EBA/CP/2020/22

14.10.2020

Consultation Paper

on the revision of the Guidelines on major incident reporting under the Payment Services Directive 2

Contents

1. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 14.12.2020. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

The EBA is consulting for a shortened period of two-months because the EBA's review of the Guidelines resulted in most of the substantive parts of the requirements to be retained and because the majority of the amendments aim at optimising and simplifying the reporting process for reporting entities and national competent authorities.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found under the Legal notice section of the EBA website.

2. Executive Summary

In July 2017, the European Banking Authority (EBA) adopted the Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)[1]. These Guidelines apply in relation to the classification and reporting of major operational or security incidents in accordance with Article 96 of PSD2 and are addressed to payment service providers (PSPs) and the competent authorities (CAs) under PSD2.

Article 96(4) of PSD2 requires the EBA, in close cooperation with the European Central Bank (ECB), to review the Guidelines on a regular basis and in any event at least every 2 years. To that end, the EBA assessed the incident reports it received in 2018 and 2019 and the reporting practices established by PSPs and CAs during that time. The assessment showed that the Guidelines would benefit from some targeted amendments, in order to optimise and simplify the major incident reporting under PSD2 and the underlying reporting templates, to capture additional security incidents, and, crucially, to reduce the number of operational incidents that are required to be reported by no longer including those that do not have a significant impact on the operations of PSPs.

In order to achieve this, the Consultation Paper (CP) proposes to increase the absolute amount thresholds of the incident classification criterion 'Transactions affected'. It also introduces changes to the calculation of the criteria 'Transactions affected' and 'Payment service users affected' in the 'lower impact level'. Furthermore, the EBA proposes to introduce a new incident classification criterion 'breach of security measures' aimed at capturing incidents where the breach of the security measures of the PSP has an impact on the availability, integrity, confidentiality and/or authenticity of the payment services related data, processes and/or systems.

In order to improve the quality of the reports collected, and at the same time to simplify the reporting process for PSPs, the EBA also proposes the use of a common standardised file for reporting major incidents to CAs. To reduce the number of reports to be submitted by PSPs, the EBA also proposes to remove the requirement for the provision of regular updates from PSPs to CAs on the intermediate report, to extend the deadline for submission of the final report, and to reduce significantly the fields in the reporting template. In addition, the EBA aligned the taxonomy on the causes of the major incidents to other incident reporting frameworks that had been developed by the European Union Agency for Cybersecurity and the Single Supervisory Mechanism of the Eurozone, and also added further granularity to some causes of incidents.

Finally, the EBA acknowledges that the European Commission published, on 24 September 2020 a new EU legislative proposal for an EU regulatory framework on digital operational resilience (DORA), which contains a proposal for incident reporting that is inspired by PSD2 but goes beyond payments-related incidents. The final details of that framework will not be known for several years, after which further time is expected to pass before they become legally applicable. The revised Guidelines proposed in this Consultation Paper, by contrast, are expected to become applicable in Q4 of 2021, and they will remain in force at least until the DORA requirements enter into force.

Next steps

The consultation period will run from 14.10.2020 to 14.12.2020. The Final report on the application of the revised Guidelines on major incident reporting under PSD2 will be published after this consultation.

[1] See: https://eba.europa.eu/sites/default/documents/files/documents/10180/1914076/3902c3db-c86d-40b7-b875-dd50eec87657/Guidelines%20on%20incident%20reporting%20under%20PSD2%20(EBA-GL-2017-10).pdf

3. Background and rationale

3.1 Background

1. Article 96 of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) requires payment service providers (PSPs) to establish a framework to maintain effective incident management procedures, including for the detection and classification of major operational or security incidents.

2. As part of this framework, and to ensure that damage to users, other PSPs or payment systems is kept to a minimum, Article 96 lays down that PSPs shall report major operational or security incidents to the competent authority (CA) in their home Member State without undue delay. PSD2 also requires said CA, after assessing the relevance of the incident to other relevant domestic authorities, to notify them accordingly.

3. To achieve this aim, Article 96(3) of PSD2 conferred a mandate on the EBA to develop, in close coordination with the ECB and after consulting all relevant stakeholders, including those in the payment services market, 'Guidelines in accordance with Article 16 of the EBA Regulation (EU) addressed to each of the following:

   a) PSPs, on the classification of major operational or security incidents and on the content, the format, including standard notification templates, and the procedures for notifying such incidents;

   b) competent authorities, on the criteria for how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities.'

4. In addition, PSD2 assigned to the EBA and the ECB a central coordination role in relation to other relevant EU and national authorities. The Directive provides that the national CA in the home Member State is to swiftly share with the EBA and the ECB relevant details of the incident, that a collective assessment of its significance for these other Union and national authorities is performed and that, where appropriate, the EBA and the ECB notify them accordingly.

5. To that end, the EBA developed and published on 27 July 2017 the EBA Guidelines on major incident reporting under PSD2 (EBA/GL/2017/10). The Guidelines set out the criteria, thresholds and methodology to be used by PSPs to determine whether or not an operational or security incident should be considered major and how said incident should be notified to the CA in the home Member State. In addition, the Guidelines prescribed how PSP may delegate the reporting obligations to a third party. Furthermore, the Guidelines set out the criteria on how CA should assess the relevance of the incident to other competent authorities and the information to be shared. The Guidelines apply as of 13 January 2018.

6. Article 96(4) of PSD2 requires the EBA, in close cooperation with the ECB, to review the Guidelines on a regular basis and in any event at least every 2 years.

7. Finally, the EBA acknowledges that the European Commission published, on 24 September 2020 a new EU legislative proposal for an EU regulatory framework on digital operational resilience (DORA), which contains a proposal for incident reporting that is inspired by PSD2 but goes beyond payments-related incidents. The final details of that framework will not be known for several years, after which further time is expected to pass before they become legally applicable. The revised Guidelines proposed in this Consultation Paper, by contrast, are expected to become applicable in Q4 of 2021, and they will remain in force at least until the DORA requirements enter into force.

3.2 Rationale

8. To address the requirement of Article 96(4) of PSD2, the EBA assessed the incident reports it received in 2018 and 2019 and the reporting practices established by PSPs and CAs during that time. The outcome of the assessment showed that the Guidelines would benefit from amendments in order to:

   - optimise the process of reporting major incidents, including by easing the burden on PSPs;
   - optimise and where possible simplify the reporting templates in order to improve the meaningfulness of the reports received;
   - capture additional security incidents that would not qualify as major under the criteria set in the original Guidelines but that experience has shown are material; and
   - reduce the number of operational incidents that will be reported, in particular those that are currently classified as major but are related to the failure of less significant tasks or single processes and are therefore not that material.

9. The remainder of this chapter sets out how the EBA proposes to amend the Guidelines in order to materialise the aforementioned aims.

3.2.1 Type of incidents and criteria triggering a major incident report

10. When it comes to the type of incidents reported, the EBA's assessment showed that the majority of the submitted incidents (around 95%) were categorised by PSPs as being of an operational nature and very few were security incidents (5%).

11. After assessing the underlying reasons for this, the EBA arrived at the view that:

   - A large number of reported operational incidents appear to have a very low impact on the institution, with most of them related to failure of less significant tasks and single processes (e.g. further processing of batch-payments in net settlement systems, temporary glitches) without a significant impact on the PSP or its PSUs;
   - Some of the security incidents appear not to be captured by the current criteria and thresholds; and

- The quantitative threshold for the absolute amount of the criterion 'Transactions affected' appears to have led to very uneven numbers between the operational and security incident reports, and in particular the threshold set for the higher impact level is too low for operational incidents.

12. The EBA is therefore proposing in this Consultation paper (CP) to increase said threshold from 5 million to 15 million EUR. Based on the available data, this would reduce by 30% the reporting of major incidents that have been triggered on the basis of the single criterion 'Transactions affected' in the higher impact level being met.

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?

13. When it comes to the criteria triggering a major incident report, EBA observed that the reporting was most often triggered because of the thresholds of the following criteria being met:

- Transactions affected (mainly higher impact level);
- Service downtime;
- High level of internal escalation (lower impact level);
- Reputational impact; and
- Payment service users affected (mainly higher impact level).

14. With regard to the individual criteria and thresholds used, the EBA considered that minor amendments in some thresholds may be needed in order to (i) avoid capturing operational incidents without a significant impact and (ii) to capture additional security incidents that the EBA deems material. Therefore, in addition to the increase of the absolute threshold of the criterion 'Transactions affected' in the higher impact level, the EBA hereby proposes In Guideline 1.4. an amendment to the assessment of the lower impact level of the 'Transactions affected' criterion by using the percentage and the absolute amount thresholds as alternatives but also adding a condition, that where the incident is of an operational nature and relates to the inability of the PSP to initiate and/or process transactions, the incident must have a duration longer than one hour. The CP proposes the same change in the lower impact level of the criterion 'Payment service users affected' since the two are interlinked.

15. With regard to the duration of the incident as referred to in the previous paragraph, it should be noted that it is different from the separate criterion 'Service downtime', with the former being limited to those operational incidents that affect the ability of the PSP to initiate and/or process transactions. The EBA considers that while the two may overlap to some extent for a small subset of major incidents, there are cases where the issues affecting the initiation and/or processing of transactions may be rectified within a period shorter than one hour but the overall unavailability of the PSPs' services to the payment service user is longer than two hours.

16. Further, the EBA proposes to increase the absolute threshold of the criterion 'Transactions affected' in the lower impact level from 100 000 EUR to 500 000 EUR. This proposal is also consistent with the increase of the threshold in the higher impact level.

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?

17. The EBA is also of the view that in order to capture additional relevant security incidents that would be of interest to CAs, a new criterion should be added. The EBA therefore proposes in this CP the additional criterion 'Breach of security measures' to be included in the Guidelines. This criterion is suggested to have a lower impact level only. In order to trigger a major incident report, this criterion would need to be used in combination with two other criteria from the lower impact level.

18. The criterion is intended to cover cases where one or more security measures, as referred to in Guideline 3.4.1 of the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)[2], have been violated, with impacts on the availability/integrity/confidentiality/authenticity of payment services related data, processes and/or systems of the payment service provider, its payment service users or a third party to which operational functions have been outsourced.

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

19. With regard to the combination of criteria triggering an incident, the EBA observed that around:

- 25% of the incidents had been triggered by a single criterion from the higher impact level (with the majority of these in combination with two other criteria from the lower impact level);
- 8% of the incidents had been triggered by 3 or more criteria from the lower impact level (without a single criterion from the higher impact level); and
- 67% of the incidents had been triggered by a mixture of criteria from the higher and lower impact level.

20. Based on these findings, the EBA came to the view that the Guidelines strike a good balance between the number of criteria used for the classification of incidents as major and therefore would not require an amendment of the Guidelines from this perspective.

21. The EBA also observed that the criteria 'High level of internal escalation' and 'Reputational impact' are often being met and subsequently reported together. The EBA considered that this may be due to the fact that these criteria are usually consequential to other criteria being triggered, they can

[2] https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

be triggered by institutions that are erring on the safe side and they are very subjective. In order to provide greater clarity on when these criteria should be used, the EBA proposes minor amendments to the description of these criteria in Guideline 1.3 and the examples provided in the Annex to the Guidelines.

22. Finally, the EBA came to the conclusion that many PSPs cannot differentiate between 'availability' and 'continuity' as properties that may be affected by an operational or security incident. Since the two are indeed very close in nature, the EBA decided to propose to merge them into 'availability' and subsequently expanded the definition of the term.

3.2.2 Deficiencies in the reporting process

23. While carrying out the assessment of the incident reports and the reporting practices, the EBA also observed that some PSPs have not applied the Guidelines as required. These include, among others:

    a) The use of different variations of the templates specified in the Annex to the Guidelines, which does not allow the EBA, the ECB and some CAs to assess efficiently the reported incidents;

    b) PSPs submitting the three different reports (initial, intermediate and final) related to the same incident separately, although the Guidelines are explicit that the reports should be submitted in an incremental manner and with the template provided in the Annex to the guidelines;

    c) PSPs not respecting the deadlines for submission of the different incident reports;

    d) PSPs not populating the template for incident reporting exhaustively;

    e) PSPs not providing sufficient details related to the incident;

    f) PSPs not updating information provided with previous reports;

    g) PSPs not informing CAs about the reclassification of the incident from major to non-major (around 16% of the reported incidents have been downgraded but were not subsequently re-classified from 'major' to 'non-major');

    h) Lack of reporting of incidents affecting services that have been outsourced to third parties; and

    i) Insufficient information provided when the reporting to CAs has been delegated.

24. All of the above issues are examples of non-compliance with the Guidelines that undermine the ability of national authorities and the EBA to assess incidents and forward the reports to other jurisdictions and reduce the impact there, on payment service users as well as other PSPs. While they can be resolved by a proper compliance with the requirements, the EBA considered that some amendments to the Guidelines might additionally facilitate said compliance. The EBA therefore proposes the following changes to the Guidelines for each of the points referred in paragraph 23 above:

    - In relation to 23(a) - the introduction of a standardised file containing the templates in the Annex to the Guidelines and this template to be made publicly available by the EBA on its website. The change was reflected in Guideline 2.1.

- In relation to 23(b) - clarifications on the requirement to submit the reports in an incremental manner, namely that it requires submitting the reports related to the same incident sequentially and that each report should contain the previous reports related to the same incident (e.g. when submitting the intermediate report, the PSP should also include a [updated] initial report). In other words, the template for incident reporting should contain the incident report and all previously submitted reports related to the same incident. These changes were reflected in Guidelines 2.2.
- In relation to 23(c) - simplification of the incident reporting process, by removing the obligation for PSPs to provide updates to the intermediate reports every 3 working days, extended the deadline for the submission of the final report from 2 weeks to 20 working days, and optimised the reporting template to ease the burden to PSPs. The EBA also clarified that the 4-hour deadline for submission of the initial report as required under Guideline 2.7 applies from the moment of classification of the incident (and not the detection of the incident).
- In relation to 23(d) - a clarification in Guideline 2.1 that all fields of the templates should be populated.
- In relation to 23(e) - a clarification as to what type of information is expected to be provided in some of the fields of the notification template in the Annex to the Guidelines, including by extending the examples given, and the introduction of specific fields requesting information that is requested under the fields with general details (e.g. information of the impact of the incident in other Member States).
- In relation to 23(f) - a clarification that the previously reported information should be updated, if applicable, and the introduction of fields specifying the changes made to the previously submitted reports related to the same incident. The main changes were introduced in Guidelines 2.2 and 2.12, as well as by introducing additional fields in the notification template in the Annex to the Guidelines.
- In relation to 23(g) - a further explanation that any re-classification of an incident from major to non-major should be communicated to the competent authority in line with the requirement of Guideline 2.21 and without undue delay.
- In relation to 23(h) - a clarification in the scope of the Guidelines that 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 CAs.
- In relation to 23(h) - a clarification that each PSP should ensure that, when an incident is caused by a disruption in the services provided by a technical service provider (or an infrastructure) that affects multiple PSPs, the delegated reporting should refer to the individual data of the PSP, except in the case of a consolidated reporting. The clarification was introduced with a new Guideline 3.6.

25. The introduction of the standardised file referred to in the first bullet of the above paragraph aims at ensuring a consistent reporting for all PSPs across the EU while facilitating an automated processing and timely assessment of the information received by NCAs and subsequently by the EBA and the ECB. Moreover, it aims at addressing concerns raised by some PSPs, part of a group present across the EU, who argued that they face different national approaches for submitting the reporting template in the different Member States, which, in turn, increases their reporting burden.

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

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?

3.2.3 Simplification of the notification process and changes to the reporting templates

26. When assessing the incident reports received in 2018 and 2019 and the reporting practices established by PSPs, the EBA also arrived at the view that there is room for optimisation and simplification of the reporting process and reporting template, namely with regard to:

- the steps of the notification process that the EBA considered redundant;
- some of the information requested from PSPs with the Guidelines that the EBA identified as having little added value;
- the need to request some additional information to improve the meaningfulness of the reports received; and
- requesting specific types of information related to the incident in a different report (e.g. the detailed information about causes of incidents to be provided in the final report instead of the intermediary).

27. The EBA identified some steps of the reporting process that appear to add limited value, in particular the requirement for PSPs to update the intermediate reports every 3 working days, which often were no more than a repetition of the information PSPs had previously reported. In that regard, the EBA proposes that a single intermediate report should be required from PSPs, and thus remove the reference to 'last intermediate report' as required under the original Guideline 2.14. The CP proposes that PSPs are only required to submit an additional intermediate report upon request by their CA or where significant changes related to the incident have occurred and a final report has not yet been submitted. The latter includes the cases where the major incident has not been resolved within the 3-day deadline specified in revised Guideline 2.12, which, based on the assessment of the EBA, is relevant for a small percentage of the incidents. The CP also extended the deadline for the submission of the final report in Guideline 2.18 from 2 weeks to 20 working days.

28. In addition, to ensure transparency of the process and better link between the different reports related to the same incident, the CP proposes to introduce a requirement for CAs in Guideline 2.7 to acknowledge the receipt of the initial report and assign a unique reference code unequivocally

identifying the incident. Competent authorities will have discretion at national level to decide on the format of said reference code and will be required to include as prefix the 2-digit ISO code[3] of their respective Member State when sharing the incident with the EBA and the ECB, to ensure uniqueness of the code at EU level.

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?

29. The EBA observed that PSPs do not populate some of the fields of the reporting templates. In addition, after assessing the information provided in those fields, the EBA arrived at the view that some information has little added value and is of limited use for supervisors. To that end, the EBA proposes that the below fields should be removed from the reporting templates and, thus, the respective information no longer be requested from PSPs:

- 'Authorisation number, if applicable' (from the initial report) since it is now covered in the field 'National identification number'. The latter is used for consistency with the ITS on the EBA Register under PSD2.
- The field with the estimated time for the next update (from the initial report) since the timeframe for the provision of the intermediate report is clearly articulated in the Guidelines;
- The data and information requested in the general details free text box of the intermediate report, which overlaps with the specific sections of that report (e.g. areas affected, service providers/third party affected or involved);
- 'Incident status' (from the intermediate report) because of limited added value;
- 'Building(s) affected (Address), if applicable' (from the intermediate report) because of limited added value;
- 'Staff affected' (from the intermediate report) because of limited added value;
- The data and information requested in the general details free text box of the final report, which overlaps with the specific sections of that report (e.g. root cause analysis); and
- Date and time of closing the incident (from the final report) since date and time when the incident was restored is contained in the intermediate report and the final report justifies that the incident has been closed.

30. On the other hand, In order to improve the quality of the information collected with the incident reports and its usefulness to CAs, the EBA also arrived at the view that additional pieces of information should be requested and further granularity should be introduced to some of the existing fields. In that regard, the EBA proposes for inclusion in the reporting templates the following additional information:

- additional sub-categories for causes of incidents;

[3] Please see the alpha-2 country codes under ISO-3166 at https://www.iso.org/iso-3166-country-codes.html

- fields seeking information on whether the incident has been reported to other authorities and what their decisions/recommendations for said incident may be;
- a distinction between the date of detection and the date of classification of the incident and introduction of a specific field for the latter;
- e-commerce as a communication channel that may be impacted by the incident;
- assessment of the actions taken during the duration of the incident; and
- clarification that the reference to relevant infrastructures covers not only card schemes but also credit transfer and direct debit schemes.

31. The original Guidelines contained six categories of causes of incidents, namely 'Internal attacks', 'External attacks', 'External events', 'Human error', 'Process failure', and 'System failure'. The EBA came to the view that further granularity is needed for these causes of incidents.

32. Therefore, it converted the categories 'Internal attacks' and 'External attacks', which had three sub-categories (Distributed/Denial of Service', 'Infection of internal systems' and 'Targeted intrusion') into a broader category 'Malicious actions', which this CP proposes to have eight sub-categories:

- 'Malicious code';
- 'Information gathering';
- 'Intrusions';
- 'Distributed/Denial of Service attack (D/DoS)';
- 'Deliberate internal actions';
- 'Deliberate external physical damage';
- 'Information context security'; and
- 'Fraud'.

33. The proposed new category and its sub-categories are aligned with the terminology used in other incident reporting frameworks, such as the Cybersecurity Incident Taxonomy developed by the European Union Agency for Cybersecurity, and also to a significant degree to the Cyber Incident Taxonomy of the Single Supervisory Mechanism in the Eurozone (SSM). This approach is also consistent with the Joint Advice of the European Supervisory Authorities on the information and communication technology risk management and cybersecurity.[4]

34. In addition, the CP proposes to introduce sub-categories for the remaining four causes of incident ('External events', 'Human error', 'Process failure', and 'System failure') as follows:

[4] See https://www.esma.europa.eu/press-news/esma-news/esas-publish-joint-advice-information-and-communication-technology-risk

- For 'Process failure' – Deficient monitoring and control, Communication issues, Operations, Change management, Inadequacy of internal procedures and documentation, and Recovery.
- For 'System failure' – Hardware failure, Network failure, Database issues, Software/application failure, and Physical damage.
- For 'Human error' – Unintended errors, Inaction, and Insufficient resources.
- For 'External events' – Failure of a supplier/technical service provider, and Force majeure.

35. The above sub-categories of causes would allow CAs to obtain specific and crucial information in relation to the nature of the incident. This, in turn, should enable them to take specific and more adequate measures to address those, if needed.

36. Finally, the EBA also considered that the submission of some of the existing type of information related to a specific incident can be moved to a different report and thus to enable on one hand CAs to receive crucial information at an earlier stage and at the same time allow for more time for PSPs to provide more detailed information. The suggested changes include:

- Requesting with the initial report high level information on the type of the incident and the criteria triggering the major incident report; and
- Requesting high level information on the cause of the incident in the intermediate report but more detailed breakdown of the cause of the incident by the newly introduced sub-categories in the final report only.

37. Finally, the EBA also introduced other minor editorial improvements throughout the Guidelines.

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

3.2.4 Other general observations

38. As of 31 December 2019, the EBA and the ECB received 5763 major incident reports with an average of 313 major incident reports per month. The EBA's assessment showed that the number of incident reports varied significantly between the Member States, ranging from a few incidents to hundreds of incidents. In terms of average number of reports per PSP, the EBA also observed divergence across the different Member States with figures ranging from less than 1 and up to 7 major incident reports per PSP for the respective jurisdiction for the period between 13 January 2018 and 31 December 2019. This means that PSPs in some jurisdictions report major incidents to their CAs regularly, while PSPs in other jurisdictions do not often report major incidents.

39. In accordance with Guideline 2.21, all incidents that have initially been classified as major but at some point during the lifetime of the incident have stopped fulfilling the criteria of the Guidelines should be reclassified as non-major and the PSP should subsequently submit a final report to their NCA. The outcome of the assessment showed that 27% of the reported major incidents have been or should have been reclassified by PSPs to non-major at some point during the lifetime of the

incident. The EBA considered these 27% to be within the expected margin of reclassified incidents, especially taking into account that the GL on major incident reporting require incidents that can probably reach the thresholds of the criteria also to be reported. However, EBA would like to highlight that PSPs that do not reclassify major incidents to non-major are in breach of the Guidelines.

40. With regard to the type of PSPs submitting major incident reports, EBA observed that on average 38% of the credit institutions in the EU have submitted an incident report so far and just around 6% of all payment institutions and e-money institutions. This means that the majority of the payment service providers have not submitted a single incident report so far. Whereas it is plausible that a large number of PSPs have not been affected by any operational or security incident, EBA considered, based also on the direct feedback from a few competent authorities, this under-reporting practice may be due to the fact that some PSPs, in particular smaller institutions, may not be fully aware of the requirements of the Guidelines or that they are not reporting incidents intentionally.

41. EBA considered that the above findings are not directly related to the requirements of the Guidelines but to how PSPs apply them. Therefore, no amendment of the Guidelines would be required from that perspective. Nevertheless, the EBA expects that the proposed changes to the Guidelines in the present CP may address some of the deficiencies in the reporting process highlighted above.

42. The EBA also expects CAs and trade associations to raise awareness to PSPs of the Guidelines on major incident reporting under PSD2 and CAs to ensure that PSPs comply with them.

4. Guidelines

EBA/GL-REC/20XX/XX

DD Month YYYY

Draft revised Guidelines

on major incident reporting under the Payment Service Directive 2

Abbreviations

CA	Competent authority
EBA	European Banking Authority
ECB	European Central Bank
ICT	Information communications technology
PSD2	Payment Services Directive (EU) 2015/2366
PSP	Payment service provider

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010[5]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.

2. Guidelines set the EBA view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website with the reference 'EBA/GL/201x/xx'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3).

[5] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p.12).

2. Subject matter, scope and definitions

Subject matter

5. These Guidelines derive from the mandate given to EBA in Article 96(3) of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2).

6. In particular, these Guidelines specify the criteria for the classification of major operational or security incidents by payment service providers as well as the format and procedures they should follow to communicate, as foreseen in Article 96(1) of the above-mentioned directive, such incidents to the competent authority in the home Member State.

7. In addition, these Guidelines deal with the way these competent authorities should assess the relevance of the incident and the details of the incident reports that, according to Article 96(2) of the said directive, they shall share with other domestic authorities.

8. Moreover these Guidelines also deal with the sharing with the EBA and the ECB of the relevant details of the incidents reported, for the purposes of promoting a common and consistent approach.

Scope of application

9. These Guidelines apply in relation to the classification and reporting of major operational or security incidents in accordance with Article 96 of Directive (EU) 2015/2366.

10. These Guidelines apply to all incidents included under the definition of 'major operational or security incident', which covers both external and internal events that could either be malicious or accidental.

11. These Guidelines apply also where the major operational or security incident originates outside the Union (e.g. when an incident originates in the parent company or in a subsidiary established outside the Union) and affects the payment services provided by a payment service provider located in the Union either directly (a payment-related service is carried out by the affected non-Union company) or indirectly (the capacity of the payment service provider to keep carrying out its payment activity is jeopardised somehow else as a result of the incident).

12. These Guidelines apply also to major incidents affecting functions outsourced by payment service providers to third parties.

Addressees

13. The first set of Guidelines (Section 4) is addressed to payment service providers as defined in Article 4(11) of Directive (EU) 2015/2366 and as referred to in Article 4(1) of Regulation (EU) 1093/2010.

14. The second and third set of Guidelines (Sections 5 and 6) are addressed to competent authorities as defined in Article 4(2) (i) of Regulation (EU) No 1093/2010.

Definitions

15. Unless otherwise specified, terms used and defined in the Directive (EU) 2015/2366 have the same meaning in the Guidelines. In addition, for the purposes of these Guidelines, the following definitions apply:

Operational or security incident	A singular event or a series of linked events unplanned by the payment service provider which has or will likely have an adverse impact on the integrity, availability, confidentiality, and/or authenticity of payment-related services.
Integrity	The property of safeguarding the accuracy and completeness of assets (including data).
Availability	The property of payment-related services being fully accessible and usable by payment service users, according to acceptable predefined levels by the payment service provider.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Authenticity	The property of a source being what it claims to be.
Payment-related services	Any business activity in the meaning of Article 4(3) of the PSD2, and all the necessary technical supporting tasks for the correct provision of payment services.

3. Implementation

Date of application

16. These guidelines apply from 1 October 2021 (6 months after the envisaged publication of the Final report).

Repeal

17. The following guidelines are repealed with effect from 1 October 2021:

Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2) (EBA/GL/2017/10)

4. Guidelines addressed to payment service providers on the notification of major operational or security incidents to the competent authority in their home Member State

Guideline 1: Classification as major incident

1.1. Payment service providers should classify as major those operational or security incidents that fulfil

a. one or more criteria at the 'Higher impact level', or

b. three or more criteria at the 'Lower impact level'

as set out in GL 1.4., and following the assessment set out in these Guidelines.

1.2. Payment service providers should assess an operational or security incident against the following criteria and their underlying indicators:

i. Transactions affected

Payment service providers should determine the total value of the transactions affected, as well as the number of payments compromised as a percentage of the regular level of payment transactions carried out with the affected payment services.

ii. Payment service users affected

Payment service providers should determine the number of payment service users affected both in absolute terms and as a percentage of the total number of payment service users.

iii. Breach of security measures

Payment service providers should determine whether one or more security measures have been violated.

iv. Service downtime

Payment service providers should determine the period of time where the service will likely be unavailable for the payment service user or where the payment order -in the meaning of Article 4(13) of the PSD2- cannot be fulfilled by the payment service provider.

v. Economic impact

Payment service providers should determine the monetary costs associated to the incident holistically and take into account both the absolute figure and, when applicable, the relative

importance of these costs in relation to the size of the payment service provider (i.e. to the payment service provider's Tier-1 capital).

vi. High level of internal escalation

Payment service providers should determine whether this incident has been or will likely be reported to their executive officers.

vii. Other payment service providers or relevant infrastructures potentially affected

Payment service providers should determine the systemic implications the incident will likely have, i.e. its potential to spill over beyond the initially affected payment service provider to other payment service providers, financial market infrastructures and/or payment schemes.

viii. Reputational impact

Payment service providers should determine how the incident can undermine user's trust in the payment service provider itself and, more generally, in the underlying service or the market as a whole.

1.3. Payment service providers should calculate the value of the indicators according to the following methodology:

i. Transactions affected:

As a general rule, payment service providers should understand as 'transactions affected' all domestic and cross-border transactions that have been or will likely be directly or indirectly impacted by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content of the payment message was altered, and those that were fraudulently ordered (have the funds been recovered or not) or where the proper execution is prevented or hampered in any other way by the incident.

For operational incidents affecting the ability to initiate and/or process transactions, payment service providers should report only those incidents with a duration longer than one hour.

Furthermore, payment service providers should understand the regular level of payment transactions to be the daily annual average of domestic and cross-border payment transactions carried out with the same payment services that have been affected by the incident, taking the previous year as the reference period for calculations. In case payment service providers do not consider this figure to be representative (e.g. due to seasonality), they should use another more representative metric instead and convey to the competent authority the underlying rationale for this approach in the corresponding field of the template (see the Annex).

ii. Payment service users affected

Payment service providers should understand as 'payment service users affected' all customers (either domestic or from abroad, consumers or corporates) that have a contract with the affected payment service provider that grants them access to the affected payment service, and that have suffered or will likely suffer the consequences of the incident. Payment

service providers should recur to estimations based on past activity in order to determine the number of payment service users that may have been using the payment service during the lifetime of the incident.

In the case of groups, each payment service provider should only consider their own payment service users. In the case of a payment service provider offering operational services to others, that payment service provider should only consider its own payment service users (if any), and the payment service providers receiving those operational services should assess the incident in relation to their own payment service users.

For operational incidents affecting the ability to initiate and/or process transactions, payment service providers should report only those incidents that affect payment service users with a duration longer than one hour.

Furthermore, payment service providers should take as the total number of payment service users the aggregated figure of domestic and cross-border payment service users contractually bound with them at the time of the incident (or, alternatively, the most recent figure available) and with access to the affected payment service, regardless of their size or whether they are considered active or passive payment service users.

iii. Breach of security measures

Payment service providers should determine whether one or more security measures, as referred to in Guideline 3.4.1 of the EBA Guidelines on ICT and security risk management[6] (EBA/GL/2019/04), have been violated with impacts on the availability/integrity/confidentiality/authenticity of payment service related data, processes and/or systems of the payment service provider, its payment service users or a third party to which operational functions have been outsourced. This also includes internal and external unauthorised access as well as data leakages.

iv. Service downtime

Payment service providers should consider the period of time that any task, process or channel related to the provision of payment services is or will likely be down and, thus, prevents i) the initiation and/or execution of a payment service and/or, ii) access to a payments account. Payment service providers should count the service downtime from the moment the downtime starts, and they should consider both the time intervals when they are open for business as required for the execution of payment services as well as the closing hours and maintenance periods, where relevant and applicable. If payment service providers are unable to determine when the service downtime started, they should exceptionally count the service downtime from the moment the downtime is detected.

v. Economic impact

[6]https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

Payment service providers should consider both the costs that can be connected to the incident directly and those which are indirectly related to the incident. Among other things, payment service providers should take into account expropriated funds or assets, replacement costs of hardware or software, other forensic or remediation costs, fees due to non-compliance of contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, payment service providers should only consider those that are already known or very likely to materialise.

vi. *High level of internal escalation*

Payment service providers should consider whether, as a result of its impact on payment-related services, the management body as defined by EBA Guidelines on ICT and security risk management has been or will likely be informed, in line with Guideline 60(d) of the EBA Guidelines on ICT and security risk management, about the incident outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. Furthermore, payment service providers should consider whether, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.

vii. *Other payment service providers or relevant infrastructures potentially affected*

Payment service providers should assess the impact of the incident on the financial market, understood as the financial market infrastructures and/or payment schemes that support it and the rest of payment service providers. In particular, payment service providers should assess whether the incident has been or will likely be replicated at other payment service providers, whether it has affected or will likely affect the smooth functioning of financial market infrastructures or whether it has compromised or will likely compromise the sound operation of the financial system as a whole. Payment service providers should bear in mind various dimensions such as whether the component/software affected is proprietary or generally available, whether the compromised network is internal or external or whether the payment service provider has stopped or will likely stop fulfilling its obligations in the financial market infrastructures it is a member of.

viii. *Reputational impact*

Payment service providers should consider the level of visibility that, to their best knowledge, the incident has gained or will likely gain in the marketplace. In particular, payment service providers should consider the likelihood of the incident to cause harm to the society as a good indicator of its potential to impact their reputation. Payment service providers should take into account whether i) payment service users and/or other payment service providers have complained about the adverse impact of the incident, ii) the incident has impacted a visible payment service related process and is therefore likely to receive or has already received media coverage (considering not only traditional media, such as newspapers, but also blogs, social networks, etc.), iii) regulatory and/or contractual obligations have been or will likely be missed, iv) sanctions have been or will likely be imposed or v) a similar type of incident has occurred before.

1.4. Payment service providers should assess an incident by determining, for each individual criterion, whether the relevant thresholds in Table 1 are or will likely be reached before the incident is solved.

Table 1: Thresholds

Criteria	Lower impact level	Higher impact level
Transactions affected	> 10 % of the payment service provider's regular level of transactions (in terms of number of transactions) **and** duration of the incident > 1 hour* **or** > EUR 500,000 **and** duration of the incident > 1 hour*	> 25 % of the payment service provider's regular level of transactions (in terms of number of transactions) **or** > EUR 15,000,000
Payment service users affected	> 5,000 **and** duration of the incident > 1 hour* **or** > 10 % of the payment service provider's payment service users **and** duration of the incident > 1 hour*	> 50,000 **or** > 25 % of the payment service provider's payment service users
Service downtime	> 2 hours	not applicable
Breach of security measures	Yes	not applicable
Economic impact	not applicable	> Max (0,1 % Tier-1 capital**, EUR 200,000) **or** > EUR 5,000,000
High level of internal escalation	Yes	Yes, and a crisis mode (or equivalent) is likely to be called upon
Other payment service providers or relevant infrastructures potentially affected	Yes	not applicable
Reputational impact	Yes	not applicable

* The threshold concerning the duration of the incident for a period longer than one hour applies only to operational incidents that affect the ability of the payment service provider to initiate and/or process transactions

**Tier-1 capital as defined in Article 25 of Regulation (EU) No 575/2013 of the European Parliament and of the Council, of 26 June 2013, on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012

1.5. Payment service providers should resort to estimations if they do not have actual data to support their judgments as to whether a given threshold is or will likely be reached before the incident is solved (e.g. this could happen during the initial investigation phase).

1.6. Payment service providers should carry out this assessment on a continuous basis during the lifetime of the incident, so as to identify any possible status change, either upwards (from non-major to major) or downwards (from major to non-major). Any re-classification of the incident from major to non-major should be communicated to the competent authority in line with the requirement of Guideline 2.21 and without undue delay.

Guideline 2: Notification process

2.1. Payment service providers should collect all relevant information, produce an incident report by completing the template in the Annex and submit it to the competent authority in the home Member State by using a standardised file made available on the website of the EBA. Payment service providers should complete all fields of the template following the instructions provided in the Annex.

2.2. Payment service providers should use the same template when submitting the initial, intermediate and final reports related to the same incident. Payment service providers should therefore complete a single template in an incremental manner and update, where applicable, the information provided with previous reports.

2.3. Payment service providers should further present to the competent authority in their home Member State, if applicable, a copy of the information provided (or that will be provided) to their users, as foreseen in the second paragraph of Article 96(1) of the PSD2, as soon as it is available.

2.4. Payment service providers should, upon request by the competent authority in the home Member State, provide any additional documents complementing the information submitted with the standardised template.

2.5. Payment service providers should follow up on any requests from the competent authority in the home Member State to provide additional information or clarifications regarding already submitted documentation.

2.6. Payment service providers should at all times preserve the confidentiality and integrity of the information exchanged and their proper authentication towards the competent authority in their home Member State.

Initial report

2.7. Payment service providers should submit an initial report to the competent authority in the home Member State after an operational or security incident has been classified as major. Competent authorities should acknowledge the receipt of the initial report and assign a

unique reference code unequivocally identifying the incident. Payment service providers should indicate this reference code when submitting the intermediate and final reports related to the same incident.

2.8. Payment service providers should send the initial report to the competent authority within 4 hours from the moment the operational or security incident has been classified as major, or if the reporting channels of the competent authority are known not to be available or operated at that time, as soon as they become available/operational again.

2.9. Payment service providers should classify the incident in a timely manner after the incident has been detected and without undue delay after the information required for the classification of the incident is available to the payment service provider.

2.10. Payment service providers should also submit an initial report to the competent authority in the home Member State when a previous non-major incident has been reclassified as a major incident. In this particular case, payment service providers should send the initial report to the competent authority immediately after the change of status is identified, or if the reporting channels of the competent authority are known not to be available or operated at that time, as soon as they become available/operational again.

2.11. Payment service providers should facilitate in their initial reports headline-level information (i.e. section A of the template), thus featuring some basic characteristics of the incident and its foreseen consequences based on the information available immediately after it was classified as major. Payment service providers should resort to estimations when actual data are not available.

Intermediate report

2.12. Payment service providers should submit an intermediate report to the competent authority within 3 working days from the submission of the initial report. The intermediate report should contain a more detailed description of the incident and its consequences (section B of the template).

2.13. Payment service providers should submit the intermediate report within the timeframe specified in Guideline 2.12 when regular activities have been recovered and business is back to normal, informing the competent authority of this circumstance. Payment service providers should consider business is back to normal when activity/operations are restored with the same level of service/conditions as defined by the payment service provider or laid out externally by an SLA (processing times, capacity, security requirements, etc.) and when contingency measures are no longer in place.

2.14. Payment service providers should update the information already provided in sections A and B of the template when they become aware of significant changes since the submission of the previous report (e.g. whether the incident has escalated or decreased, new causes identified or actions taken to fix the problem). This includes the case where the incident has

not been resolved within 3 working days, which would require payment service providers to submit an additional intermediate report. In any case, payment service providers should submit an additional intermediate report at the request of the competent authority in the home Member State.

2.15. As in the case of initial reports, when actual data are not available payment service providers should make use of estimations.

2.16. Should business be back to normal before 4 hours have passed since the incident was classified as major, payment service providers should aim at simultaneously submitting both the initial and the intermediate report (i.e. filling out sections A and B of the template) within the four-hour deadline.

Final report

2.17. Payment service providers should submit a final report when the root cause analysis has taken place (regardless whether mitigation measures have already been implemented or the final root cause has been identified) and there are actual figures available to replace any potential estimates.

2.18. Payment service providers should deliver the final report to the competent authority in a maximum of 20 working days after business is deemed back to normal. Payment service providers needing an extension of this deadline (e.g. when there are no actual figures on the impact available or the root causes have not been identified yet) should contact the competent authority before the time has lapsed and provide an adequate justification for the delay, as well as a new estimated date for the final report.

2.19. Should payment service providers be able to provide all the information required in the final report (i.e. section C of the template) within the four-hour window since the incident was classified as major, they should aim at providing the information related to initial, intermediate and final reports together.

2.20. Payment service providers should include in their final report full information, i.e.: i) actual figures on the impact instead of estimations (as well as any other update needed in sections A and B of the template), and ii) section C of the template which includes, if already known, the root cause and a summary of measures adopted or planned to be adopted to remove the problem and prevent its reoccurrence in the future.

2.21. Payment service providers should also send a final report when, as a result of the continuous assessment of the incident, they identify that an already reported incident does not fulfil anymore the criteria to be considered major and is not expected to fulfil them before the incident is solved. In this case, payment service providers should send the final report as soon as this circumstance is detected and, in any case, within the deadline for the submission of the next report. In this particular situation, instead of filling out section C of the template,

payment service providers should check the box 'incident reclassified as non-major' and facilitate an explanation of the reasons justifying this reclassification.

Guideline 3: Delegated and consolidated reporting

3.1. Where permitted by the competent authority, payment service providers wishing to delegate reporting obligations under the PSD2 to a third party should inform the competent authority in the home Member State and ensure the fulfilment of the following conditions:

a. The formal contract or, where applicable, existing internal arrangements within a group, underpinning the delegated reporting between the payment service provider and the third party unambiguously defines the allocation of responsibilities of all parties. In particular, it clearly states that, irrespective of the possible delegation of reporting obligations, the affected payment service provider remains fully responsible and accountable for the fulfilment of the requirements set out in Article 96 of the PSD2 and for the content of the information provided to the competent authority in the home Member State.

b. The delegation complies with the requirements for the outsourcing of important operational functions as set out in:

i. Article 19(6) of PSD2 in relation to payment institutions and e-money institutions, applicable mutatis mutandis in accordance with Article 3 of Directive 2009/110/EC; or

ii. the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) in relation to all payment service providers.

c. The information is submitted to the competent authority in the home Member State in advance and, in any case, following any deadlines and procedures established by the competent authority, where applicable.

d. The confidentiality of sensitive data and the quality, consistency, integrity and reliability of the information to be provided to the competent authority is properly ensured.

3.2. Payment service providers wishing to allow the designated third party to fulfil the reporting obligations in a consolidated way (i.e. by presenting one single report referred to several payment service providers affected by the same major operational or security incident) should inform the competent authority in the home Member State, facilitate the contact information included under "Affected PSP" in the template and ensure the following conditions are satisfied:

a. Include this provision in the contract underpinning the delegated reporting.

b. Make the consolidated reporting conditional on the incident being caused by a disruption in the services provided by the third party.

c. Confine the consolidated reporting to payment service providers established in the same Member State.

d. Provide a list of all PSPs affected by the incident.

e. Ensure that the third party assesses the materiality of the incident for each affected payment service provider and only includes in the consolidated report those payment service providers for which the incident results classified as major. Furthermore, ensure that in case of doubt, a payment service provider is included in the consolidated report as long as there is no evidence confirming otherwise.

f. Ensure that when there are fields of the template where a common answer is not possible (e.g. sections B2, B4 or C3 of the template), the third party either i) fills them out individually for each affected payment service provider, further specifying the identity of each payment service provider the information relates to, or ii) uses the cumulative values as observed or estimated for the payment service providers.

g. Payment service providers should ensure that the third party keeps them informed at all times of all the relevant information regarding the incident and all the interactions they may have with the competent authority and of the contents thereof, but only to the extent possible so as to avoid any breach of confidentiality as regards the information that relates to other payment service providers.

3.3. Payment service providers should not delegate their reporting obligations before informing the competent authority in the home Member State or after having been communicated that the outsourcing agreement does not meet the requirements referred to in Guideline 3.1, letter b).

3.4. Payment service providers wishing to withdraw the delegation of their reporting obligations should communicate this decision to the competent authority in the home Member State, following the deadlines and procedures established by the latter. Payment service providers should also inform the competent authority in the home Member State of any material development affecting the designated third party and its ability to fulfil the reporting obligations.

3.5. Payment service providers should materially complete their reporting obligations without any recourse to external assistance whenever the designated third party fails to inform the competent authority in the home Member State of a major operational or security incident in accordance with Article 96 of the PSD2 and with these Guidelines. Payment service providers should also ensure that an incident is not reported twice, individually by said payment service provider and once again by the third party.

3.6. Payment service providers should ensure that in the situation where an incident is caused by a disruption in the services provided by a technical service provider (or an infrastructure), which affects multiple PSPs, the delegated reporting refers to the individual data of the payment service provider (except in the case of a consolidated reporting).

Guideline 4: Operational and security policy

4.1. Payment service providers should ensure that their general operational and security policy clearly defines all the responsibilities for incident reporting under the PSD2, as well as the processes implemented in order to fulfil the requirements defined in the present Guidelines.

5. Guidelines addressed to competent authorities on the criteria on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities

Guideline 5: Assessment of the relevance of the incident

5.1. Competent authorities in the home Member State should assess the relevance of a major operational or security incident to other domestic authorities taking as a basis their own expert opinion and using the following criteria as primary indicators of the importance of said incident:

a. The causes of the incident are within the regulatory remit of the other domestic authority (i.e. their field of competence).
b. The consequences of the incident have an impact on the objectives of another domestic authority (e.g. safeguarding of financial stability).
c. The incident affects, or could affect, payment service users at a wide scale.
d. The incident is likely to receive, or has received, wide media coverage.

5.2. Competent authorities in the home Member State should carry out this assessment on a continuous basis during the lifetime of the incident, so as to identify any possible change that could make relevant an incident that was previously not considered as such.

Guideline 6: Information to be shared

6.1. Notwithstanding any other legal requirement to share incident-related information with other domestic authorities, competent authorities should provide information about major operational or security incidents to the domestic authorities identified following the application of Guideline 5.1 (i.e. 'other relevant domestic authorities'), as a minimum, at the time of receiving the initial report (or, alternatively, the report that prompted the sharing of information) and when they are notified that business is back to normal (i.e. the intermediate report).

6.2. Competent authorities should submit to other relevant domestic authorities the information needed to provide a clear picture of what happened and the potential consequences. In order to do so, they should provide, as a minimum, the information facilitated by the payment service provider in the following fields of the template (either in the initial or in the intermediate report):

- Date and time of classification of the incident as major.
- Date and time of detection of the incident.
- Date and time of beginning of the incident.
- Date and time when the incident was restored or is expected to be restored.
- Short description of the incident (including non-sensitive parts of the detailed description).
- Short description of measures taken or planned to be taken to recover from the incident.
- Description of how the incident could affect other PSPs and/or infrastructures.
- Description (if any) of the media coverage.
- Cause of the incident.

6.3. Competent authorities should conduct proper anonymisation, as needed, and leave out any information that could be subject to confidentiality or intellectual property restrictions before sharing any incident-related information with other relevant domestic authorities. Nevertheless, competent authorities should provide other relevant domestic authorities with the name and address of the reporting payment service provider when said domestic authorities can guarantee that the information will be treated confidentially.

6.4. Competent authorities should at all times preserve the confidentiality and integrity of the information stored and exchanged and their proper authentication towards other relevant domestic authorities. In particular, competent authorities should treat all information received under these Guidelines in accordance with the professional secrecy obligations set out in the PSD2, without prejudice to applicable Union Law and national requirements.

6. Guidelines addressed to competent authorities on the criteria on how to assess the relevant details of the incident reports to be shared with the EBA and the ECB and on the format and procedures for their communication

Guideline 7: Information to be shared

7.1. Competent authorities should always provide EBA and ECB with all reports received from (or on behalf of) payment service providers affected by a major operational or security incident.

Guideline 8: Communication

8.1. Competent authorities should at all times preserve the confidentiality and integrity of the information stored and exchanged and their proper authentication towards EBA and ECB. In particular, competent authorities should treat all information received under these Guidelines in accordance with the professional secrecy obligations set out in the PSD2, without prejudice to applicable Union Law and national requirements.

8.2. In order to avoid delays in the transmission of incident-related information to EBA/ECB and help minimise the risks of operational disruptions, competent authorities should support appropriate means of communication.

Annex 1 – Reporting template for payment service providers

Initial report

Major Incident Report

Initial report — within 4 hours after classification of the incident as major

Report date (DD/MM/YYYY) | Time (HH:MM)

A - Initial report						
A 1 - GENERAL DETAILS						
Type of report						
Type of report						
Affected payment service provider (PSP)						
PSP name						
PSP national identification number						
Head of group, if applicable						
Country / countries affected by the incident	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ GB ☐ GR ☐ HR ☐ HU	☐ IE ☐ IS ☐ IT ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK
Primary contact person		Email		Telephone		
Secondary contact person		Email		Telephone		
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)						
Name of the reporting entity						
National identification number						
Primary contact person		Email		Telephone		
Secondary contact person		Email		Telephone		
A 2 - INCIDENT DETECTION and CLASSIFICATION						
Date and time of detection of the incident (DD/MM/YYYY, HH:MM)						
Date and time of classification of the incident (DD/MM/YYYY, HH:MM)						
The incident was detected by		If 'Other', please specify:				
Type of Incident						
Criteria triggering the major incident report	☐ Transactions affected	☐ Payment service users affected	☐ Service downtime	☐ Breach of security measures	☐ Economic impact	☐ High level of internal escalation	☐ Other PSPs or relevant infrastructures potentially affected	☐ Reputational impact
A short and general description of the incident						
Impact in other EU Member States, if applicable						
Reporting to other authorities		If 'Yes', please specify:				

Intermediate report

Major Incident Report

Intermediate report	maximum of 3 working days from the submission of the initial report

Report date *(DD/MM/YYYY)* | Time *(HH:MM)*

Incident reference code

B - Intermediate report

B 1 – GENERAL DETAILS

More detailed description of the incident:			
What is the specific issue?			
How did the incident start?			
How did it evolve?			
What are the consequences (in particular for payment service users)?			
Was it related to a previous incident?		If 'Yes', please specify:	
Were other service providers/third parties affected or involved?		If 'Yes', please specify:	
Was crisis management started (internal and/or external)?		If 'Yes', please specify:	
Date and time of beginning of the incident (if already identified) *(DD/MM/YYYY; HH:MM)*			
Date and time when the incident was restored or is expected to be restored *(DD/MM/YYYY; HH:MM)*			
Functional areas affected	☐ Authentication/Authorisation ☐ Communication ☐ Clearing ☐ Direct settlement ☐ Indirect settlement ☐ Other	If 'Other', please specify	
Changes made to previous reports			

B 2 – INCIDENT CLASSIFICATION / INFORMATION ON THE INCIDENT

Transactions affected [2]	Number of transactions affected		
	As a % of regular number of transactions		
	Value of transactions affected in EUR		
	Duration of the incident (only applicable to operational incidents)		
	Comments:		
Payment service users affected [3]	Number of payment service users affected		
	As a % of total payment service users		
Breach of security measures	Describe how the information security policy has been violated		
Service downtime	Total service downtime *(DD:HH:MM)*		
Economic impact	Direct costs in EUR		
	Indirect costs in EUR		
High level of internal escalation	Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe		
Other PSPs or relevant infrastructures potentially affected	Describe how this incident could affect other PSPs and/or infrastructures		
Reputational impact	Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement...)		

B 3 – INCIDENT DESCRIPTION

Type of Incident			
Cause of incident	☐ Under investigation ☐ Malicious actions ☐ Process failure ☐ System failure ☐ Human errors ☐ External events ☐ Other	If 'Other', please specify:	
Was the incident affecting you directly, or indirectly through a service provider?		If 'Indirectly', please provide the service provider's name:	

B 4 – INCIDENT IMPACT

Overall impact	☐ Integrity ☐ Availability ☐ Confidentiality ☐ Authenticity		
Commercial channels affected	☐ Branches ☐ E-banking ☐ E-commerce ☐ Telephone banking ☐ Mobile banking ☐ ATMs ☐ Point of sale ☐ Other		
	If 'Other', please specify:		
Payment services affected	☐ Cash placement on a payment account ☐ Cash withdrawal from a payment account ☐ Operations required for operating a payment account ☐ Acquiring of payment instruments ☐ Credit transfers ☐ Direct debits ☐ Card payments ☐ Issuing of payment instruments ☐ Money remittance ☐ Payment initiation ☐ Account information services ☐ Other		
	If 'Other', please specify:		

B 5 – INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?	
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated?	
If so, when? *(DD/MM/YYYY; HH:MM)*	
If so, please describe	
Has the PSP cancelled or weaken some controls because of the incident?	
If so, please explain	

Final report

Major Incident Report

Please select the type of report: Final report

within 20 working days after the submission of the intermediate report

Please describe:

Report date *(DD/MM/YYYY)*

Time *(HH:MM)*

Incident reference code

C - Final report

If no intermediate report has been sent, please complete also section B

C 1 - GENERAL DETAILS

Update of the information from the initial report and the intermediate report(s)	
changes made to previous reports	
any other relevant information	
lessons learnt	
Are all original controls in place? If "No", specify which controls and the additional period required for their restoration	

C 2 - ROOT CAUSE ANALYSIS AND FOLLOW UP

What was the root cause (if already known)?	☐ Malicious action ☐ Process failure ☐ System failure ☐ Human error ☐ External event ☐ Other
Please specify:	☐ Information ☐ Intrusions ☐ Distributed/Denial of service attack (D/DoS) ☐ Deliberate internal actions ☐ Deliberate external physical damage ☐ Information context security ☐ Fraud ☐ Other ☐ Deficient monitoring and control ☐ Communication issues ☐ Operations ☐ Change management ☐ Inadequacy of internal procedures ☐ Recovery ☐ Other ☐ Hardware failure ☐ Network failure ☐ Database issues ☐ Software/application failure ☐ Physical damage ☐ Other ☐ Unintended ☐ Inaction ☐ Insufficient resources ☐ Other ☐ Failure of a supplier/technical service provider ☐ Force majeure ☐ Other If 'Other', please specify:
Other relevant information	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	

C 3 - ADDITIONAL INFORMATON

Has the incident been shared with other PSPs for information purposes?	If 'Yes', please provide details:
Has any legal action been taken against the PSP?	If 'Yes', please provide details:
Assessment of the effectiveness of the actions taken	Highly effective Please provide details:

INSTRUCTIONS TO FILL OUT THE TEMPLATE

Payment service providers should fill out the relevant section of the template, depending on the reporting phase they are in: section A for the initial report, section B for intermediate reports and section C for the final report. Payment service providers should use the same file when submitting the initial, intermediate and final reports related to the same incident. All fields are mandatory, unless it is clearly specified otherwise.

Headline

Initial report: it is the first notification that the PSP submits to the competent authority in the home Member State.

Intermediate report: contains a more detailed description of the incident and its consequences. It is an update of the initial report (and where applicable to a previous intermediate report) on the same incident.

Final report: it is the last report the PSP will send on the incident since, i) a root cause analysis has already been carried out and estimations can be replaced with real figures or ii) the incident is not considered major anymore and need to be reclassified.

Incident reclassified as non-major: the incident no longer fulfils the criteria to be considered major and is not expected to fulfil them before it is solved. PSPs should explain the reasons for this reclassification.

Report date and time: exact date and time of submission of the report to the competent authority.

Incident reference code (applicable for intermediate and final reports): the reference code issued by the competent authority at the time of the initial report to unequivocally identify the incident. Each CA should include as prefix the 2-digit ISO code[7] of their respective Member State.

A – Initial report

A 1 - General details

Type of report:

Individual: the report refers to a single PSP.

Consolidated: the report refers to several PSPs within the same Member State that are affected by the same major operational or security incident, which make use of the consolidated reporting. The fields under 'Affected PSP' should be left blank (with the exception of the field 'Country/Countries affected by the incident') and a list of the PSPs included in the report should be provided filling in the corresponding table (Consolidated report – List of PSPs).

Affected PSP: refers to the PSP that is experiencing the incident.

PSP name: full name of the PSP subject to the reporting procedure as it appears in the applicable official national PSP registry.

PSP national identification number: the unique national identification number used by the competent authority of the home Member State in its national register to identify the PSP unequivocally.

Head of group: in case of groups of entities as defined in article 4(40) of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market,

[7] Please refer to the alpha-2 country codes under ISO-3166 at https://www.iso.org/iso-3166-country-codes.html

amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) 1093/2010 and repealing Directive 2007/64/EC, please indicate the name of the head entity.

Country/countries affected by the incident: country or countries where the impact of the incident has materialised (e.g. several branches of a PSP located in different countries are affected), irrespective of the severity of the incident in the other country/countries. It may or may not be the same as the home Member State.

Primary contact person: name and surname of the person responsible for reporting the incident or, in the case that a third service provider reports on behalf of the affected PSP, name and surname of the person in charge of the incident management/risk department or similar area, at the affected PSP.

Email: email address to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email.

Telephone: telephone number through which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate phone number.

Secondary contact person: name and surname of an alternate person that could be contacted by the competent authority to inquiry about an incident when the primary contact person is not available. In case a third service provider reports on behalf of the affected PSP, name and surname of an alternate person in the incident management/risk department or similar area, at the affected PSP.

Email: email address of the alternate contact person to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email address.

Telephone: telephone number of the alternate contact person through which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate phone number.

Reporting entity: this section should be completed in case that a third party fulfils the reporting obligations on behalf of the affected PSP.

Name of the reporting entity: full name of the entity that reports the incident, as it appears in the applicable official national business registry.

National identification number: the unique national identification number used in the country where the third party is located to identify the entity that is reporting the incident unequivocally. In case the reporting third party is a PSP, the national identification number should be the unique national identification number of the PSP used by the competent authority of the home Member State in its national register.

Primary contact person: name and surname of the person responsible for reporting the incident.

Email: email address to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email.

Telephone: telephone number through which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate phone number.

Secondary contact person: name and surname of an alternate person in the entity that is reporting the incident that could be contacted by the competent authority when the primary contact person is not available.

Email: email address of the alternate contact person to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email address.

Telephone: telephone number of the alternate contact person through which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate phone number

A 2 – Incident detection and classification

Date and time of detection of the incident: date and time at which the incident was first identified.

Date and time of classification of the incident: date and time at which the security or operational incident has been classified as major.

Incident detected by: indicate whether the incident was detected by a payment service user, some other party from within the PSP (e.g. internal audit function) or an external party (e.g. external service provider). If it was none of those, please provide an explanation in the corresponding field.

Type of Incident: indicate whether, to the best of your knowledge, it is an operational or a security incident.

> **Operational:** incident stemming from inadequate or failed processes, people and systems or events of force majeure that affect the integrity, availability, confidentiality and/or authenticity of payment-related services.
>
> **Security**: unauthorised access, use, disclosure, disruption, modification, or destruction of the PSP's assets that affect the integrity, availability, confidentiality and/or authenticity of payment-related services. This may happen, among other things, when the PSP experiences cyber-attacks, due to inadequate design or implementation of security policies or inadequate physical security.

Criteria triggering the major incident report: please indicate which of the criteria have triggered the major incident report. Multiple choices may be selected between the criteria: transactions affected, payment service users affected, service downtime, breach of security measures, economic impact, high level of internal escalation, other PSPs or relevant infrastructures potentially affected, and/or reputational impact.

A short and general description of the incident: please explain briefly the most relevant issues of the incident, covering possible causes, immediate impacts, etc.

Impact in other EU Member States, if applicable: please explain briefly the impact the incident had in another EU Member State (e.g. on payment service users, payment service providers and/or payment infrastructures). If feasible within the applicable reporting deadlines, please provide a translation in English.

Reporting to other authorities: please indicate whether the incident has been/will be reported to other authorities under separate incident reporting frameworks. If so, please specify the respective authorities.

B – Intermediate report

B 1 – General details

More detailed description of the incident: please, describe the main features of the incident, covering at least the information on the specific issue and the related background, the description of how the incident started and evolved, and the consequences, especially for payment service users, etc.

Incident related to previous incidents – please indicate whether or not the incident is related to previous incidents. If the incident has been related to previous incidents, please specify which ones.

Incident affecting other service providers/third parties – please indicate whether or not the incident has affected or involved other service providers/third parties. If the incident has affected or involved other service providers/third parties, please list them and provide more information.

Crisis management started – please indicate whether or not crisis management (internal and/or external) has started. If crisis management has started, please provide more information.

Date and time of beginning of the incident: date and time at which the incident started, if known.

Date and time when the incident was restored or is expected to be restored: indicate the date and time when the incident was or is expected to be under control and business was or is expected to be back to normal.

Functional areas affected: indicate the step or steps of the payment process that have been impacted by the incident, such as authentication/authorisation, communication, clearing, direct settlement, indirect settlement and others.

> **Authentication/authorisation:** procedures which allow the PSP to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials, and the payment service user (or a third party acting on behalf of that user) giving his/her consent in order to transfer funds.
>
> **Communication:** flow of information for the purpose of identification, authentication, notification and information between account servicing PSP and payment initiation service providers, account information service providers, payers, payees and other PSPs.
>
> **Clearing:** a process of transmitting, reconciling and, in some cases, confirming transfer orders prior to settlement, potentially including the netting of orders and the establishment of final positions for settlement.
>
> **Direct settlement:** the completion of a transaction or of processing with the aim of discharging participants' obligations through the transfer of funds, when this action is carried out by the affected PSP itself.
>
> **Indirect settlement:** the completion of a transaction or of processing with the aim of discharging participants' obligations through the transfer of funds, when this action is carried out by another PSP on behalf of the affected PSP.
>
> **Other:** the functional area affected is none of the above. Further details should be provided in the free text field.

Changes made to previous reports: please indicate the changes made to previous reports related to the same incident (e.g. the initial or, where applicable, an intermediate report)

B 2 - Incident classification / Information on the incident

Transactions affected: PSPs should indicate which thresholds are or will likely be reached by the incident, if any, and the related figures: number of transactions affected, percentage of transactions affected in relation to the number of payment transactions carried out with the same payment services that have been affected by the incident and total value of the transactions. PSPs should provide concrete values for these variables, which may be either actual figures or estimations. As a general rule, PSPs should understand as 'transactions affected' all domestic and cross-border transactions that have been or will likely be directly or indirectly impacted by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content of the payment message was altered, and those that were fraudulently ordered (have the funds been recovered or not). Furthermore, PSPs should understand the regular level of payment transactions to be the daily annual average of domestic and cross-border payment transactions carried out with the same payment services that have been affected by the incident, taking the previous year as the reference period for calculations. In case PSPs do not consider this figure to be representative (e.g. due to seasonality), they should use another more representative metric instead and convey to the competent authority the underlying rationale for this approach in the field 'Comments'.

Payment service users affected: PSPs should indicate which thresholds are or will likely be reached by the incident, if any, and the related figures: total number of payment service users that have been impacted and percentage of payment service users affected in relation to the total number of payment service users. PSPs should provide concrete values for these variables, which may be either actual figures or estimations. PSPs should understand as 'payment service users affected' all customers (either domestic or from abroad, consumers or corporates) that have a contract with the affected payment service provider that grants them access to the affected payment service, and that have suffered or will likely suffer the consequences of the incident. PSPs should

recur to estimations based on past activity in order to determine the number of payment service users that may have been using the payment service during the lifetime of the incident. In the case of groups, each PSP should only consider their own payment service users. In the case of a PSP offering operational services to others, that PSP should only consider its own payment service users (if any), and the PSPs receiving those operational services should also assess the incident in relation to their own payment service users. Furthermore, PSPs should take as the total number of payment service users the aggregated figure of domestic and cross-border payment service users contractually bound with them at the time of the incident (or, alternatively, the most recent figure available) and with access to the affected payment service, regardless of their size or whether they are considered active or passive payment service users.

Breach of security measures: Payment service providers should determine whether one or more security measures, as referred to in Guideline 3.4.1 of the EBA Guidelines on ICT and security risk management, have been violated with impacts on the availability/integrity/confidentiality/authenticity of payment service related data, processes and/or systems of the payment service provider, its payment service users or a third party to which operational functions have been outsourced. This also includes internal and external unauthorised access as well as data leakages.

Service downtime: PSPs should indicate whether the threshold is or will likely be reached by the incident and the related figure: total service downtime. PSPs should provide concrete values for this variable, which may be either actual figures or estimations. PSPs should consider the period of time that any task, process or channel related to the provision of payment services is or will likely be down and, thus, prevents i) the initiation and/or execution of a payment service and/or, ii) access to a payments account. PSPs should count the service downtime from the moment the downtime starts, and they should consider both the time intervals when they are open for business as required for the execution of payment services as well as the closing hours and maintenance periods, where relevant and applicable. If payment service providers are unable to determine when the service downtime started, they should exceptionally count the service downtime from the moment the downtime is detected.

Economic impact: PSPs should indicate whether the threshold is or will likely be reached by the incident and the related figures: direct costs and indirect costs. PSPs should provide concrete values for these variables, which may be either actual figures or estimations. PSPs should consider both the costs that can be connected to the incident directly and those which are indirectly related to the incident. Among other things, PSPs should take into account expropriated funds or assets, replacement costs of hardware or software, other forensic or remediation costs, fees due to non-compliance of contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, PSPs should only consider those that are already known or very likely to materialise.

> **Direct costs**: amount of money (euro) directly caused by the incident, including those needed for the correction of the incident (e.g. expropriated funds or assets, replacement costs of hard- and software, fees due to non-compliance to contractual obligations).
>
> **Indirect costs**: amount of money (euro) indirectly caused by the incident (e.g. customer redress/compensation costs, revenues lost due to missed business opportunities, potential legal costs).

High level of internal escalation: Payment service providers should consider whether, as a result of its impact on payment-related services, the management body as defined by EBA Guidelines on ICT and security risk management has been or will likely be informed, in line with Guideline 60(d) of the EBA Guidelines on ICT and security risk management, about the incident outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. Furthermore, payment service providers should consider whether, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.

Other PSPs or relevant infrastructures potentially affected: payment service providers should assess the impact of the incident on the financial market, understood as the financial market infrastructures and/or payment schemes that support it and the rest of PSPs. In particular, PSPs should assess whether the incident has been or

will likely be replicated at other PSPs, whether it has affected or will likely affect the smooth functioning of financial market infrastructures or whether it has compromised or will likely compromise the solidity of the financial system as a whole. PSPs should bear in mind various dimensions such as whether the component/software affected is proprietary or generally available, whether the compromised network is internal or external or whether the PSP has stopped or will likely stop fulfilling its obligations in the financial market infrastructures it is a member of.

Reputational impact: PSPs should consider the level of visibility that, to their best knowledge, the incident has gained or will likely gain in the marketplace. In particular, PSPs should consider the likelihood of the incident to cause harm to the society as a good indicator of its potential to impact their reputation. PSPs should take into account whether i) payment service users and/or other payment service providers have complained about the adverse impact of the incident, ii) the incident has impacted a visible payment service related process and is therefore likely to receive or has already received media coverage (considering not only traditional media, such as newspapers, but also blogs, social networks, etc. However, media coverage in this context means not only a few negative comments by followers, but there should be a valid report or a significant number of negative comments/alerts.), iii) regulatory and/or contractual obligations have been or are likely to be missed, iv) sanctions have been or are likely to be imposed or v) similar type of incident has occurred before.

B–3 - Incident description

Type of Incident: operational or security. Further explanation is provided in the corresponding field in the initial report.

Cause of incident: indicate the cause of the incident and, if it is not known yet, the one that is the most likely to be. Multiple choices may be selected.

Under investigation – please check the box when the cause is currently unknown.

Malicious action – actions intentionally targeting the PSP.

Process failure: the cause of the incident was a poor design or execution of the payment process, the process controls and/or the supporting processes (e.g. process for change/migration, testing, configuration, capacity, monitoring).

System failure: the cause of the incident is associated with a non-adequate design, execution, components, specifications, integration or complexity of the systems, networks, infrastructures and databases that support the payment activity.

Human error: the incident was caused by the unintentional mistake of a person, be it as part of the payment procedure (e.g. uploading the wrong payments batch file in to the payments system) or related with it somehow (e.g. the power is accidentally cut-off and the payment activity is put on hold).

External events: the cause is associated with events generally outside the organisation's direct control (e.g. natural disasters, a failure of technical service provider) .

Other: the cause of the incident is none of the above. Further details should be provided in the free text field.

Was the incident affecting you directly, or indirectly through a service provider?: an incident can target directly a PSP or affect it indirectly, through a third party. In case of an indirect impact, please provide the name of the service provider(s).

B 4- Incident impact

Overall impact: please indicate which dimensions have been affected by the incident. Multiple choices may be selected.

Integrity: the property of safeguarding the accuracy and completeness of assets (including data).

Availability: the property of payment-related services being fully accessible and usable by payment service users, according to acceptable predefined levels.

Confidentiality: the property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Authenticity: the property of a source being what it claims to be.

Commercial channels affected: indicate the channel or channels of interaction with payment service users that have been impacted by the incident. Multiple boxes may be checked.

Branches: place of business (other than the head office) which is a part of a PSP, has no legal personality and carries out directly some or all of the transactions inherent in the business of a PSP. All of the places of the business set up in the same Member State by a PSP with a head office in another Member State should be regarded as a single branch.

E-banking: the use of computers to carry out financial transactions over the Internet.

Telephone banking: the use of telephones to carry out financial transactions.

Mobile banking: the use of a specific banking application on a smartphone or similar device to carry out financial transactions.

ATMs: an electromechanical device that allows payment service users to withdraw cash from their accounts and/or access other services.

Point of Sale: physical premise of the merchant at which the payment transaction is initiated.

E-commerce: the payment transaction is initiated at a virtual Point of Sale (e.g. for payments initiated via the internet using credit transfers, payment cards, transfer of electronic money between e-money accounts).

Other: the commercial channel affected is none of the above. Further details should be provided in the free text field.

Payment services affected: indicate those payment services that are not working properly as a result of the incident. Multiple boxes may be checked.

Cash placement on a payment account: the handing of cash to a PSP in order to credit it on a payment account.

Cash withdrawal from a payment account: the request received by a PSP from its payment service user to provide cash and debit his/her payment account by the corresponding amount.

Operations required for operating a payment account: those actions needed to be performed in a payment account in order to activate, deactivate and/or maintain it (e.g. opening, blocking).

Acquiring of payment instruments: a payment service consisting in a PSP contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee.

Credit transfers: a payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the PSP which holds the payer's payment account, based on an instruction given by the payer.

Direct debits: a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider.

Card payments: a payment service based on a payment card scheme's infrastructure and business rules to make a payment transaction by means of any card, telecommunication, digital or IT device or software if this results in a debit or a credit card transaction. Card-based payment transactions exclude transactions based on other kinds of payment services.

Issuing of payment instruments: a payment service consisting of a PSP contracting with a payer to provide them with a payment instrument to initiate and process the payer's payment transactions.

Money remittance: a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another PSP acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.

Payment initiation services: a payment service to initiate a payment order at the request of the payment service user with respect to a payment account held at another PSP.

Account information services: an online payment service to provide consolidated information on one or more payment accounts held by the payment service user with either another PSP or with more than one PSP.

Other: the payment service affected is none of the above. Further details should be provided in the free text field.

B 5 - Incident mitigation

Which actions/measures have been taken so far or are planned to recover from the incident?: please, provide details about actions that have been taken or planned to be taken in order to temporarily address the incident.

Have the Business Continuity Plans and/or Disaster Recovery Plans been activated?: please, indicate whether it has been the case and if so, provide the most relevant details of what happened (i.e. when they were activated and what it consisted of).

C – Final report

C 1 – General details

Update of the information from the initial report and the intermediate report(s) (summary): please, provide further information on the incident, including the specific changes made to previous reports submitted. Please also include any lessons learnt and any other relevant information.

Are all original controls in place?: please, indicate whether or not the PSP had to cancel or weaken some controls at any time during the incident. If so, please indicate whether all controls are back in place and, if not, explain in the free text field which controls are not back in place and the additional period required for their restoration.

C 2 - Root cause analysis and follow up

What was the root cause, if already known?: please, indicate which is the root cause of the incident or, if it is not known yet, the one that is the most likely to be. Multiple choices may be selected. *(please note that the root cause should be distinguished from the impact of the incident)*

Malicious action – external or internal actions intentionally targeting the PSP. These are separated into the following categories:

Malicious code - e.g. such as a virus, worm, trojan, spyware.

Information gathering - e.g. scanning, sniffing, social engineering.

Intrusions - e.g. privileged account compromise, unprivileged account compromise, application compromise, bot.

Distributed/Denial of service attack (D/DoS) - an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

Deliberate internal actions – e.g. sabotage, theft.

Deliberate external physical damage - e.g. sabotage, physical attack of the premises/data centers.

Information context security - unauthorized access to information, unauthorized modification of information).

Fraud - unauthorized use of resources, copyright, masquerade, phishing.

Others (please specify) - the cause of the incident is none of the above. Further details should be provided in the free text field.

Process failure: the cause of the incident was a poor design or execution of the payment process, the process controls and/or the supporting processes (e.g. process for change/migration, testing, configuration, capacity, monitoring). These are separated into the following categories:

Deficient monitoring and control - e.g. in relation to running operations, certificate expiring dates, licence expiring dates, patch expiring dates, defined maximum counter values, database fill levels, user rights management, dual control principle.

Communication issues - e.g. between market participants or within the organisation.

Operations - e.g. no exchange of certificates, cache is full.

Change management - e.g. unidentified configuration errors, roll-out including updates, maintenance issues, unexpected errors.

Inadequacy of internal procedures and documentation - e.g. lack of transparency regarding functionalities, processes and occurrence of malfunctioning, absence of documentation.

Recovery - e.g. contingency management, inadequate redundancy.

Others (please specify) - the cause of the incident is none of the above. Further details should be provided in the free text field.

System failure: the cause of the incident is associated with a non-adequate design, execution, components, specifications, integration or complexity of the systems, networks, infrastructures and databases that support the payment activity. These are separated into the following categories:

Hardware failure – failure of physical technology equipment that runs the processes and/or stores the data needed by PSPs to carry out their payment-related activity (e.g. failure of hard drives, data centres, other infrastructure).
Network failure – failure of telecommunications networks, either public or private, that allow the exchange of data and information (e.g. via the Internet) during the payment process.
Database issues – data structure which stores personal and payment-related information needed to execute payment transactions.
Software/application failure – failures of programs, operating systems, etc. that support the provision of payment services by the PSP (e.g. malfunctions, unknown functions).
Physical damage - e.g. unintentional damage caused by inadequate conditions, construction work.
Other (please specify) - the cause of the incident is none of the above. Further details should be provided in the free text field.

Human error: the incident was caused by the unintentional mistake of a person, be it as part of the payment procedure (e.g. uploading the wrong payments batch file in to the payments system) or related with it somehow (e.g. the power is accidentally cut-off and the payment activity is put on hold). These are separated into the following categories:

Unintended - e.g. mistakes, errors, omissions, lack of experience and knowledge.

Inaction - e.g. due to lack of skills, knowledge, experience, awareness.

Insufficient resources - e.g. lack of human resources, availability of staff.

Other (please specify) - the cause of the incident is none of the above. Further details should be provided in the free text field.

External event: the cause is associated with events generally outside the organisation's control. These are separated into the following categories:

Failure of a supplier/technical service provider - e.g. power outage, internet outage, legal issues, business issues, service dependencies.

Force majeure - e.g. power failure, fires, natural causes such as earthquakes, floods, heavy precipitation, heavy wind.

Other (please specify) - the cause of the incident is none of the above. Further details should be provided in the free text field.

Other: the cause of the incident is none of the above. Further details should be provided in the free text field.

Other information: please, provide any additional details on the root cause, including the preliminary conclusions drawn from the root cause analysis.

Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known: please, describe the main actions that have been taken or are planned to be taken in order to prevent a future reoccurrence of the incident.

C 3 - Additional information

Has the incident been shared with other PSPs for information purposes?: please, provide an overview as to which PSPs have been reached out, either formally or informally, to debrief them about the incident, providing details of the PSPs that have been informed, the information that has been shared and the underlying reasons for sharing this information.

Has any legal action been taken against the PSP?: please, indicate whether, at the time of filling out the final report, the PSP has suffered any legal action (e.g. taken to court, lost the licence…) as a result of the incident.

Assessment of the effectiveness of the actions taken: please include a self-assessment of the effectiveness of the actions taken during the duration of the incident.

5. Accompanying documents

5.1 Draft cost-benefit analysis / impact assessment

Article 96(4) of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) mandates the EBA to review the Guidelines on major incident reporting developed under the mandate in Article 96(3) PSD2.

Article 16(2) of the EBA Regulation provides that the EBA should carry out an analysis of 'the potential related costs and benefits' of any Guidelines it develops. This analysis should provide an overview of the findings regarding the problem to be dealt with, the solutions proposed and the potential impact of these options. The following section provides the impact assessment from amending the Guidelines on incident reporting.

A. Problem identification

The EBA published on 27 July 2017 Guidelines on major incident reporting under PSD2. The final report introduced three sets of Guidelines separately addressed to payment service providers (PSPs), to competent authorities (CAs) reporting to other domestic authorities, and to CAs reporting to the EBA and the ECB.

The Guidelines specify the criteria for the classification of major operational or security incidents by PSPs as well as the format and procedures they should follow to communicate such incidents to the CA in the home Member State. In addition, the Guidelines determine the criteria that should govern the sharing of incident-relevant information between CAs and other domestic authorities and harmonise the reporting process between CAs and the EBA and the ECB. The Guidelines apply since 13 January 2018.

Under its mandate to review the Guidelines under Article 96(4) PSD2, the EBA carried out an assessment of the incident reports received in 2018 and 2019 and the reporting practices established by PSPs and CAs. The assessment identifies weaknesses in the current procedure PSPs established to classify and report major operation and/or security incidents. Under the status quo, the baseline scenario, the number of incidents reported varies significantly across jurisdiction, type of PSP and type of incidents, reflecting the imbalanced application of the Guidelines by PSPs as well as the need to optimise the Guidelines.

The current criteria triggering a major incident report result in reporting of some operational incidents, which have low impact on the institutions and the financial system. At the same time, the reported incidents do not capture some of the relevant security incidents. Further, the current reporting process causes part of the information reported not to been useful for the supervisors, which lead to unnecessary reporting and monitoring burden for PSPs and CAs respectively. Lastly, the current reporting template collects information, which can be improved for an effective

classification of major incidents. To address these issues, the EBA revised the Guidelines on major incident reporting as outlined in this Consultation Paper (CP).

B. Policy objectives

In general, the outlined revisions to the Guidelines contribute to the EBA's objective of fostering regulatory and supervisory convergence and the development of a single market for payment services in the Union. It further contributes to the EBA's objective to create efficient, secure and easy retail payments.[8]

More specifically, the revisions to the Guidelines contribute to maintain effective incident management procedures and improve the application of a common and consistent approach across entities and member states. It also fosters prompt reaction to incidents, the containment of potential spill-over effects and the prevention of future similar events. This restricts the negative impact of major operational and security incidents, which could affect the integrity, availability, confidentiality and/or authenticity of the payment services provided by PSPs. Therefore, the Guidelines help to ensure that the damage from operational and security incidents to payment service users, other PSPs, payment systems or other third parties is minimised.

At the technical level, the revision to the Guidelines will improve criteria triggering a major incident report. It aims to decrease the number of reported operational incidents by removing the reporting of incidents, which have minor effect on the operations of the PSP. In addition, the revised Guidelines aim to capture additional relevant security incidents.

They further address deficiencies in the reporting process. The reporting process is significantly simplified by reducing the number of intermediate reports to one report, which should be submitted after three days. The EBA assessment shows that only a small number of incidents are resolved in more than three days. In those cases, an additional intermediate report should be submitted once the incident is resolved or at any time when requested by the CA. This simplification, along with other changes in the reporting process, aim to reduce significantly the reporting burden of PSPs.

Lastly, the amended Guidelines optimise the reporting templates with the aim to improve the overall quality of the reporting and reduce the burden to PSPs and CAs.

C. Options considered

Criteria triggering a major incident report and their thresholds

The revised Guidelines addressed to PSPs respond to the need to optimise the classification of major incidents under PSD2. With regard to the individual criteria and thresholds used, the EBA was of the view that amendments in the criteria and some thresholds may be beneficial in order to (i)

[8] EBA (2019): EBA Annual Report 2019: EBA (2020): The EBA 2020 Work programme.

avoid capturing operational incidents without a significant impact and thereby reduce CAs and PSPs administrative burden and (ii) to capture additional security incidents.

Under the current Guidelines, a major incident needs to be reported when the incident affects payment transactions of an amount higher than EUR 5 million. This would trigger the criterion 'transaction affected' on the 'higher impact' level. The EBA assessment showed that this threshold is too low and results in the reporting of insignificant operational incidents. Thus, the following options are considered to increase the threshold:

> **Option 1.1**: Increase the absolute amount of the 'higher impact' threshold from the criterion 'transaction affected' to EUR 10 mm.
>
> **Option 1.2**: Increase the absolute amount of the 'higher impact' threshold from the criterion 'transaction affected' to EUR 15 mm.
>
> **Option 1.3**: Increase the absolute amount of the 'higher impact' threshold from the criterion 'transaction affected' to EUR 20 mm.

In addition, the EBA assessment showed an unproportioned high amount of operational incidents reported under the 'lower impact' threshold of the same criterion and the 'lower impact' threshold of the criterion 'Payment service users affected'. The EBA therefore proposes in this CP an amendment to the assessment of the lower impact thresholds of the 'Transactions affected' and 'Payment service users affected' criteria and considers following options:

> **Option 2.1**: Amend the 'lower impact' level thresholds of the 'Transactions affected' and 'Payment service users affected' criteria by using a percentage threshold only.
>
> **Option 2.2**: Amend the 'lower impact' thresholds of the 'Transactions affected' and 'Payment service users affected' criteria by using a percentage threshold or an amount threshold, which for the criterion 'Transactions affected' should be increased to EUR 500 000. In addition, operational incidents must last more than one hour to trigger the threshold.

The EBA is also of the view that in order to capture to a greater extent relevant security incidents that would be of interest to CAs, a new criterion could be included in the Guidelines.

> **Option 3.1**: Add to the Guidelines the criterion 'Breach of security measures' with a 'lower impact' level only.
>
> **Option 3.2**: Add to the Guidelines the criterion 'Breach of security measures' with a 'higher impact' level only.
>
> **Option 3.3**: Keep the original criteria for determining whether an operational or security incident is major.

Causes of major incidents

The EBA is of the view that more comprehensive information are needed in relation to the causes of major incidents. This would allow PSPs and CAs to understand better the underlying cause of the

incident, whether it can have a spill-over effect and how it can be prevented. To do so, the following amendments are considered:

Option 4.1: Change the reporting template by amending the causes of incidents 'Process failure', 'Human error', 'System failure' and 'External events' as introduced in the original Guidelines in the following way:

- **Processes failure**: Deficient monitoring and control, Communication issues, Operations, Change management, Inadequacy of internal procedures and documentation, and Recovery
- **Human error**: Unintended errors, Inaction, and Insufficient resources
- **System failure**: Hardware failure, Network failure, Database issues, Software/Application failure, and Physical damage
- **External events**: Failure of a supplier/technical service provider, and Force majeure

Option 4.2: Change the reporting template by amending the causes of incidents 'Process failure', 'Human error', 'System failure' and 'External events' as introduced in the original Guidelines in the following way:

- **Operational Cause - Procedural dimension**: Deficient change management, Deficient capacity planning, Deficient vulnerability management, Deficient monitoring, In breach of internal procedures, Lack of internal procedures, and Human error
- **Operational Cause - Technical dimension**: Application failure, Database failure, Software failure, Network/Infrastructure failure, Hardware failure, and Datahall/Physical damage

Option 4.3: Change the reporting template by amending the causes of incidents 'Process failure', 'Human error', 'System failure' and 'External events' as introduced in the original Guidelines in the following way:

- **Processes failure**: Deficient monitoring and control, Communication issues, Operations, Change management, Inadequacy of Documentation, and Recovery
- **Human error**: Unintended errors, Insufficient resources, Lack of information Knowledge, and Abuse behavior
- **System failure**: Hardware failure, Custom and Off-the-shell software failure, and Inadequate or unavailable premises
- **External events**: Malevolence, Failure of service providers, and Force majeure

Finally, the EBA came to the view that the information collected under the causes of incidents 'Internal attacks' and 'External attacks' can be further improved by adding additional granularity and aligning the terminology to other incident reporting frameworks. Therefore, the EBA introduced a new cause of incident – 'Malicious actions', which contains the following sub-categories of causes: Malicious code, Information gathering, Intrusions, Distributed/Denial of Service, Deliberate internal actions, Deliberate external physical damage, Information context security, and Fraud.

D. Cost-Benefit Analysis and Preferred options

Criteria triggering a major incident report and their thresholds

Under each of the proposed Options 1.1 to 1.3, the amount of major incidents reported will decrease and thus the reporting burden for PSPs would decrease. Based on the result of the EBA assessment of major incidents reported in 2018 and 2019, an increase of the threshold for the 'higher impact' level of the criterion 'Transaction affected' will lead to a decrease of the total number of major incidents by 2% to 4%.

The reduction in overall major incidents reported will benefit PSPs by reducing its recurring reporting costs and will help them to identify and handle only incidents with significant impacts. For NCAs and supranational supervisors monitoring costs might also decrease.

The higher threshold will allow PSPs and supervisors to concentrate on significant incidents only and thereby improve the immediate understanding of the nature and extend of the problem. As a result this helps to define the best potentially required actions to address them in a satisfactory manner.

In term of major incidents reports based on the criterion 'Transactions affected' only, the number of incidents reported is expected to decrease by 21% under Option 1.1, which will insufficiently decrease the number of reports submitted. Under Option 1.3, 47% of the major incidents only due to the criterion 'Transaction affected' are expected to not be reported. This threshold is therefore too high, as it cannot ensure that all significant incidents are captured. Option 1.2 strikes the correct balance to reduce the number of operational incidents reported, while still capturing the significant incidents. **Option 1.2** is the preferred option.

Under Option 2.1, a simple threshold based on a percentage of the PSP's regular level of transactions/ payment users affected is considered. This option has the advantage to provide one simple quantitative threshold, which facilitates the application by PSPs. However, without a threshold on the total absolute amount of transactions affected and total number of payment service users affected, significant incidents, especially from larger PSPs, might not be captured.

Under Option 2.2, the two-level approach is retained, while the precise quantitative threshold for the criterion 'Transactions affected' is increased and operational and security incidents are separately considered. This option has the benefit that it reduces the number of operational incidents reported, by increasing the threshold from EUR 100,000 to EUR 500,000 and by applying a time dimension of one hour to operational incidents. In addition, the absolute amount threshold, which applies to all incidents, allows to capture significant security incidents, both from smaller and larger payment service providers.

Option 2.2 has the disadvantage to be more complex and requires PSPs to monitor the duration of incidents, however, PSPs already need to monitor any service downtown under the current framework and it is therefore expected that the increase in monitoring costs is small. At the same time, it will achieve the objectives of reducing the number of reported operational incidents and

capturing relevant security incidents with an overall decrease in the reporting burden for PSPs. **Option 2.2** is the preferred option.

Under Option 3.3, the number of criteria to determine whether an operational or security incident is major remains the same. Under this option, PSPs and CAs are expected to have no additional direct costs such as costs related to the implementation of a new criterion. However, the rise of security risk in recent years[9] makes PSPs more vulnerable towards security breaches, especially, when no pre-cautions measures are in place to address them timely and adequately. Retaining the same criteria may not allow the identification of relevant major security incidents.

Under Option 3.2, PSPs need to update their current systems to identify and report major incidents in order to implement the additional criterion. This option is considered to allow reporting of almost all security incidents that may affect a PSP, however, also including those that are insignificant for its operations. This would go contrary to the objective of the Guidelines to report only major incidents. In addition, the reporting of all security incidents would substantially increase the reporting burden for PSPs, which is unproportional to the additional benefit under this option.

Under Option 3.1, PSPs need to update their current systems to identify and report major incidents in order to implement the additional criterion. This includes the system to identify a major incident based on three 'lower impact' incidents. In addition, PSPs' assessment of a breach of security measures requires identification, monitoring and notification of those incidents under the EBA Guidelines on ICT and security measures. However, the related costs for such an assessment are expected to be low since PSPs' security measures are based on the institution's own information security policy, for which PSPs are required to have already adequate (monitoring) policies in place (Guideline 3.4 of the EBA Guidelines on ICT and security measures). At the same time, the EBA expect that under Option 3.1, the number of major security incidents will increase.

Including the criterion 'Breach of security measures' to the Guidelines addressed to PSPs is expected to increase the number of reported major security incidents, which will improve PSP's preparedness towards such incidents, compliance with the EBA Guidelines on ICT and security measures and thereby positively affect the abilities of PSPs to provide services. **Options 3.1** is the preferred option.

Causes of major incidents

The creation of a clear taxonomy for sub-categories of incident causes, which is aligned with other incident reporting frameworks, should decrease the reporting and monitoring burden for PSPs and CAs. On the other hand, while some of the newly added sub-categories of causes of incidents may be considered more burdensome by some PSPs, the more comprehensive sub-categories should assist PSPs to identify and consequently report those incidents and support the comparability and analysis of such incidents by PSPs and supervisors.

[9] EBA (2019): EBA Guidelines on ICT and security risk management.

Under Option 4.2, the sub-categories proposed are similar to the definition of operational and security risk, which will decrease the clarity of the Guidelines. Further, the incomprehensive nature would not allow relevant causes to be identified and clearly distinguished.

Under Option 4.3, the sub-categories proposed were also considered incomprehensive and some parts were not mutually exclusive. This would not allow relevant causes to be identified and clearly distinguished.

Under Option 4.1, the taxonomy for sub-categories of incident causes follows broadly the categories of the current Guidelines, however, the categories provide more granularity and enhanced definitions. This is expected to allow PSPs and CAs to understand better the underlying cause of the incident, whether it can have spill-over effects and how similar incidents can be prevented in the future. **Option 4.1** is the preferred option.

With regard to the new cause of an incident 'Malicious actions' and its sub-categories, the categories are streamlined and merged where appropriate. Further, the sub-categorisation is, to the greatest extend possible, in line with existing taxonomies of other incident reporting frameworks PSPs might be subject to. This has therefore the benefit for PSPs to continue to use established taxonomies and to provide further clarity to the PSD2 major incident reporting. This should also contribute to decrease the reporting burden for PSPs.

5.2 Overview of questions for consultation

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?

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?

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

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

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?

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?

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