation reporting them. For example, "reputational impact" is rather challenging and subjective. The same goes for the economic impact as costs that are indirectly linked to the incident are not easy to determine (e.g. lost revenues).

The timeline for the initial report seems therefore very short as resources will primarily be dedicated to containing and solving the incident. A 24-hour reporting deadline seems more reasonable. Alternatively, a very short report on the "General details" could be provided to

the supervisory authority within 2 hours from the moment the incident was classified as major. The interim report would subsequently provide more details on the incident.

Equally, an incident suspected to be major could eventually be de-classified if it appears it is not major after all. An additional box for "declassified" reported incident could be usefully added to the template. For consistency purposes, we would suggest that guidelines 2.7 and 2.8 both refer to "initial report" instead of "initial notification" as mentioned under 2.8.

In order to be useful, the intermediary report should be submitted within 5 to 8 days (excluding bank holidays and week-ends) whilst leaving the duty to communicate intermediary reports to the discretion of payment service providers, as rightly stated in the Rationale.

Regarding the final report, we suggest clarifying the timing for submitting it: when the root cause has been identified or when the business is back to normal or when actual impact figures are available.

Some flexibility should be foreseen for the final report as some cases are very complex to investigate and may require a much longer period than the 2 weeks deadline proposed. We would therefore propose giving PSPs more flexibility in this respect to allow them to send a final report once the incident is being fully investigated.

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 procedure proposed in the draft guideline will certainly provide added value for smaller PSPs provided they share the same reporting platform or are members of the same payment scheme.

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

We understand that consolidated reporting will only be possible within the limits of national boundaries, whereas many groups are active in several countries within and outside of the European Union. It should therefore be clarified that consolidated reporting is to be done by the headquarter of the group, even if a major incident took place in a different Member State.

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.5 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:

Pascale-Marie BRIEN
Senior Policy Adviser, payments and digital
p.brien@ebf.eu
+32 2 508 37 24
+32 478 31 68 96