European Payment Institutions Federation aisbl

MARCH 2017

EPIF RESPONSE TO THE EBA GUIDELINES MAJOR INCIDENT REPORTING

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 190 authorised payment institutions and other non-bank payment providers as our members offering services in every part of Europe. EPIF thus represents roughly one third of all authorized Payment Institutions in Europe. Our diverse membership includes a broad range of business models, including:

- 3-party Card Network Schemes
- Acquirers
- Money Transfer Operators
- FX Payment Providers
- Mobile Payments
- Payment Processing Service Providers
- Card Issuers
- Third Party Providers
- Digital Wallets

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as a provider for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).

EPIF RESPONSE

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

No, we do not consider the definitions to be sufficiently clear and would welcome clarification on the following elements:

Scope: Paragraph 11 on page 7 notes that these Guidelines only cover incidents affecting payment services. Paragraph 13 on page 7 and the definition on page 21 suggest that *any* incidents that also impacts payment services (including 'supporting tasks') are also covered. This could include things like power outages. Greater clarity on what exactly is included would be appreciated. Notably, in the definition of payment related services, ensuring that "necessary technical supporting tasks" are related only to the supporting tasks of which an outage would cause an outage of the payment services.

Coherence with other reporting requirements: In some cases the same incident will need to be reported to different Competent Authorities – such as the Data Protection Regulator, the Financial Services Regulator or the Cyber Security Regulator. Streamlining these different reporting requirements would help reduce the administrative burden on firms and provide a more harmonized supervisory approach. If at all applicable, it would be useful for the EBA (or the national Competent Authority) to confirm if these Guidelines supersede any other reporting requirements.

Definition of major operational or security incident: This seems to imply that firms would need to report incidents that have not yet hit the triggers but may potentially hit them. This may apply to incidents where, for example, banking deadlines are at risk due to technical challenges (but not triggered until a specific time). Can you please clarify?

Definition of authenticity: We are unclear what authenticity means in the context of the incident management process. Can you please clarify?

Definition of reputation: We would welcome further clarity on reputational impact, which could be more clearly defined.

2. 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?

No, we do not consider the criteria and methodology to be sufficiently clear.

Generally, we think the criteria for the assessment of major incidents should emphasize loss of data or loss of services as opposed to fraud. The focus of incident reporting should be on the dollar impact/service disruption/loss of data where PSPs' own systems caused it.

We would appreciate further details on the following points:

Transactions Affected:

- The meaning of *affected*: does this only concern the transactions compromised as part of the breach, or also those impacted by the wider service interruption? Under what circumstances is a transaction considered as affected? (E.g. loss of data/type of data compromised/loss of service/delays in the service, the transaction type, etc.).
- Further clarification is also required on the proposed thresholds of 10% and 25% of Transactions Affected. Is that a percentage of the transactions on that particular payment platform/gateway or a percentage of transactions from across all of the platforms/gateways? Moreover, is the percentage a factor of the transactions performed within the affected Member State(s), or the totality of transactions performed by the payment service provider – in the EU, or globally?

Clients Affected:

- We have similar questions here about the meaning of the term *affected* and the calculation of the *total number of clients*: is the percentage a factor of the total number of clients in the affected Member State(s), in the EU, or globally?
- Can you please confirm that individual incidents (such as customer phishing or account takeovers), when bundled into a campaign carried out by the same perpetrators and which may meet some of the proposed thresholds, do not in fact qualify under these Guidelines?

Service Downtime:

- Does this concern total outages of the payment system or also partial outages?
- Is a service considered "unavailable" if an alternative channel is not affected? (e.g. only the web browser is affected by the incident but not the mobile application)
- Is that 2 hours since the incident was detected, even if we are only experiencing a partial outage?
- Planned system outages should be clearly defined within the Guidelines as out of scope.

Thresholds: This is confusing as we consider L1 higher than L2 (as most firms would) can these be changed around?

We also have concerns about the subjectivity of the criteria on *High Level of Internal Escalation* and *Reputation Impact*:

- The level of internal escalation is subjective to each payment provider: each payment provider's internal escalation procedures are notably subject to different risk appetites.
- More clarity on how to measure reputational impact is necessary, as this can be a highly subjective area that is difficult to measure objectively.

Finally, we would like to clarify that the outcome of external application testing programs are not within scope of the Guidelines. These external programs – whereby external vendors/individual contributors signal security vulnerabilities in exchange for compensation – are an essential part of any company's ongoing security monitoring programs.

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 reasoning

We think that the methodology will capture more incidents as 'major'.

Given the low values in the proposed thresholds, there is a risk that even minor incidents could be considered as "major". This will likely result in more incidents being considered as "major", undermining the meaning of "major" and devaluing the reporting procedure.

Providing further clarifications on the criteria set out under question 2 will contribute to reducing the volume of reported incidents. In addition, rather than basing the reporting timelines on the moment where the incident is identified, we recommend using the point where the incident is confirmed as major, once the forensic analysis / diagnostics are completed.

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.

We propose to amend the thresholds as follows:

In general, the static values are generally quite low and will lead to an increased number of reported incidents. This would need amendment to higher values.

With regard to Other PSPs/ relevant infrastructures potentially affected, PSPs are arguably not best placed to assess the external impact of a particular incident. The PSP in question is expected to make industry/ systemic risk assessments with limited visibility of the incident's impact beyond their own organisation.

Arguably, National Competent Authorities are best placed to make this judgement.

The Reputational Impact criteria is too subjective. This criteria will often be decided by the level of media attention an incident receives, which is often an inconsistent measure of the severity of an incident. The criteria should either be more strictly defined, or removed entirely.

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

Yes, we think that the information is generally sufficient, but have some comments.

A two hour reporting window from the detection of an incident is unreasonable. The proposed report asks for too much detail considering the timeframe. If there is an incident, the focus should be on understanding and containing the incident—not on running to prepare a report. The two hour reporting window is going to create a lot of unnecessary reporting. PSPs can do a report after they have contained the incident.

We would like to refer to other regulatory reporting practice and would suggest the EBA align this with other regulatory timelines (e.g. GDPR). Alternatively, an initial brief report could be supplied within two hours, followed by a more detailed report later.

Further consideration should be given to the wider security incident and firm's activities, for example, in the context of payment service impact such as a DDOS attack, this may have been reported to law enforcement/other agencies and this may be useful for a Competent Authority to understand in the event of a large-scale attack impacting more than one provider and for working collaboratively in the event with other government authorities.

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.

Yes, they are sufficiently clear.

Annotation on whether amounts are estimates or final figures could also be included. We would also welcome further clarity on what is meant under authenticity as already mentioned under question 1.

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.

No, we do not consider the deadlines and circumstances feasible.

We do not consider the deadline of 2 hours for the initial report to be feasible: it often takes a few hours and sometimes days or weeks, to determine the true impact of an incident. Focus during an incident is given to identifying and resolving the problem(s): this short deadline for reporting will divert essential resources away from resolving the incident. Furthermore, many companies operate in different regions with different time zones and it may be necessary to harvest information from business units in these locations to include in the initial report. The impact of an incident often changes over its lifetime particularly during the early stages, therefore the full impact may not be known when the incident is first detected and initially may incorrectly activate (or not activate) the triggers.

We would recommend aligning this deadline to the one found in other reporting requirements, such as the General Data Protection Regulation, where a timeframe of 72 hours has been provided. Rather than basing the reporting timelines on the moment where the incident is identified, we would also recommend using the point where the incident is confirmed as major, once the forensic analysis / diagnostics are completed.

Under 2.10 "Payment service providers should also include in their initial report the date for the next update, which should be as short as possible and under no circumstances go beyond 3 business days". Again we would like to see this deadline set at 5 business days for the reasons provided above.

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

Yes, we believe this will add value to the market, but have some comments.

We have concerns about the obligation that the third party should be based in the EU: what is the rationale for this? As a global company, the incident reporting and response teams can be based anywhere in the world and across different time zones to enable quick responses at any time of the day or night.

Then, what exactly is the EBA's understanding of a 'third-party'? Are intra-group agreements included in that notion? (e.g. delegation to another entity owned by the same group company or a non-EU head office reporting on behalf of the EU entity).

Finally, we would like to see the EBA clarify further on the confidentiality measures in place to protect the reporting company's rights (in light of the sharing of information between Competent Authorities).

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

Yes, we believe that the consolidated procedure will provide added value.

As mentioned under question 8, we would appreciate clarity on the reason for including the limitation introduced in the current text (Guideline 3, 3.2.c) that requires consolidated reporting to be confined to PSPs "established in the same Member State".

The EBA should go back to principles and consider what the purpose of gathering the information proposed within the consultation is – i.e. once it is gathered will it be analysed? Will the analysis/data be disseminated back to the participant PSPs, institutions and/or government bodies and central banks for use and reflection in determining procedures, operational gaps or policies going forward? Will the information be used to form future policy, regulations, or procedure and if so, by whom?