ABI Associazione Bancaria Italiana

Italian Banking Association's response to the European Banking Authority (EBA) Consultation Paper on the revision of the Guidelines on major incident reporting (EBA/CP/2020/22) under the Payment Services Directive 2 (PSD2)

December 2020

This response, prepared by the Italian Banking Association (ABI) on the basis of the contributions provided by its Members and in collaboration with ABILab, its technology competence centre, reveals first of all that the changes proposed by the EBA have been generally welcomed by the Members, especially as they appear to be conducive to achieving greater efficiency in the process of reporting major incidents.

In general, ABI stresses the importance of facilitating payment service providers (PSP) in the reporting process by creating the most immediate and proper harmonization with what they already report in relation to other incident reporting frameworks, developed within the European Union and of a similar nature to the one that is under this Consultation. In particular, we would like to mention the following existing frameworks:

- The "**Eurosystem major incident reporting framework for payment schemes and retail payment systems**", whose scope is limited to operators in the retail payment systems ("*European Payment Council*" - EPC) and card schemes;
- The **cyber security incidents reporting** developed by the European Union Agency for Cybersecurity (ENISA) and the Single Supervisory Mechanism/European Central Bank ("SSM/ECB");
- The new European legislative proposal for a European regulatory **framework for digital operational resilience** (DORA), which is also recalled in this Consultation;
- The **reporting of incidents that generate economic losses** in the context of operational risks, with specific reference to the possibility of listing incidents in relation to, for example: 1) Event Type and Business Line under Basle rules, 2) the criteria related to the reporting of the date of occurrence of the incident, the date of detection/awareness of the bank and the date of accounting the first of any losses recorded in the Profit & Loss account or in the form of reserves, 3) other characteristics related to the definition of the gross actual loss if any (that is the sum of various economic effects related to a single incident), 4) the number of cards/customers involved, 5) the presence of insurance or other means of recovery.

Full harmonization among all the above mentioned reporting frameworks would be mostly welcome as it would make it possible to guarantee full uniformity of the reports to be sent to the various Authorities concerned, with obvious benefits also for the Authorities themselves in terms of the information set to be managed, methods and tools for transmitting information and notification times.

In addition to this main general comment, a number of observations/requests for more detailed clarifications are set out in this response in relation to aspects that could weigh down the reporting process and for which ABI Members provide proposals for improvement (e.g. aspects relating to the introduction of different thresholds in relation to the duration of the incident, see question no. 2; aspects related to the introduction of the new criterion "Breach of security measures", see question no. 3).

Questionario

Ref. #	Domande delle Linee Guida in consultazione
1	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?
Risposta	We agree with the proposal of the EBA with respect to the aforementioned increase in the absolute amount threshold from 5 to 15 million euros of the "transactions affected" criterion at the highest level of impact. Indeed, according to a first assessment carried out by payment service providers (PSPs) of the impact of the EBA guidelines currently in force, some PSPs felt the need to adjust the threshold proportionally to its operations, where, for example, it was found for some incidents that the current threshold of 5 million euros did not effectively represent a "major" operational incident. In particular, for large banking groups, it is proposed to provide for an ad hoc rule whereby the threshold of 15 million euros is considered with reference to a single legal entity of the affected banking group. Where two or more legal entities of the same banking group are involved, it is therefore proposed to raise the threshold (e.g. to 50 million euros) to limit the number of significant reports. As an alternative to the above proposed changes, considering that, for large banking groups, raising the threshold from 5 to 15 million euro could not lead to a significant reduction in incident reporting, especially for operational incidents (where even in the case of limited service interruptions, that threshold could be reached), the criteria could refer only to a percentage threshold so that its achievement is not linked to the size and operations of the reporting PSP.
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?
Risposta	It should be noted that the introduction of different thresholds in relation to the duration of the incident (i.e. the duration of one hour for the criteria "transactions affected" and "payment service users affected" and the duration of two hours for the "service downtime") could, in some cases, generate such an overlap that the methodology for classifying the incident for reporting purposes would be complicated (e.g. linked to the fact that the threshold for "transactions affected" would only be applicable to operational incidents). Therefore, it is suggested to maintain only the two-hour duration with reference only to the criterion "service downtime". Indeed, with a view to simplifying the assessment algorithm, since a specific threshold on the duration of the service failure is already foreseen, we believe that it is more useful to refer to the current criterion of "service downtime", which in association with the two low impact thresholds "transactions affected" and "payment service users affected" would in any case trigger the need for reporting. Furthermore, the introduction of such a duration criterion would entail the need to better define how the proposed one hour value should be calculated with reference to "transactions affected", which is not currently made explicit in the EBA draft guideline under consultation.
3	Do you agree with the inclusion of the new criterion 'Breach of security measures' in Guidelines 1.2, 1.3 and 1.4?
Risposta	In relation to the proposal to include the new criterion "breach of security measures", it should be noted that, similarly to what is reported in the answer to question no. 2, additional burdens may arise for PSPs during classification activities, introducing a further complication in the incident classification methodology for reporting purposes (e.g. in view of the association with two other lower impact levels to classify the incident as "major"). In addition, a breach of security measures could compromise the availability, confidentiality or integrity of security systems, data and applications, regardless of whether it impacts payment transactions or other activities. In this case, if the breach has been assessed as a major ICT security incident, proper reporting to the European Central Bank (ECB) must be carried out through a direct or indirect process. Therefore, the inclusion of the above mentioned criterion appears to be a duplication of what is already foreseen in terms of reporting to the ECB. Finally, the introduction of a new criterion in relation to PSD2 regulated payment services would require that the criteria underlying the assessment of ICT security incidents are clearly and comprehensively expressed so as not to lead to different interpretations by PSPs. Specifically, it should be clarified whether the assessment of incidents should also take into account the (actual or potential) impacts of the event.

Ref. #	Domande delle Linee Guida in consultazione
	In view of the above, it is considered appropriate to maintain the criteria already provided for in the Guidelines currently in force.
4	Do you agree with the proposed changes to the Guidelines aimed at addressing the deficiencies in the reporting process?
Risposta	We agree with the proposed changes and indeed it is considered necessary that the reporting process be harmonised in terms of templates (information set, format, transmission times, etc.) with the reporting currently foreseen both to the national competent authority (NCA) and to European Authorities (ECB, EPC, European Commission, etc.) for all types of incidents involved, also taking into account further applicable EU legal provisions (e.g. NIS, GDPR, eIDAS). Member PSPs do hope for a fully harmonized set of rules, with a single model for reporting to the different Authorities, especially if the reporting covers the same scope (i.e. payment sector), valid in all countries of the European Economic Area. Indeed, for example, the consultation of the European Commission on DORA, Articles 17 and 18, highlights the need for harmonisation of the criteria for incident reporting to assess an ICT security incident as "major", the timing of reporting and the model for communicating with the competent authorities. In addition, this consultation provides an opportunity to seek clarification on Guideline 3 and therefore on the applicability of the proposed amendments to PSPs within a banking group, both within and outside the euro area. Specifically, confirmation is requested that: - the Guidelines revised by the EBA continue to include the specific table "Consolidated report - list of PSPs", with respect to the list of affected entities within the same group, as currently foreseen in the Guidelines of 27 July 2017 (EBA/GL/2017/10); - in case of consolidated report, the Parent Company is responsible for reporting major incidents regardless of whether they occur at branches or subsidiaries within or outside the euro area and regardless of whether the incident detected (e.g. at a subsidiary) has an impact on the Parent Company itself. If this is the case, confirmation of the following is also required: o Insertion of the Parent Company's name in the "Head of Group" field of the initial report (and therefore not in the "Reporting entity" field, which must be used only in the case of delegated reporting to third parties not belonging to the Group); o If the PSP makes use of the consolidated reporting option, the fields under the heading "PSP affected" should be left blank (with the exception of the field "Country(ies) affected by the incident") and a list of PSPs included in the report should be provided by completing the table "Consolidated Report - List of PSPs". In general, in the context of Guideline 3, precise clarification of the concepts of "consolidated reporting" and "delegated reporting" is sought, so that there are no doubts about the precise scope of application, especially with reference to banking groups that use the same outsourcer/information system. Specifically, it is deemed that it should be left to the discretion of the PSP to use "delegated reporting" in the case of banking groups sharing the same outsourcer/information system, whether or not the banking groups opt for consolidated reporting. Therefore, the reporting to the Authorities could be entirely entrusted to the outsourcer (i.e. initial, intermediate and final reports), or to each of the entities affected by the incident belonging to the same banking group (or to the Parent Company in the case of consolidated reporting) that share the same outsourcer/information system. Without prejudice to the provisions on prior information to the NCA and the requirements to be met (Guideline 3.1.), this discretionary delegation 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.
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?

Ref. #	Domande delle Linee Guida in consultazione
Risposta	We are in favour of introducing a standardised file with preference for the "MS excel" format with pre-set fields to be filled in. This preference is dictated by the easy of use and updating, as well as the greater widespread knowledge of this tool by PSPs. Moreover, we propose to insert all the information directly in a centralized repository (e.g. on the dedicated EBA website), where each PSP can update the reports. In this way, staff can upload/download the file on/from this web repository. Finally, as also mentioned in response to question no. 4, it is considered extremely important to align all reporting requirements to the Authorities, in terms of structure, type of reporting model, etc., especially when they are defined by Authorities in the same sector.
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?
Risposta	We agree with the proposed amendments and, by analogy with the answer to question no. 4, it is also requested that, where consolidated and/or delegated reporting is opted for, discretion be left in the entire reporting process, while respecting the prior information to be provided to the national competent authority and the requirements to be met (Guideline 3.1). As already highlighted in previous responses, it is important to align the EBA Guidelines and the various obligations for incident reporting to the Authorities, including the future DORA provisions of the European Commission, in order to fully harmonise the reporting processes and procedures.
7	Do you agree with the proposed changes to the templates in the Annex to the Guidelines?
Risposta	We agree with the proposed changes as long as they are combined together with less stringent deadlines for transmitting the initial report in order to allow the enrichment of the information requested. Otherwise, the preference is to restrict the proposed changes to intermediate and final reports only, leaving only the strictly necessary data in the initial report. As already highlighted in previous responses, it is important to align the EBA Guidelines and the various obligations for incident reporting to the Authorities, including the future DORA provisions of the European Commission, in order to fully harmonise the reporting processes and procedures.