14 December 2020

EBF Response to the EBA Consultation on the revision of the of the Guidelines on major incident reporting under PSD2

INTRODUCTORY REMARKS

The **EBF welcomes the EBA initiative** to simplify reporting templates and to ease the burden on Payment Service Providers (PSPs) as regards major incident reporting. Currently, **the reporting process is complex and resource-consuming** and reports already contain a great amount of information to be collected in a very limited timeframe, while **this should be kept at the lowest level possible**. This need is particularly mandated by the currently high resources and the time required to abide by these obligations, as well as to the sensitive information reported. Additionally, further complexity on the methodology to assess incidents would be detrimental to achieving the goals of this revision and should be avoided.

Moreover, we have identified **conflicts with rules that require high confidentiality** for very sensitive information, such as national legal requirements that relate to national security. This should be considered when increasing requirements relating to security incident reporting and descriptions of root-causes. Based on this, the EBF is **against any suggestions to increase the amount of information or fields in the templates**.

A **harmonization between National Competent Authorities (NCAs) implementation** would be preferred for multi-market PSPs. Local regulators have currently introduced the reporting templates with tweaks and minor discrepancies. These discrepancies have major effect on the ability to introduce a standardized escalating and reporting process cross-border. Therefore, it should be ensured in the Guidelines (GLs) revision that **the local regulators avoid tweaks and changes to the extent possible**, so that **cross-border uniformity** can be applied. The importance of this is highlighted even more when considering that the revised GLs are expected to enter into force in Q4 2021, and that the PSPs are depending on the NCAs actions and approach to these GLs as the incident reporting might be implemented in their respective regulations.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

The EBF highlights the need for **harmonization of cyber incident reporting** across EU legislation, where different taxonomies, timelines, thresholds, information requirements and templates are in place.[1] As mentioned above, harmonization should be ensured also in terms of level of details to be provided, especially because of the **cybersecurity risks** it entails. The industry should aim for **spreading as little sensitive information as possible** and keep the communication of details that could be of interest to cyber criminals to an absolute minimum

In the Consultation Paper, the EBA makes mention of the European Commission proposal for EU regulatory framework on digital operational resilience (DORA), stating that the incident reporting requirements introduced therein are inspired by the PSD2, but go beyond payments-related incidents and that it will take much longer time for those to enter into force, contrarily to the current GL revisions which are to become applicable in Q4 2021. It is, thus, implied that the DORA incident reporting requirements will in due course replace the current EBA GLs on major incident reporting under PSD2.

However, DORA's accompanying proposed Directive amending the PSD2 harmonizes incident reporting only vis-à-vis ICT-related incidents. In light of this, **the extent to which incident reporting harmonization is expected to be achieved should be better clarified**, taking into account that **only full harmonization** of the different requirements included in various EU legal provisions (e.g. GDPR, eIDAS, ECB/SSM) **would be meaningful**, to efficiently address this longstanding concern of the industry which ultimately hinders the efforts to ensure higher levels of cybersecurity and resilience in the Union.

[1] For a more detailed presentation of the current fragmentation in incident reporting, the need for harmonization and specific proposals towards this direction, see the EBF Position on Cyber incident reporting.

EBF REPLIES TO THE CONSULTATION PAPER QUESTIONS

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 EBF **agrees in principle** with the proposal to increase the threshold for transactions affected in the higher impact level and believes that this would be a positive change.

However, as regards large banks, such a change **does not lead to a major reduction in reporting incidents**, especially for operational incidents, where even in case of limited service downtime the threshold could be reached. Therefore, we would be supportive of an even **higher amount threshold** (e.g. 25 million EUR), particularly for large banks whose average transaction value will typically be higher, as the proposed threshold is still likely to be triggering reporting of low impact operational incidents which do not have significant impact to the PSP or PSUs.

As a further hypothesis, additionally to raising the threshold in the absolute amount, it could be proposed to **refer only to the percentage threshold** so that the achievement of that threshold is not linked to the size of the operations of the bank.

Q.2 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 EBF **agrees in principle** with the proposal to raise the 'Transactions affected' criteria concerning the lower impact level. However, the **inclusion of a time factor might cause confusion** with the "service downtime" criteria. The distinction between the criteria "duration of incident" and "service downtime" should be more clearly defined, as both relate to a PSP's ability to process transactions and provided services to PSUs.

Inserting **a new time threshold**, relating to the duration of the **incident may generate further complexity** during the assessment phase of the reporting need; this threshold would also be applicable only to operational incidents, creating further complications in the assessment methodology. Since there is already a specific threshold on the duration of the disservice, the EBF is of the view that it would be more useful to **refer to the criterion relating to service downtime**, which, in association with the two low-impact thresholds ('Transactions affected 'and' 'Payment service users affected'), would in any case trigger the reporting, all with a view to simplifying the evaluation algorithm.

Q.3 Do you agree with the inclusion of the new criterion 'Breach of security measures' in Guidelines 1.2, 1.3 and 1.4?

T**he EBF understands the purpose of the introduction of a new criterion** for incident classification to capture additional relevant security incidents and to ensure that NCAs have appropriate oversight of major incidents with impact to a PSPs systems and security protocols.

However, **the definition of "breach of security measures"** (as set out in paragraph 1.3.iii of the proposed GL) **is too broad and requires clarification**.

In order to narrow the scope of said definition, we recommend that it is limited to breaches or violations that have a direct link or connection to the incident to be reported. That is, the incident to be reported must directly flow from the breach or violation of the security measure. If there are other breaches or violations of security measures that are not connected or indirectly connected to the incident, these should not be part of the determination of what constitutes a "major" incident, as it would lead to unnecessary and inaccurate reporting which could undermine the validity of any conclusions drawn from data supplied to NCAs.

In addition to the breadth of the definition, the inclusion of breach of security measures, introduces a **further specification within the methodology of incident reporting**, adding **complexity**.

Regarding the goal of this criterion, it should be better **clarified whether it is to gather information on unintentional deeds** as well. In the "malicious actions" category, the following items are described that do not clearly express intent as such and could be understood as unintentional actions: "information gathering" and "information context". This could lead to possible **divergences of interpretation**, as it would seem applicable also to operational incidents, e.g. related to unintentional actions such as human error.

Also, either due to intentional malicious actions or unintentional actions, in a scenario where a single individual's data could be compromised, the other two lower impact criteria would still most likely be triggered, which would be **disproportionate** compared to other incidents reported.

Furthermore, a breach of security measures could compromise the availability, confidentiality or integrity of security systems, data and applications, regardless of whether it affects payment transactions or other operations. In such a case, if the breach has been assessed as a major security incident, proper reporting to the European Central Bank (ECB) must be made. Therefore, the inclusion of the above criterion seems to be a **duplication of what is already foreseen in terms of reporting to the ECB**.

In the unwelcome case that the new criterion will still be used as proposed, it needs to be **clarified how it should be aligned with the cyber-incident reporting framework established by the European Central Bank** for EUR countries about significant cyber and security incidents. The EBF would also welcome the EBA providing **examples to help**

guide PSPs when considering these types of incidents, to guarantee that PSPs report incidents of which the NCAs and the EBA want to have appropriate knowledge.

Q.4 Do you agree with the proposed changes to the Guidelines aimed at addressing the deficiencies in the reporting process?

The EBF agrees with the proposed changes, with the following remarks:

GL 2.1: In certain cases, **specific information is challenging to provide** (e.g. economic impact). All fields suggested in the amended template are not possible to fill in for all kind of incidents. Therefore, it should **be possible to leave a field blank or set "n/a"**, or to be filled if **best estimate is acceptable value.** As mentioned above, the EBF stresses the importance of keeping the amount of information in the reports at the lowest possible level.

GL 2.14: The revised wording implies that an intermediate report would be due every 3 days even if there are no significant changes, which seems to **contradict section 24 point 3** of the consultation, which suggests simplification by removing the obligation for PSPs to provide updates to intermediate report every 3 working days.

GL 2.21: **The right way to deliver information to the NCA should be clarified**. Specifically, clarifications are required on whether the final report should be filed with the updated information and whether there is a need to submit the complete final report if the incident is reclassified.

A similar **clarification on the "service downtime"** as for reporting criterion would be welcome, i.e. that downtime applies from the moment of classification and not the detection, since incidents sometimes start as non-major and then evolve to major over time (e.g. login issues for a small portion of customers, that grows to issues for a large portion of customers). Another example of the need to further clarify "service downtime" is when the last daily payment batch process service has dropped, in which case, even if the service/process is immediately restored and the incident duration might be only 5 minutes, the batch will be processed next morning, meaning that the absolute downtime can be 12 hours (or even more if the third party payment infrastructure is not accessible, e.g. due to holidays).

It would be helpful for the GL to provide further clarity on a PSP's major incident reporting obligations in the case of third-party incidents beyond the PSP's direct control which affect the PSPs ability for process transactions. Examples include incidents at the clearing or at a correspondent bank which may affect their ability to process payments on behalf of the PSP.

The proposed clarifications made in this consultation in relation to the scope of the GLs by which "they apply also to major incidents affecting functions outsourced by payment service providers to third parties and that these incidents should also be communicated from PSPs to NCAs" brings challenges to the **PSPs**, as they **do not own the timings in these cases and are subject to the third party communicating to them in due**

time. This is why it should be **left to PSPs the discretion** whether to outsource to third-party the responsibility for the notification, as the party responsible for the major incident. Therefore, without prejudice to the provisions on prior information to the NCA and the requirements to be met (Guideline 3.1.), this discretion would allow governance and responsibilities to be maintained in accordance with what each PSP defines in its general operational and security policy for incident reporting, as set out in Guideline 4. Alternatively, we would ask the EBA to consider **allowing additional time for PSPs to collate the necessary information** and report the incident and provide ongoing notifications to the NCA to **allow PSPs sufficient time to liaise with the third party**.

Q.5 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?

The EBF is of the view that standardized template should be used for all reporting purposes and supports the **continuation of using the MS Excel format as a first preference**, since it is flexible, commonly known and widely supported across PSPs.

A **PDF format** would **also be welcomed as alternative** format that is **optionally available**, for better readability and providing a simplified process for manually populating incident reports along with MS Excel. Additionally, we would also recommend the introduction of **further optionally available alternative formats** -such as "xml"- to enable PSPs to automate creation of incident reports where feasible.

Ideally, an **online platform for reporting purposes** could contribute to better address the format issues. Alternatively, as the EBF acknowledges that building cross-country/NCAs systems might still pose a challenge, we propose the creation of a **centralised repository** (e.g. on the dedicated EBA website), where each PSP can upload/download reports.

Q.6 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 EBF agrees with the changes. Simplifying the process and extending submission timeframes enable more extensive and complete reports. It should be clarified well in advance how the national NCAs will communicate the individual reference code to PSPs.

Q.7 Do you agree with the proposed changes to the templates in the Annex to the Guidelines?

In general, the EBF **supports the proposed changes**. However, we have some specific **suggestions** for more understandable terms and other comments to the proposed sub-categories:

- "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**, as a very limited number of cases are to be reported to other agencies.

- "assessment of the actions taken during the duration of the incident ": **The inclusion of this field is not clear**. Specifically, it is unclear whether this means objective assessment on whether the actions during the incident were adequate or effective. The actions and lessons learnt are already covered by the current template and the EBF sees **little added value** concerning this field.

- The proposed sub-categories stated in section 32 (Malicious actions) and section 34 (Process failure) **should be consistently presented**, i.e. either describe the Process failures as following:

monitoring and control, communication, operations, etc., or by adding an adverb to specify what kind of failure, e.g. deficient monitoring and control, communication issues, improper operations. In the suggestions presented in the consultation paper, it is a combination of both, therefore inconsistent.

- In section 32, the proposed sub-category is "Information context security". However, in Cyber incident taxonomy the term "Information content security" is used. This **terminology should be aligned**.

- Into the root cause category "System failure", we recommend **including "Infrastructure failure"** in order to capture such failure type.

The intermediate report references 'describe how the security policy was violated' - this definition is not apparent under the 'breach of security measures' definition in the GLs. If this is the intention, this piece should be referenced in the definition. Also, the overall impact cites 'availability, integrity, confidentiality, authenticity' - the link between the 'breach of security measures' and the overall impact criteria should be more clearly coming through. To this end, we recommend narrowing the scope of the "breach of security measures" definition, as proposed above, under Question 3.

The economic impact cites 'potentially missed business opportunities, potential legal fines'. This is not in line with the reporting requirements of operational risk events, where financial impact should be considered in actual terms and should not include opportunity costs (except near miss events).

The reputational impact cites '...incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement...)...' Mixing reputational and

regulatory impact of an event could prove to be difficult in the internal classification of incidents, as well as in the reporting process and record keeping.

Lessons learnt references seem to have been removed from the Final Report. There are benefits to keep lesson learnt as an optional information within the template.

For more information:

Dimos KARALIS
Policy Adviser
Cybersecurity & Innovation
d.karalis@ebf.eu

Anni MYKKÄNEN
Senior Policy Adviser
Payment & Digital
a.mykkanen@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu