Commission de Surveillance du Secteur Financier

Luxembourg, le 17 Décembre 2018

A tous les prestataires de services de paiement

CIRCULAIRE CSSF 18/704

Concerne : Adoption des Orientations de l'Autorité bancaire européenne sur les notifications des incidents majeurs en vertu de la directive (UE) 2015/2366 (PSD2), (EBA/GL/2017/10)

Mesdames, Messieurs,

L'objet de la présente circulaire est :

- de porter à votre attention les Orientations de l'Autorité bancaire européenne (« ABE ») sur les notifications d'un incident opérationnel ou de sécurité majeur (EBA/GL/2017/10 - les « Orientations »), que la CSSF entend respecter ; et

- de fournir des précisions quant à l'obligation des prestataires de services de paiement de notifier un incident opérationnel ou de sécurité majeur tel que prévu à l'Article 105-2, paragraphe (1) de la loi modifiée du 10 novembre 2009 qui dispose qu' *« en cas d'incident opérationnel ou de sécurité majeur, les prestataires de services de paiement informent sans retard injustifié la CSSF » ;* notamment en ce qui concerne le processus de notification à la CSSF.

1. Les Orientations ABE

Les Orientations spécifient, en particulier, les critères pour la classification des incidents opérationnels ou de sécurité majeurs par les prestataires de services de paiement (ci-après les « PSP ») ainsi que le format et les procédures que ces derniers devraient appliquer pour informer l'autorité compétente dans l'Etat membre d'origine.

Les Orientations s'appliquent à tous les incidents couverts par la définition d' « incident opérationnel ou de sécurité majeur », qui englobe les évènements externes et internes qui pourraient être malveillants ou accidentels.

Les Orientations s'appliquent également lorsque l'incident opérationnel ou de sécurité majeur trouve son origine en dehors de l'Union européenne et affecte les services de paiement fournis par un PSP situé dans l'Union européenne soit directement soit indirectement.
Il convient de se référer au texte complet des Orientations en ce qui concerne les définitions applicables, la classification des incidents opérationnels ou de sécurité majeurs, ou tout autre point relatif au processus de notification à suivre.

L'annexe 1 des Orientations contient les modèles de notification à utiliser par les PSP.

2. Instructions techniques pour le processus de notifications à la CSSF

Les instructions techniques détaillées pour transmettre les données à la CSSF figurent à l'annexe 1 de la présente circulaire.

3. Les délais requis pour la notification à la CSSF

Les PSP devraient soumettre une notification initiale à la CSSF dans les 4 heures suivant la détection de l'incident opérationnel ou de sécurité majeur.

Les PSP devraient soumettre des notifications intermédiaires chaque fois qu'ils considèrent qu'il y a une mise à jour pertinente du statut et, au minimum, à la date de la prochaine mise à jour indiquée dans la notification précédente (notification initiale ou notification intermédiaire).

Les PSP devraient remettre leur notification finale à la CSSF dans un délai maximum de deux semaines après que l'activité soit considérée comme revenue à la normale.

Il convient de se référer au texte complet des Orientations concernant les détails relatifs aux différentes étapes de notification requises.

4. Délégation des obligations de notification à un tiers

Une délégation des obligations de notifications d'un incident opérationnel ou de sécurité majeur à un tiers n'est pas admissible.

5. Entrée en vigueur et application

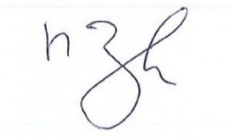
La présente circulaire, par laquelle la CSSF adopte les Orientations, entre en vigueur avec effet immédiat.

Les Orientations sont annexées à la présente circulaire et sont disponibles sur le site de l'ABE à l'adresse suivante :

http://www.eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf/3902c3db-c86d-40b7-b875-dd50eec87657

Veuillez recevoir, Mesdames, Messieurs, l'assurance de nos sentiments très distingués.

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER



Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude SIMON
Directeur

Claude MARX
Directeur général

Annexes

Annexe 1: Instructions techniques pour l'envoi des fichiers

Pour la transmission des données à la CSSF, les entités rapportantes doivent utiliser le template disponible sur le site CSSF sous:

https://www.cssf.lu/fr/Document/notification-incidents-majeurs/

Instructions de remise

Le rapport principal doit être une copie du fichier ".xlsx" ci-dessus remplie avec les données de l'incident. Le fichier ci-dessus est préformaté et **sa structure ne doit être modifiée de quelque façon que ce soit** par les entités rapportantes.

Les fichiers annexes au rapport principal peuvent avoir des extensions tyiques d'application de type Office (".pdf", ".docx", etc)

Tous les fichiers doivent être envoyés à la CSSF via un canal de transmission selon la circulaire CSSF 08/334. La convention de nom à utiliser est OTH.

La structure de nom générale à utiliser est (voir détails ci-dessous) :

OTHREP-ENNNN-MAJINCREP-YYYYMMDDHHMM-AAAA.extension

Exemples:

OTHREP-B0999-MAJINCREP-201901301700-0000.xlsx

Pour le document principal du rapport d'incident remis par la banque B999 pour un incident du 30 janvier 2019 à 17:00

OTHREP-B0999-MAJINCREP-201901301700-0001.pdf

Pour une première annexe au document principal du rapport d'incident ci-dessus

OTHREP-W0999-MAJINCREP-201901301700-0000.xlsx

Pour le document principal du rapport d'incident remis par l'établissement de monnaie électronique W999 pour un incident du 30 janvier 2019 à 17:00

Remarque: si une nouvelle version du rapport principal ou d'une autre annexe doit être envoyée pour refléter une évolution de la situation, le même numéro d'annexe que pour l'envoi précédent sera réutilisé.

Signification :

Code	Signification	Structure	Valeurs autorisées
TYR	Type de rapport	Char(3)	Constante 'OTH'
DIR	Direction	Char(3)	'REP' pour Report → fichier vers CSSF 'FBR' pour accusé de réception → confirmation de bonne réception par la CSSF à l'entité rapportante
-	Séparateur	Char(1)	Constante '-' (tiret)
E	Entité	Char(1)	Tout type d'entité assigné par la CSSF, p.ex. 'B' pour Banques, 'P' for PSF, 'W' pour établissements de monnaie électronique, …
NNNN	CSSF ID	Number(4)	0001…9999 Identifiant de l'entité assigné par la CSSF
-	Séparateur	Char(1)	Constante '-' (tiret)
TTTTTTTTT	TYPE	Char(9)	La seule valeur autorisée est 'MAJINCREP' (Major Incident Report).
-	Séparateur	Char(1)	Constante '-' (tiret)
YYYYMMDDHHMM	Date et heure identifiant l'incident	Number(12) in format YYYYMMDDHHMM	Timestamp représentant la date et l'heure de l'incident identifiant l'ensemble de tous les documents qui s'y rapportent p.ex. '201901301700' pour un incident du 30 janvier 2019 à 17:00. (**ce timestamp servira de clé/identifiant de l'incident** et sera

			réutilisé pour toutes les annexes de l'ensemble de documents)
-	Séparateur	Char(1)	Constante '-' (tiret)
AAAA	Annexe	Number(4)	0001…9999 L'annexe 0000 sera le document principal de l'ensemble de documents (le template ci-dessus à télécharger du site CSSF), 0001 à 9999 peuvent être utilisées pour des annexes supplémentaires au document principal
Ext	Extension	Char(5)	L'annexe 0000 est en .xlsx (téléchargé du site CSSF). En general, toutes les extensions "Office" sont permises pour les autres annexes (".pdf", ".docx", etc.).

EBA/GL/2017/10

27/07/2017

Final Report

Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)

Abbreviations

AISP	Account information service provider
ASPSP	Account servicing payment services provider
B2B	Business to Business
B2C	Business to Consumer
CA	Competent Authority
CEBS	Committee of European Banking Supervisors
EBA	European Banking Authority
ECB	European Central Bank
EMD	Electronic Money Directive
GL	Guideline
PISP	Payment initiation services provider
PSD2	Payment Services Directive (EU) 2015/2366
PSP	Payment services provider
SSM	Single Supervisory Mechanism
TPPs	Third Party Providers

Contents

1. Executive Summary **4**

2. Background and rationale **5**

2.1. Background 5

2.2. Rationale 6

3. Guidelines **14**

4. Accompanying documents **45**

4.1. Cost-benefit analysis / impact assessment 45

4.2. Feedback on the public consultation 49

1. Executive Summary

Article 96(3) of Directive (EU) 2015/2366 on Payment Services in the Internal Market (PSD2) confers on the European Banking Authority (EBA) the mandate to develop, in close cooperation with the European Central Bank (ECB), Guidelines addressed to payment services providers (PSP) on the classification and notification of major operational or security incidents, and to competent authorities on the criteria to assess their relevance and the details to be shared with other domestic authorities. To fulfil this mandate, the EBA and the ECB have assessed existing scenarios and practices as regards incident reporting and have produced the Guidelines included in this Final Report.

These Guidelines set out the criteria, thresholds and methodology to be used by payment service providers to determine whether or not an operational or security incident should be considered major and, therefore, be notified to the competent authority in the home Member State. Moreover, these Guidelines establish the template that payment service providers will have to use for this notification and the reports they have to send during the lifecycle of the incident, including the timeframe to do so.

To ensure that current practices are reflected to the greatest extent possible, these Guidelines also allow for the possibility that payment service providers delegate their incident-reporting obligations to a third party, provided that a number of conditions are met. Furthermore, the Guidelines give payment service providers the possibility of reporting their incidents through a service provider in a way that is consolidated with other affected payment service providers, provided that the incident originates within said provider.

Furthermore, these Guidelines establish a set of criteria that competent authorities have to use as primary indicators when assessing the relevance of a major operational or security incident to other domestic authorities in the context of PSD2. Moreover, they detail the information that, as a minimum, competent authorities should share with these domestic authorities when an incident is considered of relevance for the latter.

Finally, for the purposes of promoting a common and consistent approach, these Guidelines also establish requirements regarding the reporting process envisaged in Article 96(2) of PSD2 between competent authorities in the home Member State and the EBA/ECB.

To seek the views of the market, the EBA published a Consultation Paper on the draft Guidelines on major incident reporting on 7 December 2016. The consultation ran for three months, and 43 responses were received. Following analysis of the comments put forward by the market, the EBA has made some amendments to the draft Guidelines, in particular as regards further defining the criteria, reviewing one of the thresholds, extending the deadline for the first report, streamlining the amount of information to be provided at that stage and generally clarifying the information to be provided in each of the reports.

2. Background and rationale

2.1. Background

1. Article 96 of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) requires payment service providers 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 payment service providers or payment systems is kept to a minimum, Article 96 lays down that payment service providers shall report major operational or security incidents to the competent authority in their home Member State without undue delay. It is also expected that this competent authority, after assessing the relevance of the incident to other relevant domestic authorities, will notify them accordingly.

3. To achieve this aim, Article 96(3) of PSD2 confers 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. payment service providers, 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 assigns to the EBA and the ECB a central coordination role in this context in relation to other relevant EU and national authorities. The Directive provides that the competent authority in the home Member State swiftly shares 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. On 7 December 2016 the EBA launched a consultation on the draft Guidelines on major incident reporting, which ended on 7 March 2017. The EBA received 43 responses to the Consultation Paper, 36 of which gave permission for the EBA to publish them on the EBA website. In what follows in the rationale section below, this Final Report summarises the comments received and the decisions that the EBA has taken.

2.2. Rationale

6. The EBA has assessed all the responses and has arrived at the main conclusions set out below, which are presented using the structure of the Guidelines: they start with the definitions, followed by the Guidelines addressed to payment service providers, and finish with some general comments, some of which refer to the Guidelines addressed to competent authorities. Additional, more detailed, feedback to all concerns received is provided in the feedback table in Chapter 4.2 of this Final Report.

Definitions

7. In general, the definitions seemed to be clear enough, although several respondents proposed adopting definitions from international standards to ensure a common understanding and reduce the burden on firms. Furthermore, there were some suggestions aiming to improve the clarity of the definitions by, for instance, specifying further the scope of 'major operational or security incident' or defining more precisely the five dimensions that could be affected. Several respondents also favoured focusing the definition on 'operational or security incident' instead of on 'major operational or security incident'.

8. The EBA has assessed the comments received and notes that the definitions are generally based on international standards, although it acknowledges that there is not an exact correlation. The reason for this is that they had to be adapted to the scope of PSD2, on which the EBA's mandate is based. The EBA particularly relied on international standards for the definition of the five dimensions, and that is why the EBA considers they should remain unchanged. The only exception would be the term 'continuity', since the definition of this term does not come from any international standard, and the EBA acknowledges that it could be confused with the concept of 'availability'. Therefore, the EBA has further clarified it to avoid misunderstandings. The other main change as regards the dimensions is the replacement of the word 'client' with 'payment service user' in the definition of 'availability' and throughout the Guidelines, since it led to confusion. Over and above, by relying on the latter term, the Guidelines manage to align even more closely with PSD2.

9. As regards the suggestion to specify the scope of 'major operational or security incident', the EBA concludes that part of the confusion came from the Background and Rationale section of the Consultation Paper and, hence, there is no need to clarify further in the Guidelines that all major operational or security incidents affecting payment services or any tasks needed to carry them out are included under their scope.

10. Also, to avoid confusion, the Guidelines have been amended so that the definition section now refers to the broader concept of 'incidents', while the criteria for the classification of the subset of incidents that are 'major' are set out separately in Guideline 1. Relatedly, the scope of application section has been amended to clarify that all external and internal events that have not been planned by the payment service provider would be included in the definition, bearing in mind that these could be either malicious or accidental.

11. Finally, the EBA has assessed the proposal to define 'operational or security incident' instead of 'major operational or security incident', but has discarded the idea, since the EBA believes that the term that needs to be defined in the Guidelines is the one that PSD2 refers to. Nevertheless, the definition has been amended to improve clarity by dropping the term 'material' and explaining further what 'major' is.

12. A specific comment on the definition of 'major operational or security incident' was also received, namely that it should not include incidents that have only a potential (not materialised) major impact. The EBA, however, could not take this proposal fully on board, since it would go against the spirit of PSD2, i.e. that the competent authority in the home Member State is informed of a major operational or security incident as soon as possible. The Guidelines, however, now clarify that incidents that could have been major but are resolved before they reach that point (i.e. 'near misses') are not included and, hence, do not need to be reported. Furthermore, the revised definition limits the range of potential incidents to be reported by replacing the term 'may have [impact]' with 'will probably have [impact]'.

Criteria, thresholds and methodology

13. A majority of the respondents considered that the proposal would result in a higher number of incidents being classified as major than is currently the case. The main arguments put forward were the use of qualitative criteria (which, in addition, were considered too broadly defined) and the use of absolute values as thresholds (in particular as regards 'transactions affected'). Respondents therefore suggested removing both the qualitative criteria (or at least specifying them further) and the absolute thresholds (or else significantly increasing them). There was also a suggestion to remove the 'economic impact' criterion, since it was considered too difficult to estimate (in particular, the indirect costs).

14. A few respondents also suggested laying down that a given condition must be met if an incident is to be classified as major, regardless of whether the criteria are fulfilled or not, and others proposed having a second layer of assessment by senior management to ensure that only the actually relevant incidents are reported. It is also worth mentioning that some respondents pointed out that the terms 'Level 1' and 'Level 2' were counterintuitive. Moreover, a few of them expressed doubts about whether the use of cumulative thresholds in Level 1 and non-cumulative in Level 2 was intentional or not and, if so, what its goal was.

15. The EBA has assessed all these comments and wishes to highlight that qualitative criteria are widely used in the current reporting frameworks at local level, with apparently no issues. Furthermore, the EBA considers these criteria to be a very good complement of the quantitative ones, since they help provide a more accurate assessment of the incident on the basis of past experience at times when actual data (i.e. figures) on the impact of the incident may not be easily available. The EBA acknowledges, however, that the way the qualitative criteria should be assessed could be specified further, and has therefore introduced several clarifications in Guideline 1.2. The EBA also considers that the 'economic impact' criterion should remain, since it is consistent with the EU's Single Supervisory Mechanism SSM's approach and gives an additional dimension about the relevance of the incident, but has introduced a nuance in the way it should

be measured in order to make it easier. In any case, the EBA notes that the use of estimations and educated guesses is possible when assessing whether or not an incident is major.

16. As regards the thresholds, the EBA has taken note of the potential confusion introduced by the terms 'Level 1' and 'Level 2' and has replaced them with 'Lower impact level' and 'Higher impact level'. The EBA is also of the view that cumulative versus alternative thresholds, where applicable, introduce proportionality. This allows the striking of an important and necessary balance between both smaller and larger payment service providers, so the EBA has made the necessary amendments to the Guidelines to highlight where and when PSPs should take them into account simultaneously or not.

17. Furthermore, the EBA has reassessed the possibility of removing the absolute thresholds, but is still of the opinion that they are necessary to ensure a level playing field between smaller and larger payment service providers. The EBA has also explored the possibility of increasing the 'Higher impact level' thresholds, since those are in principle the ones that could lead to over-reporting, and has concluded that the threshold associated with 'transactions affected' could indeed be too low on account of the nature of Business-to business (B2B) payments. As a result, the EBA has raised it to EUR 5 million.

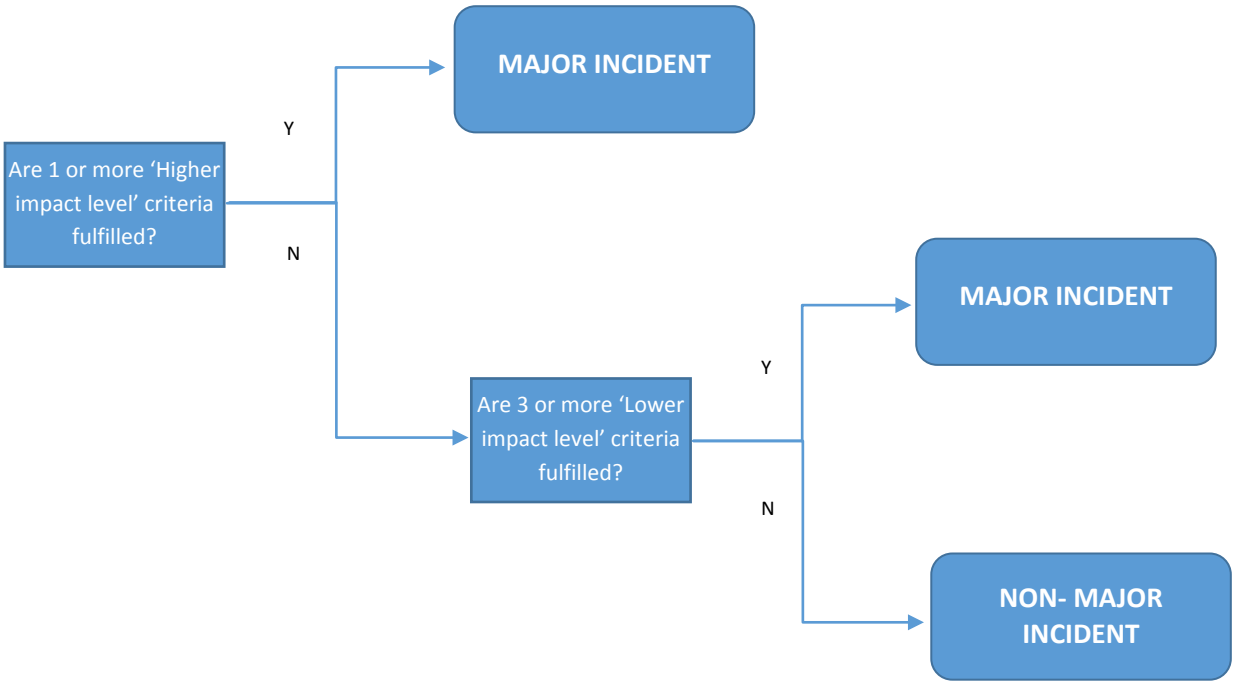
18. Finally, and contrary to the suggestions made by some respondents, the EBA has decided not to introduce any type of particular condition beyond the chosen criteria. In fact, the EBA believes that most of the suggested conditions would already be covered by the criteria considered in the Guidelines. Likewise, the EBA is against allowing payment service providers to somehow override the conclusions of the assessment on the basis of a subjective decision, since the main purpose of the Guidelines is precisely to harmonise the classification and reporting of major incidents for all payment service providers.

19. Several comments were also received on the methodology for assessing the different criteria (beyond the request to further specify the qualitative ones) as well as on the way they should be combined to conclude whether the incident is major or not. As regards the former, a large majority of respondents considered that more instructions were needed on how to calculate 'transactions affected' and 'clients (now payment service users) affected'. As regards the latter, a few respondents questioned the chosen number of criteria needed for an incident to qualify as major and others requested further clarity by, for instance, including Diagram 1 in the Guidelines. In addition, a number of respondents considered that more clarity was needed on whether the thresholds would actually have to be exceeded or the mere possibility of their being exceeded at some point in the future would suffice in view of the classification process.

20. The EBA acknowledges that the way the criteria should be measured was not detailed enough, and has therefore expanded Guideline 1.2 to clarify the different issues put forward by the respondents. Furthermore, the EBA considers that the requirement to fulfil three criteria at the 'Lower impact level' strikes an important and necessary balance between smaller and larger payment service providers and between quantitative and qualitative criteria. As regards the possibility of introducing the diagram in the Guidelines, the EBA notes that diagrams are not meant to be part of a set of actual EBA Guidelines, but it has kept it in the Rationale section for clarity. Finally, the EBA has amended Guidelines 1.3 and 1.4 to explain that, to assess whether or

not an incident should be labelled as major, payment service providers should consider both if the thresholds are reached and if there is a possibility that they will be reached before the incident is resolved.

Diagram 1: Decision tree for assessing whether or not an operational or security incident is major



Legend:
- If an incident meets or will probably meet one or more 'Higher impact level' thresholds, it qualifies as major.
- If an incident does not meet and probably will not meet any 'Higher impact level' thresholds, but meets or will probably meet 3 or more 'Lower impact level' thresholds, it qualifies as major.
- If an incident does not meet and probably will not meet any 'Higher impact level' thresholds and does not meet and probably will not meet at least three 'Lower impact level' thresholds, it does not qualify as major.

21. Over and above those, a few respondents made suggestions along the lines of applying criteria and/or thresholds in a way that differentiates between categories of payment service providers on the basis of the type of payment service that they provide (e.g. to consider the downtime of the ASPSP's dedicated interface for third party providers – PISPs, AISPs – a major incident for the ASPSP). The EBA has assessed these proposals but finally decided not to adopt them, as the benefits of such an approach are not clear while it would most likely lead to increased and unnecessary complexity, resulting in a less level playing field.

Template and instructions

22. A large group of respondents considered that the template was not clear enough as regards what should be reported in each phase of the incident and which fields are mandatory and which are not. A few of them understood that payment service providers needed to fill out as many fields as possible, and this was seen too complicated in the given timeframe. Several comments regarding

different fields of the template (e.g. the list of incident statuses, payment services affected, systems and components affected) and suggestions on potential improvements (e.g. clarify that multiple boxes may be ticked in some instances, indicate if figures are estimations, include a measurement of staff impact) were also received.

23. The EBA acknowledges that it was indeed not always comprehensible from the outset which information is expected from payment service providers in each phase. Hence, taking into consideration the concerns about the time needed to fill it out, the EBA has reorganised the template in three clear sections, one for each type of report: initial, intermediate and final. Payment service providers are therefore expected to complete each of the sections in a cumulative way, so the final report contains information on all fields. This means that all fields are in principle mandatory, unless the template explicitly states otherwise (e.g. 'if applicable' or 'if already known'). The other comments and suggestions received have been considered by the EBA, and the necessary changes have been introduced in the template when relevant.

24. A few comments were also received on the instructions to complete the template, mainly seeking clarification as regards certain fields, e.g. unique identification number, country(ies) affected by the incident, incident discovery, operational incident. There was also a request to include the instructions in the Guidelines themselves.

25. The EBA notes that the instructions are technical and rather too complex to be placed in the text of the Guidelines. It emphasises that the annex is a fully fledged part of the Guidelines as well, thus having the same legal effects. As regards all other suggestions, the EBA has assessed the possibility of improving the clarity of the instructions and has amended them when considered relevant.

Notification process

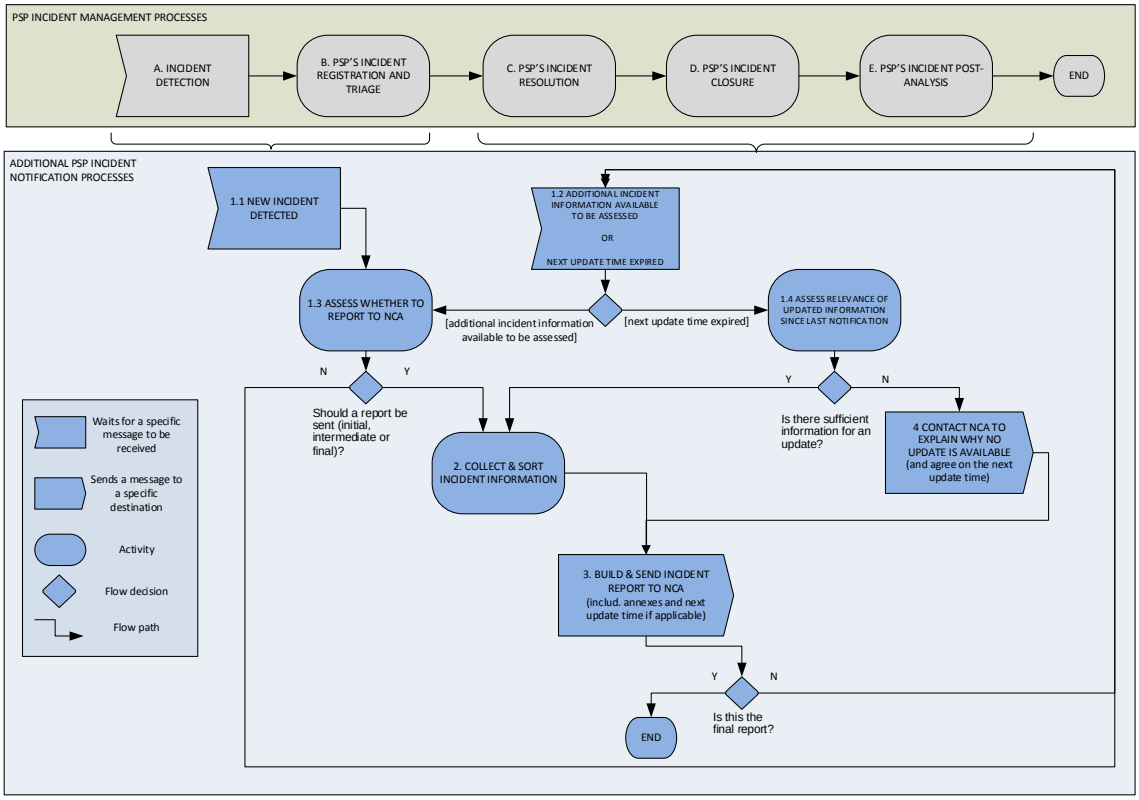
26. Respondents generally agreed with the notification process, the main exception being the deadline for submitting the initial report, which was deemed too short by most respondents given the need to devote resources to resolving the incident. Several suggestions were received on alternative deadlines, ranging from 3 to 72 hours. Furthermore, some respondents proposed that this deadline should be from the moment the incident is classified as major, and not from the moment it is detected. A few comments were also received on intermediate reports (mainly suggesting to remove them and to extend the deadline) and on final reports (to extend the deadline).

27. The EBA has assessed all replies and considers that the respondents' arguments are sensible and well founded as regards the deadline for the initial report. It has therefore extended the deadline from 2 hours to 4 hours along with limiting the amount of information to be provided in the initial report. Nevertheless, the EBA considers the deadlines for the other reports to be adequate to balance the burden on payment service providers and the need for competent authorities to be informed of the development of the incident. That is also why the EBA considers that intermediate reports should remain.

28. Furthermore, some requests for clarification were put forward, namely on (i) the way to proceed when a major incident has been resolved within the deadline for submitting the initial report, (ii) whether or not intermediate and/or final reports are needed when the source is in an external provider and (iii) whether or not Diagram 2 constitutes a requirement to set up a separate sub-process having exactly the same structure.

29. The EBA wishes to clarify that major incidents resolved within the deadline to submit the initial report should also be notified, with the peculiarity that the initial report may also constitute the last intermediate report and, potentially, the final report. Furthermore, the EBA confirms that intermediate and final reports are indeed required when the source is in an external provider and that Diagram 2 is not a requirement, since it is not included in the Guidelines, but simply aims to depict the notification process for clarity purposes. The EBA still believes in the usefulness of this diagram and has, accordingly, kept it in the Rationale section as seen below.

Diagram 2: Incident notification process from payment service providers to the competent authority in the home Member State



Delegated and consolidated reporting

30. A majority of respondents welcomed the option to delegate the reporting, also in a consolidated way, although a few of them noted that incident reporting should be the responsibility of the payment service provider. To benefit further from this option, some respondents requested that the following conditions be removed: that the third party should be established in the Union, that the competent authority should be informed beforehand, and that the consolidated report is limited to incidents stemming from a disruption of technical services. Another respondent asked for the possibilities of providing average values for measuring the impact instead of the figures corresponding to each payment service provider, and of assessing the incident on a consolidated

basis. In addition, a number of respondents requested further clarifications in the Guidelines as regards the formal procedures to be followed for the designation of such a third party – including where the delegated entity is located in a different country – as well as for the communication of incident reports by those parties to competent authorities.

31. The EBA wishes to highlight that payment service providers remain fully responsible for the reporting of major operational or security incidents, regardless of whether this has been delegated or not. Furthermore, the EBA has assessed the suggestions received and considers that, in general, they would improve the usability of delegated and consolidated reporting, so the conditions that the third party should be established in the Union and that the incident has to stem from a technical disruption have been removed. Nevertheless, the EBA believes that competent authorities should know in advance who will send the report in case of incident, and therefore no changes have been introduced in this regard.

32. Moreover, for the particular case of consolidated reporting, the EBA notes that Article 96 of PSD2 requires that the assessment is done on an individual basis, although it expects that, in practice, the impact is similar for all payment service providers and, therefore, a detailed analysis is not necessary in most cases. As regards the impact-related information, the Guidelines – and the template – have been amended to allow the designated third party to provide value ranges (i.e. the value corresponding to the least affected payment service provider and the value corresponding to the most affected payment service provider) instead of individual information. Finally, the EBA is of the view that the formal designation and communication procedures to be applied in the case of the intervention of a third party remain within the scope of each competent authority, so no changes have been made to the Guidelines on this particular point.

Guidelines addressed to competent authorities

33. Many respondents questioned the way the EBA would treat the information provided in the incident reports, both when stored and in transit. The EBA agrees that the Guidelines could explain that the professional secrecy obligations set out in PSD2 apply, and has therefore introduced this clarification in the Guidelines.

General comments

34. Most respondents mentioned the existence of other incident-reporting frameworks and the convenience of aligning them by harmonising criteria, templates and notification processes. They also mentioned having one-stop-shop mechanisms. Many respondents also raised questions about how the EBA and relevant authorities will use the collected information and, in particular, if it will be shared with other payment service providers. Moreover, on the argument about the importance of encouraging collaboration amongst firms on these matters, several respondents expressed a desire that the Guidelines be used to promote and establish best practices addressing collaboration (especially in the case of incidents affecting Third Party Providers TPPs).

35. The EBA acknowledges that other incident notification frameworks exist, but it is not in a position to address the issue, since its mandate is limited to the scope of PSD2. The EBA would, however, like to highlight that it has tried to align the Guidelines as much as possible with the SSM's cyber

incident-reporting framework. As regards the use of the information by competent authorities and, in particular, on the issue of sharing or promoting the sharing of such information with/among payment service providers, the EBA would like to recall that this is not in the scope of PSD2 mandate and, therefore, it cannot be covered by the Guidelines. In any case, the EBA would like to underline the fact that the Guidelines do not forbid payment service providers to share information about reported incidents on a voluntary basis, and concurs that such an initiative would bring about benefits if it became standard practice in the market.

3. Guidelines

EBA/GL/2017/10

27/07/2017

Guidelines

on major incident reporting under Directive (EU) 2015/2366 (PSD2)

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.[1] 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 out the EBA's 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. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA that they comply or intend to comply with these Guidelines, or otherwise give 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 to compliance@eba.europa.eu with the reference 'EBA/GL/2017/10'. 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 the EBA.

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

[1] 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 the 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 laid down 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 be either 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 in some other way as a result of the incident).

Addressees

12. 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.

13. The second and third sets 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

14. 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 probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity 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 accessible and usable by payment service users.
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.
Continuity	The property of an organisation's processes, tasks and assets needed for the delivery of payment-related services being fully accessible and running at acceptable predefined levels.
Payment-related services	Any business activity in the meaning of Article 4(3) of PSD2, and all the necessary technical supporting tasks for the correct provision of payment services.

3. Implementation

Date of application

15. These Guidelines apply from 13 January 2018.

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. Service downtime

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

iv. Economic impact

Payment service providers should determine the monetary costs associated with 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).

v. High level of internal escalation

Payment service providers should determine whether or not this incident has been or will probably be reported to their executive officers.

vi. Other payment service providers or relevant infrastructures potentially affected

Payment service providers should determine the systemic implications that the incident will probably 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 card payment schemes.

vii. Reputational impact

Payment service providers should determine how the incident can undermine users' 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 probably be directly or indirectly affected 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 (whether the funds have been recovered or not).

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. If payment service providers do not consider this figure to be representative (e.g. because of 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 Annex 1).

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 probably suffer the consequences of the incident. Payment service providers should resort to estimations based on past activity 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 consider only its own payment service users. In the case of a payment service provider offering operational services to others, that payment service provider should consider only 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.

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 to 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. 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 probably be down and, thus, prevents (i) the initiation and/or execution of a payment service and/or (ii) access to a payment 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.

iv. Economic impact

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 with contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, payment service providers should consider only those that are already known or very likely to materialise.

v. *High level of internal escalation*

Payment service providers should consider whether or not, as a result of its impact on payment-related services, the Chief Information Officer (or similar position) has been or will probably be informed 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 or not, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.

vi. *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 card payment schemes that support them and other payment service providers. In particular, payment service providers should assess whether or not the incident has been or will probably be replicated at other payment service providers, whether or not it has affected or will probably affect the smooth functioning of financial market infrastructures and whether or not it has compromised or will probably 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 and whether or not the payment service provider has stopped or will probably stop fulfilling its obligations in the financial market infrastructures of which it is a member.

vii. *Reputational impact*

Payment service providers should consider the level of visibility that, to the best of their knowledge, the incident has gained or will probably gain in the marketplace. In particular, payment service providers should consider the likelihood that the incident will cause harm to society as a good indicator of its potential to affect their reputation. Payment service providers should take into account whether or not (i) the incident has affected a visible 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.), (ii) regulatory obligations have been or will probably be missed, (iii) sanctions have been or will probably be breached or (iv) the same type of incident has occurred before.

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

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** > EUR 100 000	> 25% of the payment service provider's regular level of transactions (in terms of number of transactions) **or** > EUR 5 million
Payment service users affected	> 5 000 **and** > 10% of the payment service provider's payment service users	> 50 000 **or** > 25% of the payment service provider's payment service users
Service downtime	> 2 hours	Not applicable
Economic impact	Not applicable	> Max. (0.1% Tier 1 capital,* EUR 200 000) **or** > EUR 5 million
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

*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 of whether or not a given threshold is or will probably be reached before the incident is resolved (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, to identify any possible status change, either upwards (from non-major to major) or downwards (from major to non-major).

Guideline 2: Notification process

2.1. Payment service providers should collect all relevant information, produce an incident report using the template provided in Annex 1 and submit it to the competent authority in the home Member State. Payment service providers should fill out the template following the instructions provided in Annex 1.

2.2. Payment service providers should use the same template to inform the competent authority throughout the lifetime of the incident (i.e. for initial, intermediate and final reports, as described in paragraphs 2.7 to 2.21). Payment service providers should complete the template in an incremental manner, on a best effort basis, as more information becomes readily available in the course of their internal investigations.

2.3. Payment service providers should also 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 laid down in the second paragraph of Article 96(1) of PSD2, as soon as it is available.

2.4. Payment service providers should furnish the competent authority in the home Member State, if available and deemed relevant for the competent authority, with any additional information by appending supplementary documentation to the standardised template as one or various annexes.

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 with the competent authority in their home Member State and also authenticate themselves properly 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 when a major operational or security incident is first detected.

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

2.9. Payment service providers should also submit an initial report to the competent authority in the home Member State when a previously non-major incident becomes 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 operational at that time, as soon as they become available/operational again.

2.10. Payment service providers should include headline-level information (i.e. section A of the template) in their initial reports, thus featuring some basic characteristics of the incident and its expected consequences based on the information available immediately after it was detected or reclassified. Payment service providers should resort to estimations when actual data are not available. Payment service providers should also include in their initial report the date for the next update, which should be as soon as possible and under no circumstances go beyond 3 business days.

Intermediate report

2.11. Payment service providers should submit intermediate reports every time they consider that there is a relevant status update and, as a minimum, by the date for the next update indicated in the previous report (either the initial report or the previous intermediate report).

2.12. Payment service providers should submit to the competent authority a first intermediate report with a more detailed description of the incident and its consequences (section B of the template). Moreover, payment service providers should produce additional intermediate reports by updating the information already provided in sections A and B of the template at least, when they become aware of new relevant information or significant changes since the previous notification (e.g. whether the incident has escalated or decreased, new causes identified or actions taken to fix the problem). In any case, payment service providers should produce an intermediate report at the request of the competent authority in the home Member State.

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

2.14. Furthermore, payment service providers should indicate in each report the date for the next update, which should be as soon as possible and under no circumstances go beyond 3 business days. Should the payment service provider not be able to comply with the estimated date for the next update, it should contact the competent authority in order to explain the reasons behind the delay, propose a new plausible submission deadline (no longer than 3 business days) and send a new intermediate report updating exclusively the information regarding the estimated date for the next update.

2.15. Payment service providers should send the last intermediate report when regular activities have been recovered and business is back to normal, informing the competent authority of this circumstance. Payment service providers should consider that business is back to normal when activity/operations are restored to the same level of service/conditions as defined by the payment service provider or laid out externally by a Service Level Agreement (SLA) in terms of processing times, capacity, security requirements, etc., and contingency measures are no longer in place.

2.16. Should business be back to normal before 4 hours have passed since the incident was detected, payment service providers should aim to submit both the initial and the last intermediate report simultaneously (i.e. filling out sections A and B of the template) by the 4-hour deadline.

Final report

2.17. Payment service providers should send a final report when the root cause analysis has taken place (regardless of whether or not mitigation measures have already been implemented or the final root cause has been identified) and there are actual figures available to replace any estimates.

2.18. Payment service providers should deliver the final report to the competent authority within a maximum of 2 weeks after business is deemed back to normal. Payment service providers needing an extension of this deadline (e.g. if there are no actual figures on the impact available yet) should contact the competent authority before it 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 4-hour window since the incident was detected, they should aim to submit in their initial report the information related to initial, last intermediate and final reports.

2.20. Payment service providers should aim to include in their final reports 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 the root cause, if already known, and a summary of measures adopted or planned to be adopted to remove the problem and prevent its recurrence 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 no longer fulfils the criteria to be considered major and is not expected to fulfil them before the incident is resolved. In this case, payment service providers should send the final report as soon as this circumstance is detected and, in any case, by the estimated date for the next report. In this particular situation, instead of filling out section C of the template, payment service providers should tick the box 'incident reclassified as non-major' and explain the reasons justifying this downgrading.

Guideline 3: Delegated and consolidated reporting

3.1. Where permitted by the competent authority, payment service providers wishing to delegate reporting obligations under 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 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 (EMD); or

   ii. the CEBS Guidelines on outsourcing in relation to credit institutions.

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, include the contact

information included under 'Affected PSP' in the template and make certain that 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's 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. Ensure that the third party assesses the materiality of the incident for each affected payment service provider and includes in the consolidated report only those payment service providers for which the incident is 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 that it should not.

e. Ensure that, when there are fields of the template where a common answer is not possible (e.g. section B 2, B 4 or C 3), the third party either (i) fills them out individually for each affected payment service provider, further specifying the identity of each payment service provider to which the information relates, or (ii) uses ranges, in those fields where this is an option, representing the lowest and highest values as observed or estimated for the different payment service providers.

f. 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 that the third party may have with the competent authority and of the contents thereof, but only as far as is compatible with avoiding 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 informed 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, in accordance with 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 PSD2 and with these Guidelines. Furthermore, payment service providers should ensure that an incident is not reported twice, individually by said payment service provider and once again by the third party.

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 PSD2, as well as the processes implemented 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. its 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 on 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, to identify any possible change that could make an incident relevant 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. last 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. To do so, they should provide, as a minimum, the information given 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 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 with other relevant domestic authorities and also authenticate themselves properly 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 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 the EBA and the ECB with all reports received from (or on behalf of) payment service providers affected by a major operational or security incident (i.e. initial, intermediate and final reports).

Guideline 8: Communication

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

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

Annex 1 – Reporting templates for payment service providers

Major Incident Report		
☐ Initial report	within 4 hours after detection	
☐ Intermediate report	maximum of 3 business days from previous report	
☐ Last intermediate report		
☐ Final report	within 2 weeks after closing the incident	
☐ Incident reclassified as non-major	Please explain:	
Report date	DD/MM/YYYY	Time HH:MM
Incident identification number, if applicable (for interim and final reports)		

A - Initial report					
A 1 - GENERAL DETAILS					
Type of report					
Type of report	☐ Individual	☐ Consolidated			
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
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					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION					
Date and time of detection of the incident	DD/MM/YYYY, HH:MM				
The incident was detected by (1)		If Other, please explain:			
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)					
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM				

B - Intermediate report		
B 1 - GENERAL DETAILS		
Please provide a more DETAILED description of the incident. e.g. information on: - What is the specific issue? - How it happened - How did it develop - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Areas affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (Central Bank Crisis management)) - PSP internal classification of the incident		
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM	
Incident status	☐ Diagnostics ☐ Repair	☐ Recovery ☐ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM	

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT	
Overall impact	☐ Integrity ☐ Confidentiality ☐ Continuity ☐ Availability ☐ Authenticity
Transactions affected [2]	Number of transactions affected ☐ Actual figure ☐ Estimation As a % of regular number of transactions ☐ Actual figure ☐ Estimation Value of transactions affected in EUR ☐ Actual figure ☐ Estimation Comments:
Payment service users affected [3]	Number of payment service users affected ☐ Actual figure ☐ Estimation As a %-of total payment service users ☐ Actual figure ☐ Estimation
Service downtime [4]	Total service downtime DD:HH:MM ☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR ☐ Actual figure ☐ Estimation Indirect costs in EUR ☐ Actual figure ☐ Estimation
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO 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	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)
B 3 - INCIDENT DESCRIPTION	
Type of Incident	☐ Operational ☐ Security
Cause of incident	☐ Under investigation ☐ External attack → Type of attack: ☐ Distributed/Denial of Service (D/DoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other (If Other, specify) ☐ Internal attack ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other If Other, specify
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly If indirectly, please provide the service provider's name
B 4 - INCIDENT IMPACT	
Building(s) affected (Address), if applicable	
Commercial channels affected	☐ Branches ☐ Telephone banking ☐ Point of sale ☐ E-banking ☐ Mobile banking ☐ Other ☐ ATMs If Other, specify:
Payment services affected	☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement ☐ Communication ☐ Direct settlement ☐ Other If Other, specify:
Systems and components affected	☐ Application/software ☐ Hardware ☐ Database ☐ Network/infrastructure ☐ Other If Other, specify:
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)
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? If so, please describe	☐ YES ☐ NO DD/MM/YYYY, HH:MM
Has the PSP cancelled or weakened some controls because of the incident? If so, please explain	☐ YES ☐ NO

C - Final report	
If no intermediate report has been sent, please also complete section B	
C 1 - GENERAL DETAILS	
Please update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root cause analysis - lessons learnt - addittional actions - any other relevant information	
Date and time of closing the incident	DD/MM/YYYY, HH:MM
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place?	☐YES ☐ NO
If so, please explain	
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP	
What was the root cause (if already known)? (possible to attach a file with detailed information)	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	
C 3 - ADDITIONAL INFORMATION	
Has the incident been shared with other PSPs for information purposes?	☐YES ☐ NO
If so, please provide details	
Has any legal action been taken against the PSP?	☐YES ☐ NO
If so, please provide details	

Notes:
(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above
(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100000; > 25% of regular level of transactions or > EUR 5 milion; none of the above
(3) Pull-down menu: > 5000 and > 10% payment service users; > 50000 or > 25% payment service users; none of the above
(4) Pull-down menu: > 2 hours; < 2 hours
(5) Pull-down menu: > Max (0,1% Tier 1 capital, EUR 200000) or > EUR 5 million; none of the above

CONSOLIDATED REPORT - LIST OF PSPs		
PSP Name	**PSP Unique Identification Number**	**PSP Authorisation number**

INSTRUCTIONS FOR FILLING OUT THE TEMPLATES

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. All fields are mandatory, unless it is clearly specified otherwise.

Headline

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

Intermediate report: this is an update of a previous (initial or intermediate) report on the same incident.

Last intermediate report: this informs the competent authority in the home Member State that regular activities have been recovered and business is back to normal, so no more intermediate reports will be submitted.

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 any more.

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 resolved. PSPs should explain the reasons for this downgrading.

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

Incident identification number, if applicable (for intermediate and final report): the reference number issued by the competent authority at the time of the initial report to uniquely identify the incident, if applicable (i.e. if such a reference is provided by the competent authority).

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 making use of the consolidated reporting option. 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 by 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 unique identification number, if relevant: the relevant unique identification number used in each Member State to identify the PSP, to be provided by the PSP if the field 'PSP authorisation number' is not filled in.

PSP authorisation number: home Member State authorisation number.

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, 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.

Home country: Member State in which the registered office of the PSP is situated; or if the PSP has, under its national law, no registered office, the Member State in which its head office is situated.

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). It may or may not be the same as the home Member State.

Primary contact person: first name and surname of the person responsible for reporting the incident or, if a third party reports on behalf of the affected PSP, first 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 to call with any requests for further clarifications, if needed. It can be either a personal or a corporate phone number.

Secondary contact person: first name and surname of an alternative person who could be contacted by the competent authority to inquiry about an incident when the primary contact person is not available. If a third party reports on behalf of the affected PSP, first name and surname of an alternative person in the incident management/risk department or similar area, at the affected PSP.

Email: email address of the alternative 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 alternative contact person to call with any requests for further clarifications, if needed. It can be either a personal or a corporate phone number.

Reporting entity: this section should be completed if 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.

Unique identification number, if relevant: the relevant unique identification number used in the country where the third party is located to identify the entity that is reporting the incident, to be provided by the reporting entity if the field 'Authorisation number' is not filled in.

Authorisation number, if applicable: the authorisation number of the third party in the country where it is located, when applicable.

Primary contact person: first 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 to call with any requests for further clarifications, if needed. It can be either a personal or a corporate phone number.

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

Email: email address of the alternative 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 alternative contact person to call with 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 initial classification

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

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.

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

What is the estimated time for the next update?: indicate the estimated date and time for the submission of the next update (interim or final report).

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 points featured in the questionnaire (what specific issue the PSP is facing, how it started and developed, possible connection with a previous incident, consequences, especially for payment service users, etc.).

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

Incident status:

Diagnostics: the characteristics of the incident have just been identified.

Repair: the attacked items are being reconfigured.

Recovery: the failed items are being restored to their last recoverable state.

Restoration: the payment-related service is being provided again.

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.

B 2 – Incident classification/Information on the incident

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

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

Availability: the property of payment-related services being accessible and usable by payment service users.

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.

Continuity: the property of an organisation's processes, tasks and assets needed for the delivery of payment-related services being fully accessible and running at acceptable predefined levels.

Transactions affected: PSPs should indicate which thresholds are or will probably 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 specific values for these variables, which may be either actual figures or estimations. Entities reporting on behalf of several PSPs (i.e. consolidated reporting) may provide value ranges instead, representing the lowest and highest values observed or estimated within the group of PSPs included in the report, separated by a hyphen. As a general rule, PSPs should understand as 'transactions affected' all domestic and cross-border transactions that have been or will probably be directly or indirectly affected 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 (whether the funds have 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. If PSPs do not consider this figure to be representative (e.g. because of 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 probably be reached by the incident, if any, and the related figures: total number of payment service users that have been affected 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. Entities reporting on behalf of several PSPs (i.e. consolidated reporting) may provide value ranges instead, representing the lowest and highest values observed or estimated within the group of PSPs included in the report, separated by a hyphen. 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 probably suffer the consequences of the incident. PSPs should resort to estimations based on past activity 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 consider only its own payment service users. In the case of a PSP offering operational services to others, that PSP should consider only 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 to 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.

Service downtime: PSPs should indicate if the threshold is or will probably 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. Entities reporting on behalf of several PSPs (i.e. consolidated reporting) may provide a value range instead, representing the lowest and highest values observed or estimated within the group of PSPs included in the report, separated by a hyphen. PSPs should consider the period of time that any task, process or channel related to the provision of payment services is or will probably be down and, thus, prevents (i) the initiation and/or execution of a payment service and/or (ii) access to a payment 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 if the threshold is or will probably 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. Entities reporting on behalf of several PSPs (i.e. consolidated reporting) may provide a value range instead, representing the lowest and highest values observed or estimated within the group of PSPs included in the report, separated by a hyphen. 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 with contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, PSPs should consider only those that are already known or very likely to materialise.

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

High level of internal escalation: PSPs should consider whether or not, as a result of its impact on payment-related services, the Chief Information Officer (or similar position) has been or will probably be informed about the incident outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. In the case of delegated reporting, the escalation would take place within the third party. Furthermore, PSPs should consider whether or not, 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 card payment schemes that support it and the rest of the PSPs. In particular, PSPs should assess whether or not the incident has been or will probably be replicated at other PSPs, whether or not it has affected or will probably affect the smooth functioning of financial market infrastructures and whether or not it has compromised or will probably 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 and whether or not the PSP has stopped or will probably stop fulfilling its obligations in the financial market infrastructures of which it is a member.

Reputational impact: PSPs should consider the level of visibility that, to the best of their knowledge, the incident has gained or will probably gain in the marketplace. In particular, PSPs should consider the likelihood that the incident will cause harm to society as a good indicator of its potential to affect their reputation. PSPs should take into account whether or not (i) the incident has affected a visible 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.), (ii) regulatory obligations have been or are likely to be missed, (iii) sanctions have been or are likely to be breached or (iv) the same type of incident has occurred before.

B 3 – Incident description

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, authenticity and/or continuity of payment-related services.

Security: unauthorised access, use, disclosure, disruption, modification or destruction of the PSP's assets that affect the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services. This may happen when, among other things, the PSP experiences cyberattacks, inadequate design or implementation of security policies, or inadequate physical security.

Cause of incident: indicate the cause of the incident or, if it is not known yet, the one that it is most likely to be. Multiple boxes may be ticked.

Under investigation: the cause has not been determined yet.

External attack: the source of the cause comes from outside, and is intentionally targeting the PSP (e.g. malware attacks).

Internal attack: the source of the cause comes from inside, and is intentionally targeting the PSP (e.g. internal fraud).

Type of attack:

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

Infection of internal systems: harmful activity that attacks computer systems, trying to steal hard disk space or CPU time, access private information, corrupt data, spam contacts, etc.

Targeted intrusion: unauthorised act of spying, snooping and stealing information through cyberspace.

Other: any other type of attack the PSP may have suffered, either directly or through a service provider. In particular, if there has been an attack aimed at the authorisation and authentication process, this box should be ticked. Details should be added in the free text field.

External events: the cause is associated with events generally outside the organisation's control (e.g. natural disasters, legal issues, business issues and service dependencies).

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 to the payments system) or related to it somehow (e.g. the power is accidentally cut off and the payment activity is put on hold).

Process failure: the cause of the incident was 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 inadequate design, execution, components, specifications, integration or complexity of the systems that support the payment activity.

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 a PSP directly or affect it indirectly, through a third party. In the case of an indirect impact, please provide the name of the service provider(s).

B 4 – Incident impact

Building(s) affected (Address), if applicable: if a physical building is affected, please indicate its address.

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

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: electromechanical devices that allow 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.

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 ticked.

Cash placement on a payment account: the handing of cash to a PSP 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 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 in a PSP contracting with a payer to provide her with a payment instrument to initiate and process the payer's payment transactions.

Money remittance: a payment service whereby 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 whereby such funds are received on behalf of and made available to the payee.

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

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

Functional areas affected: indicate the step or steps of the payment process that have been affected by the incident. Multiple boxes may be ticked.

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 to transfer funds or securities.

Communication: flow of information for the purpose of identification, authentication, notification and information between the 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.

Systems and components affected: indicate which part or parts of the PSP's technological infrastructure have been affected by the incident. Multiple boxes may be ticked.

Application/software: programs, operating systems, etc. that support the provision of payment services by the PSP.

Database: data structure which stores personal and payment information needed to execute payment transactions.

Hardware: physical technology equipment that runs the processes and/or stores the data needed by PSPs to carry out their payment-related activity.

Network/infrastructure: telecommunications networks, either public or private, that allow the exchange of data and information during the payment process (e.g. the internet).

Other: the system and component affected is none of the above. Further details should be provided in the free text field.

Staff affected: indicate whether or not the incident has had any effects on the PSP's staff and, if so, provide details 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 to temporarily address the incident.

Have the Business Continuity Plans and/or Disaster Recovery Plans been activated?: please indicate whether or not and, if so, provide the most relevant details of what happened (i.e. when they were activated and what these plans consisted of).

Has the PSP cancelled or weakened some controls because of the incident?: please indicate whether or not the PSP has had to override some controls (e.g. stop using the four eyes principle) to address the incident and, if so, provide details of the underlying reasons justifying the weakening or cancelling of controls.

C – Final report

C 1 – General details

Update of the information from the intermediate report (summary): please provide further information on the actions taken to recover from the incident and avoid its recurrence, analysis of the root cause, lessons learnt, etc.

Date and time of closing the incident: indicate the date and time when the incident was considered closed.

Are the original controls back in place?: if the PSP had to cancel or weaken some controls because of the incident, indicate whether or not such controls are back in place and provide any additional information in the free text field.

C 2 – Root cause analysis and follow-up

What was the root cause, if already known?: please explain which is the root cause of the incident or, if it is not known yet, the preliminary conclusions drawn from the root cause analysis. PSPs may attach a file with detailed information if considered necessary.

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 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 of which PSPs have been contacted, 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 or not, at the time of filling out the final report, the PSP has suffered any legal action (e.g. been taken to court or lost its licence) as a result of the incident.

4. Accompanying documents

4.1. Cost-benefit analysis/impact assessment

Article 96(3) of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) mandates the EBA to issue Guidelines to payment service providers on the classification and notification of major operational or security incidents, and to competent authorities on the criteria to assess the incidents' relevance and on the provision of information to other domestic authorities.

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. This annex contains the impact assessment from adopting the Guidelines on incident reporting.

A. Problem identification

The market for payment services in the Union is developing very dynamically, with the number of users and providers of innovative payment services rising continuously,[2] increasing the need for an adequate regulatory and governance framework. PSD2 brings important improvements to the legal framework of the Union payment market. The Directive requires payment service providers to establish a framework to maintain effective incident management procedures, including for the detection and classification of major operational or security incidents. Article 96(1) of the Directive demands that payment service providers shall report major operational or security incidents to the competent authorities in their Member State. Article 96(2) states that competent authorities are expected to notify such incidents to the EBA and the ECB and to assess their relevance, in order to inform other national authorities accordingly.

The baseline scenario, the status quo, is the currently established incident reporting based on the requirements set by each Member State if compulsory payment-related incident reporting is already in place. The EBA stock-taking exercise depicts the current status of payment-related incident reporting in Union Member States. In general, the result states that, as the reporting of operational or security incidents is developing, there are disparities in the criteria presently applied by competent authorities for the fulfilment of reporting obligations, individual payment service providers' judgments about the appropriateness of a notification prevail and most reporting procedures currently in place are unstructured. The status quo thus allows competent authorities to apply different standards on the reporting needs, leading to different

[2] EBA (2016), *EBA Consumer Trends Report 2016*; European Commission (2015), *Green Paper on Retail Financial Services*

administrative obligations on payment service providers in different Member States and thereby hampering the establishment of a level playing field and internal market for payment services in the Union.

To address these issues, these Guidelines on incident reporting 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 such incidents to the competent authorities in the home Member State. In addition, the Guidelines determine the criteria that should govern the sharing of incident-relevant information between competent authorities and other domestic authorities and harmonise the reporting process between competent authorities and the EBA and the ECB.

B. Policy objectives

This Final Report introduces three sets of Guidelines consisting of separate Guidelines addressed to payment service providers, to competent authorities reporting to other domestic authorities, and to competent authorities reporting to the EBA and the ECB.

In general, the outlined 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. They will contribute to consistent, efficient and effective implementation of the provisions of PSD2 and enhance supervisory convergence across Member States.[3]

More specifically, the framework proposed by these Guidelines could contribute to maintaining effective incident management procedures and establishing a common and consistent approach regarding the reporting process. The notification of other national authorities as well as the EBA and the ECB contributes to improving the assessment of the collective impact on the different stakeholders in the domestic and Union payment service markets. 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, authenticity and/or continuity of the services provided by the payment service provider. Therefore, the Guidelines help to ensure that the damage to users, other payment service providers or the payment systems from operational and security incidents is minimised.

Operationally, the Guidelines are drafted considering several options, with a view to incorporating current national payment-related incident requirements and to considering the legal status and size of various types of payment service providers under the scope of PSD2.

[3] EBA (2015), *EBA Annual Report*; EBA (2016), *Work programme 2017*

C. Options considered and preferred option

During the drafting process, the prevailing classification methods, which differ widely among Member States and have a material impact on payment service providers and competent authorities, were of major concern. The EBA's stock-taking exercise shows that, while currently incidents tend to be categorised according to a compulsory requirement, in some jurisdictions reporting agents themselves can decide on the severity of the incident and if reporting is needed. In jurisdictions in which a categorisation is predefined, usually a combination of quantitative and qualitative criteria is used to determine the incident category. In general, criteria thresholds are not always clear-cut and definitions may differ substantially from one authority to another. Not only are there differences in the applicable thresholds but sometimes they are defined very broadly, thus leaving room for interpretation.

In the preferred option, the Union-wide criteria and thresholds to determine whether or not an operational or security incident is major are defined. As summarised in Table 1 of Guideline 1 on incident classification, a combination of seven quantitative and qualitative criteria is retained. They are chosen based on most commonly used practices in the Member States. In general, they consider the magnitude and scope of the impact, the amount at risk, the impact on other payment service providers or other payment infrastructures, and the reputational risk for the service provider. For the four quantitative criteria, clear numerical threshold are defined. For the criteria *transactions affected* and *payment service users affected*, two threshold options are retained for two different levels. For the *duration* of the incident, a major incident is reached if the incident hinders operations for more than 2 hours. For the three qualitative criteria, no single qualitative element currently seems to clearly dominate the landscape. However, *reputational impact* due to an incident is one of the main concerns in most Member States. A benchmark is reached if the qualitative criterion is triggered.[4]

Payment service providers should classify an incident as major if it fulfils either one or more criteria at the 'Higher impact level' or at least three criteria at the 'Lower impact level'.

In the preferred option, the thresholds provide consistent labelling of those incidents that are to be reported. The two-level approach sets precise quantitative standards while allowing proportionality considerations. Therefore, the approach spans a broad range of payment service providers which differ in size and legal status, but identifies only severe operational and security incidents in order to keep the burden for payment service providers and competent authorities appropriate. It further avoids the use of solely quantitative criteria for which, in general, data are often not available upon occurrence of the incident or can be unreliable.

[4] The criterion *high level of internal escalation* is also separated into two levels.

D. Cost-benefit analysis[5]

The adoption of the Guidelines considering the option outlined above will affect payment service providers and competent authorities. The EBA stock-taking exercise shows that in at least 17 Member States a compulsory incident-reporting system is already in place.

The introduction of Guidelines regulating the management of payment-related incident reporting is expected to introduce transient administrative implementation costs for payment service providers to implement or adjust their reporting system. The precise definition of data elements required for supervisory purposes will force payment service providers to adjust their IT systems/databases to the new reporting requirements. Payment service providers operating in different jurisdictions will benefit from the Guidelines, as the common standards among Union countries will create synergies, which decrease reporting costs among their entities. The use of a standardised template with a clear set of classification rules will enable greater comparability and automation in the management of information, further mitigating the cost of implementing/adapting a reporting system.

It is expected that competent authorities will face increased administrative costs for implementing an appropriate assessment of the reported incident and for implementing a mechanism to share relevant information with other domestic and supranational authorities. However, in 16 Member States a similar assessment and notification system is already in place and in 14 Member States incident data are already systematically evaluated and used for risk monitoring.

The Guidelines will benefit competent authorities, which will have access to reliable, up-to-date and comparable data on operational or security incidents. With a standardised framework, competent authorities can build an appropriate organisational setup to ask for information from the affected actors, analyse and summarise the information, give feedback and contact other stakeholders. The developed standards allow a clear understanding of the nature and extent of the actual problems at stake. As a result the framework helps define the best potentially required actions to address them in a satisfactory manner. A defined process for sharing information with other domestic authorities and the EBA and the ECB ensures a coordinated approach to handling operational and security incidents and enables pooling experience and knowledge. It therefore helps identify good practices in responding to specific types of incident and the decision-making process on the potential actions to be taken in each situation.

The above positive impacts of these Guidelines strengthen the users' trust in the services offered and contribute to the creation of a framework for stable growth and further integration of the payment service market in the Union.

[5] For complementary information, see also European Commission (2013), *Impact assessment accompanying the proposal for PSD2*.

4.2. Feedback on the public consultation

The EBA publicly consulted on the draft proposal contained in this paper. The consultation period lasted for three months and ended on 7 March 2017. Forty-three responses were received, thirty-six of which were published on the EBA website.

This section presents a summary of the key points and other comments that arose from the consultation, the analysis and discussion triggered by these comments, and the actions taken to address them if deemed necessary.

In some cases, several industry respondents made similar comments or the same respondent repeated its comments in response to more than one question. In such cases, the comments and the EBA's analysis of the comments are included in the table below. Changes to the draft Guidelines have been incorporated as a result of the responses received during the public consultation, as described in detail below.

Summary of key issues and the EBA's feedback

As already stated in Section 2.2 'Rationale' above, the EBA has decided to make changes to the draft Guidelines to reflect some of the concerns raised by respondents. In the feedback table that follows, the EBA has summarised the comments received and explains which responses have and have not led to changes, and the reasons for this.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
	Feedback on General remarks			
(1)	General remarks	Many respondents had questions on the way the incident information will be sent and treated by the NCA (formats, security, etc.). They considered that the information (both that provided by the PSPs but also that provided by a third party in the case of delegated reporting) would be sensitive/confidential and expected measures by the NCA to be aligned with this classification. They requested more clarity on what these measures would be, for information both stored and in transit (when sent and when exchanged with other authorities). One respondent pointed out that data sharing with other authorities should apply the same rules of reciprocal confidentiality and privacy. Another one considered that it is not necessary to share the full template among authorities and a third was of the view that the information should not be distributed without approval of the ASPSP (except perhaps in case of events of international significance). One other respondent wondered which information will be shared with the EBA/ECB and subsequently with other competent authorities.	The EBA agrees that incident-related data are, by default, sensitive information for the payment service provider. As is nowadays the case with any other sensitive information that is being reported to NCAs and/or exchanged with other authorities, this will be treated accordingly. Among other things, Article 24 of PSD2 on professional secrecy will apply. Guidelines 6.4 and 8.1 address the confidentiality of the information in transit, but the EBA acknowledges that no reference is made in the Guidelines to the security of the information in storage. Therefore, a clarification has been included. Furthermore, the EBA takes note of the opinion that there is no need to share the full template with other authorities. That is why there is no such requirement as regards other domestic authorities. In the case of the EBA/ECB, though, the EBA considers that, the more information they have, the better they can assess whether or not the incident may be relevant to other competent authorities. This also answers the last doubt put forward: the full report will be shared with the EBA/ECB. The information that will be shared by them with other competent authorities is beyond the scope of these Guidelines. Finally, the suggestion to check with the PSP before sharing the information cannot be taken on board, since this is a requirement already set out in PSD2.	Amendment of Guidelines 6.4 and 8.1 to explain that the competent authority should ensure the security of the information stored and, in particular, treat all information in accordance with the professional secrecy obligations set out in PSD2. *Guideline 6.4: 'Competent authorities should at all times preserve the confidentiality and integrity of the information stored and exchanged […] In particular, competent authorities should treat all information received under these Guidelines in accordance with the professional secrecy obligations set out in PSD2, without prejudice to applicable Union law'.* *Guideline 8.1: 'Competent authorities should at all times preserve the confidentiality and integrity of the information stored and exchanged […] In particular, competent authorities should treat all information received under these Guidelines in accordance with the professional secrecy obligations set out in PSD2, without prejudice to applicable Union law'.*
(2)	General remarks	A very significant number of respondents pointed out that firms already fall under other incident-reporting requirements and in some cases the same incident will need to be reported to different competent authorities such as the Data Protection Regulator, the Financial Services Regulator or the Cyber Security Regulator. Several respondents wondered if the EBA has considered these other requirements and they noted that streamlining this process would help reduce the administrative burden on firms and provide a more harmonious supervisory approach. In particular, there were suggestions to harmonise criteria, templates and notification processes and also to have	PSD2 acknowledges the fact that other incident-reporting obligations exists as a result of other legal acts and establishes that its very own security incident reporting obligations are to be applied without prejudice to the former. Furthermore, the EBA is aware of these multiple reporting stemming from different legal acts, but it is not in a position to address the issue, since its mandate is limited to the scope of PSD2-related notification requirements. With respect to the SSM Cybercrime incident reporting for Significant (Credit) institutions, the EBA recognises the inconvenience of possible multiple reporting requirements, but notes that alignment has been sought as far as possible. However, the EBA was given a specific	None.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		one-stop-shop mechanisms. Moreover, it was not clear to some respondents whether or not this reporting will replace similar reporting obligations prescribed by the competent authority at national level.	mandate by the European Commission and, moreover, the SSM incident reporting is limited to cybercrime. Similarly, the Guidelines cannot clarify whether other, domestic, reporting obligations will remain or not, since this is a decision to be taken within each Member State.	
(3)	General remarks	One respondent considered that operational and security incidents should be treated separately. Another one thought that the focus should be on incidents caused by the PSPs' systems, and not by fraud, while others believed that it is important to include cyberattacks. Finally, there was a suggestion to include an incident list in the Guidelines, but this idea was not further elaborated.	According to PSD2, the Guidelines must address the classification and notification of major operational or security incidents, and the EBA considers that they should be treated together, since the lines between the two types of incidents may be blurred at times. Furthermore, the EBA acknowledges there are different views in the market as regards which incidents are more relevant (operational or security), but the scope of PSD2 covers both (including cyber attacks) and, therefore, the EBA has not made any change in this regard. Finally, the EBA could not take on board the suggestion to have an incident list, since the respondents did not elaborate further on this idea.	None.
(4)	General remarks	Many respondents raised questions about how the EBA and relevant authorities are going to use the incident data collected (e.g. one respondent wondered if they will be used as a basis for the elaboration of future regulations or policies). A few suggested that NCAs should harmonise the actions they may take and there were also a few suggestions to set deadlines for these actions. Many respondents would like to have information of common interest provided to all other PSPs (or at least to those affected) or shared among them (the case of ASPSPs and TPPs is specifically mentioned), and hence used to encourage collaboration amongst firms. One respondent suggested that ENISA and the ECB should develop guidance about this based on best practices. It was also suggested that competent authorities issue warnings, provide feedback and produce high-level statistics to support threat and vulnerability assessments.	Incident-related information can help NCAs understand whether or not payment service providers have established and maintain effective incident management procedures. CAs, together with the EBA and ECB, will also use it to assess the relevance of each given incident for other NCAs. The use of the information by NCAs and, in particular, information sharing between PSPs and from NCAs to PSPs are not in the scope of the mandate. In any case, the Guidelines do not forbid information sharing between PSPs to take place, based on bilateral agreements between these PSPs.	None.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
(5)	Scope of application	One respondent requested more clarity as regards the scope, in particular when incidents happen outside the EU.	The EBA acknowledges that the relevant sentence could be redrafted to provide more clarity and, in particular, more information could be included on what is understood by direct and indirect impact.	Amendment of current paragraph 11 under Scope of application to further clarify the case when an incident happens outside the EU. *Paragraph 11: 'These ~~draft~~ 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 ~~impacts the services provided via a parent or a subsidiary~~ established outside the Union) and affects~~, either directly or indirectly,~~ 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 in some other way as a result of the incident).'*
	Feedback on responses to Question 1			
(6)	General remarks	Multiple organisations pointed out that the EBA should adopt definitions from internationally recognised standards such as ISO, BIS or ENISA to increase clarity and reduce the burden on firms. References to the standards used were also considered useful by a few respondents.	The EBA notes that internationally recognised standards were one of the inputs used for elaborating the definitions to be found in the Guidelines. However, there is not an exact correlation with them because, where necessary, they had to be adapted to better accommodate the terms and concepts used in PSD2, on which the EBA's mandate is based. The EBA therefore considers it best not to make references to those standards. Moreover, by avoiding cross-references to documents whose governance process is outside the remit of the EBA, it is ensured that the Guidelines remain a self-contained document.	None.
(7)	General remarks	When commenting on what was paragraph 11 of the Background and rationale section in the Consultation Paper some respondents noted that it stated that these Guidelines covered incidents affecting payment services, while incidents related to non-payment services would fall under the Network	The EBA notes that the explanations provided in the Background and rationale section of the Consultation Paper may not have been clear enough. However, judging from the understanding of the respondents, it seems that the definitions included in the Guidelines accurately explain the scope, i.e. major operational or security	None.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		and Information Security Directive. Yet, they continued, paragraph 13 of the Consultation Paper and the definition of major operational or security incident suggested that any incidents that affect payment services are also covered. Organisations would appreciate greater clarity on what those supporting tasks are, and generally what types of incident affecting payment services are included.	incidents with an effect on payment services, which includes incidents affecting supporting services and hence disrupting the provision of payment services. All other incidents with no impact whatsoever on payment services would exclusively fall under the Network and Information Security Directive. Since this seemed to be clear enough from the definition of 'major operational or security incident', the EBA is of the view that no amendments are needed.	
(8)	Definition of major operational or security incident	A few respondents considered that operational and security major incidents should be defined separately and there was also a request to split the definition of major operational or security incident in two: one for incidents related to the availability and continuity of services and another one for incidents related to security, integrity and authenticity.	The EBA considers that adding segmentation would introduce unjustified confusion. Furthermore, PSD2 does not make this distinction and, similarly, the Guidelines apply equally to all operational or security incidents, regardless of the type or the dimensions affected. Therefore, the EBA is of the view that there should be only one definition of a major operational or security incident.	None.
(9)	Definition of major operational or security incident	Several respondents considered there is a need to specify further the definition of an incident, to explain whether or not aspects such as external events, scheduled events, testing or cyber attacks are included. Two respondents also wondered if the definition includes incidents that affect client data or the PSP's reputation. Furthermore, two respondents requested clarification regarding whether or not incidents that are bundled together into a campaign (e.g. phishing) or consist of different intermittent interruptions of several systems would be considered a single incident in the Guidelines. Several questions were also received about incidents that have the potential to cause loss or near-miss incidents. In this respect, half of the respondents considered that incidents that have only a potential (not materialised) major impact should not be included (i.e. they requested that the expression 'may have' be excluded from the definition of major incident), since, as there is no time limit, this could include threats and minor security breaches with the potential to cause significant detriment. Finally, a few respondents were of the opinion that the definition should focus only on 'incident' and not on 'major	In view of the doubts put forward by several respondents, the EBA considers that the scope of 'major operational or security incident' should be further clarified by explaining that all external and internal events that have not been planned by the PSP would be included, bearing in mind that these could be malicious (e.g. cyber attack) or accidental (e.g. human error). Testing gone wrong and, thus, affecting the normal provision of payment services would be considered an unplanned event and, hence, an incident. The EBA has therefore amended the definition and introduced an additional clarification in the Scope of application section. As regards incidents that are bundled together, the EBA points out that the definition of 'major operational or security incident' refers to either a single event or a series of linked events. Therefore, the examples provided by the respondents, and any others that could be understood as being 'linked events', should be considered as a single incident and would be included under the Guidelines. The EBA believes that there is no need to introduce further clarifications in this regard. As regards incidents with the potential to cause loss or near-miss incidents, the EBA considers that CAs should be aware of a major operational or security incident as soon as possible, which is in line with the PSD2 requirements. Therefore, the sooner an NCA is made aware of a major or potentially major incident, the better.	Amendment of the definition of 'operational or security incident' to avoid misunderstandings about the notion of what is 'major' and to better explain that it covers only unplanned events, limiting the range of potential incidents to be considered and excluding the reference to 'material'. ~~*Major*~~ *Operational or security incident: 'A singular event or a series of linked events unplanned by the payment service provider which* ~~*have*~~ *has or* ~~*may*~~ *will probably have an* ~~*material*~~ *adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.'* Introduction of an additional clarification under Scope of application to explain that both external and internal events are covered and that these can be either malicious or accidental. *Paragraph 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*

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		incident', while others suggested defining what a 'material impact' is or including the classification methodology (namely what was Guideline 1.5 in the Consultation Paper) in the definition.	Nevertheless, the EBA acknowledges that the chosen drafting (i.e. the expression 'may have') could be too broad and has therefore limited the range of potential incidents to be reported, by slightly amending the drafting of the definition. Furthermore, the EBA has clarified that this assessment does have a time limit. Finally, the EBA understands the rationale behind the idea of limiting the definition to 'incident' and has, therefore, chosen to drop any reference to 'major' in this context. Moreover, the EBA sees benefits in avoiding the use of the word 'material' in the definition. As a result, the word has now been removed. Following the above, the EBA has also rearranged Guideline 1 to focus its content more directly on the process of classifying an operational or security incident. With this purpose, former Guideline 1.5 in the Consultation Paper has now become Guideline 1.1.	*malicious or accidental.'* Reallocation and redrafting of what was Guideline 1.5 in the Consultation Paper (now Guideline 1.1) to focus of the requirements of this section on the classification of a given operational or security incident. *GL 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.'* Amendment of what were Guidelines 1.3 and 1.4 in the Consultation Paper (now Guidelines 1.4 and 1.5) to clarify that PSPs should asses not only if the thresholds have been surpassed, but also if they are likely to be surpassed before the incident is resolved. *GL 1.4: 'Payment service providers should assess an incident by determining, for each individual criterion, whether or not the relevant thresholds in Table 1 are or will probably be reached before the incident is resolved ~~met or surpassed~~.'* *GL 1.5: 'Payment service providers should resort to estimations ~~should~~ if they do not have actual data to support their judgments of whether or not a given threshold is or will probably be reached before the incident is resolved ~~met or surpassed~~ (e.g. this could happen during the initial investigation phase).'*

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				Replacement of 'may [have impact]' with 'will probably [have impact]' and deletion of the references to 'material' throughout the Guidelines.
(10)	Definition of the five dimensions	A few respondents were of the view that there is a need to define more precisely 'authenticity' in the scope of payments; moreover, one respondent considered this term to be included within the concept of 'integrity'. More clarity was also requested by a few respondents as regards 'integrity' (in particular, which data it refers to) and 'confidentiality' (one respondent suggested including the concept of privacy and another one would add a reference to payment-related services). The definitions of 'availability' and 'continuity' were considered very similar and some respondents asked the EBA to clarify why both are used and how they are differentiated. A few suggested replacing 'continuity' with 'recovery' and another one pointed out that the reference to 'acceptable predefined levels' is not precise enough. In addition, one respondent commented that the definition of 'availability' assumes that services are available 24/7, whereas this is not necessarily the case, as some services are subject to certain time restrictions. Moreover, one respondent suggested that, in the case of 'availability', the definition of payment-related services should be restricted to the ones provided by the PSP. Finally, the word 'client' in the definition of 'availability' and throughout the Guidelines was not always clear or was seen as too broad and several respondents asked to have it replaced with 'payment service user'. There was also a request to define 'authorised client'.	The EBA is of the view that the definitions should be kept as close as possible to the international standards they are based on, since this would help ensure a common understanding. In fact, all these terms are widely used by the industry and should be clearly understood without the need to define them. Therefore, the EBA does not consider it appropriate to introduce any modification. Moreover, the EBA does not see the need to include explicit references to the scope of payments or to explain that the concepts have to be understood in that sense (e.g. data would be all data needed to carry out payment services), since that is a constant feature throughout the Guidelines. Likewise, there is no need to clarify further in the definitions that they refer only to the payment services included in Annex I of PSD2, since that is already the scope of the Directive. Nevertheless, the EBA acknowledges that the similarities between the definitions of 'availability' and 'continuity' could indeed lead to confusion and, considering that the definition of 'continuity' does not actually come from any international standard, it would merit further clarification. The EBA notes that the main difference is in the point of view: availability refers to the user's perception (i.e. whether or not the service is available, as far as the user is concerned) and continuity refers to whether or not the PSP is actually able to receive and process a payment order. It could therefore happen that both availability and continuity are affected, or only continuity may be affected. Therefore, the EBA considers that both concepts should remain and there is no need for alternative terms, but the EBA has slightly changed the definition of 'continuity' to make the difference between them clearer. Furthermore, the EBA recognises that the expression 'upon demand' in the definition of 'availability' may be confusing and has struck it out. No change, however, has been made to the concept 'acceptable predefined levels', since this generalisation is needed to cater for all types of PSPs and of payment-related tasks.	Amendment of the definition of 'continuity' to make clearer the difference from the term 'availability'. *Continuity: 'The property of an organisation's processes, tasks and assets needed for the ~~being capable of~~ delivering ~~its~~ of payment-related services being fully accessible and running at acceptable predefined levels ~~after disruptive incidents occur~~.'* Amendment of the definition of 'availability' to avoid giving the impression that services should be available 24/7 and to replace 'authorised client' with 'payment service user'. *Availability: 'The property of payment-related services being accessible and usable ~~upon demand by authorised clients~~ payment service users.'* Replacing 'client' with 'payment service user' throughout the Guidelines.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			Finally, the EBA sees that there could be benefits in referring to 'payment service user' (in the sense of PSD2) instead of 'client' to ensure consistency with PSD2 and avoid misunderstandings. As regards the term 'authorised', the EBA recognises that it is redundant, since an unauthorised user should not be able to access the payment service; therefore, the word has been removed.	
(11)	Paragraph 14 – Definition of payment-related services	There were two suggestions to clarify whether or not 'payment-related services' are those of Annex I of PSD2. Two other respondents wondered if they include ATM services or payment-related complaints and their processing.	The EBA believes that the definition itself clarifies that 'payment-related services' include the payment services in Annex I of PSD2 and all the relevant tasks needed for the provision of those payment services. Furthermore, as stated above, the EBA considers that the reference to PSD2 should be enough and therefore does not see the need to clarify that ATM services are included as long as they relate to the payment services of Annex I of the Directive (e.g. cash withdrawal). Payment-related complaints and their processing, however, would not be included, since this task does not affect the provision of payment services.	None.
(12)	Definition of additional terms	There were also requests to define additional terms, such as event, support tasks, business activity, designated third party, reputation and crisis mode.	The EBA considers that most of the terms that are suggested to be defined are commonly understood concepts that do not merit a definition.	None.
	Feedback on responses to Question 2			
(13)	General remarks	A few general remarks on the criteria and methodology were received from different respondents. The most recurrent one, but still from a limited number of respondents, was that there should be a different set of criteria for TPPs or, at least, for AISPs, although no concrete proposal was put forward.	The EBA notes that the criteria included in the Consultation Paper are generally applicable to TPPs, the only exception being the 'transactions affected' criterion, and only as far as AISPs are concerned. Therefore, the EBA is of the opinion that there is not clear evidence of the need for a different set of criteria for TPPs. In addition, the EBA believes that having this differentiation would risk introducing an uneven playing field among the different types of actors and adding complexity to the assessment.	None.
(14)	General remarks	Five respondents considered that a particular condition should be met to classify an incident as major, regardless of whether the criteria are fulfilled or not. This particular condition differed among respondents: three of proposed to consider major only those incidents that have a certain duration or for which there are no impact prevention actions in place; another one focused on the need for it to breach an SLA (at least for incidents that	The EBA considers that the first proposal is covered by the suggested criteria. That is, if the incident is resolved immediately, the impact in terms of clients (now payment service users) and transactions affected is likely to be low, and so will the service downtime, reputational impact, level of escalation, etc. As for the breaching of SLAs and the condition that it has a material damage on PSPs or payment service users, the EBA understands that	None.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		are related to availability and continuity); and the other two respondents considered that for an incident to be major it has to cause material damage on the PSPs or its clients. In a similar line, two respondents were of the opinion that the focus should be on whether or not the incident can cause damage to users and if this damage could be avoided by reporting the incident.	affecting a large number of users, for instance, does not necessarily mean that all of them are actually suffering material consequences. Nevertheless, the assessment of whether or not there is a material damage seems too subjective, not only as far as the PSP is concerned, but especially as regards the user, and hence difficult to measure, so the EBA does not see the introduction of this additional requirement as appropriate.	
(15)	General remarks	Another respondent was in favour of adding a second layer of assessment, which would be carried out by senior management, after it has been checked whether or not the criteria are fulfilled, to ensure that only the relevant ones are reported. Aiming at a similar result, another respondent argued for the possibility to allow an incident that has met a Level 2 threshold to nevertheless not be considered as an incident under the scope of PSD2 if the PSP does not internally classify the incident as major. A suggestion to follow a principle-based approach instead of a finite set of criteria was also received and the EBA understands that this proposal could be along the same lines, but it was not further explained by the respondent.	The EBA would like to point out that the main purpose of the Guidelines is to harmonise the classification and reporting of major incidents for all PSPs. Allowing an individual PSP not to report a major incident because it does not consider it to be major based on its own internal classification methodology would render the Guidelines ineffective and redundant.	None.
(16)	General remarks	Other marginal remarks on the criteria were that they seem to be more related to operational than to security incidents and that they should make reference to the five dimensions included in the definition. In this regard, a few respondents considered that there should be two sets of criteria: one for availability and continuity issues and another one for integrity, confidentiality and authenticity matters.	The EBA acknowledges that the criteria may be too general, but considers that introducing security-specific criteria would add too much complexity to the assessment process. Making reference to the five dimensions would also complicate the definition of the criteria without adding obvious value, since any of the five dimensions could potentially be affected. Finally, the EBA considers that having a single set of criteria instead of two is consistent with the EBA's decision to have only one definition of 'incident'.	None.
(17)	General remarks	There was a suggestion to run a pilot scheme to test the appropriateness of the proposal.	The EBA, while considering this proposal useful, notes that it is not intended for this process. Nevertheless, Question 3 tries to cover this and, moreover, a review period is foreseen, at least, every 2 years.	None.
(18)	General remarks	When commenting on what was the Background and rationale section in the Consultation Paper, two respondents suggested that part of its information should be included in the Guidelines (e.g. paragraph 20 or the diagram). Another one suggested also including Diagram 1 in the Guidelines and moving the text in what was Guideline 1.5 of the Consultation Paper to what was	The EBA considers that the methodology is explained clearly enough in the Guidelines and sees no need to include additional explanations from the Background and rationale section of the Consultation Paper. Diagrams, in particular, are not intended o be part of a guideline and, therefore, should not be included. Finally, the EBA sees no problem in moving the text of what was	None.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		Guideline 1.3.	Guideline 1.5 in the Consultation Paper to what was Guideline 1.3, but, considering that the current drafting follows a concrete logic (i.e. chronological order) and that this proposal came from only one respondent, the EBA has considered it best to leave it unchanged.	
(19)	General remarks	Three respondents requested a more detailed explanation of the rationale of the chosen methodology.	The EBA notes that the rationale for the methodology is explained in paragraph 20 of the Background and rationale section of the Consultation Paper. Elaborating on this, the EBA has set the number of criteria that need to be fulfilled at Level 1 (now Lower impact level) at no fewer than three, to avoid an incident being categorised as major only on the basis of qualitative criteria (which are by definition more difficult to assess in a fully consistent way) yet still to provide the necessary flexibility and proportionality to the assessment process. Moreover, it was set at three, not higher, because the EBA considered that the fulfilment of any combination of three criteria was already a good indicator that the incident was major. The EBA hopes that this explanation answers the respondents' concerns and considers that no amendments are needed in the Guidelines.	None.
(20)	General remarks	One respondent considered that the text on page 8 of the Consultation Paper was not aligned with what was Guideline 1.1.a.	The EBA acknowledges the possible misunderstanding, but confirms the accuracy of what was Guideline 1.1.a in the Consultation Paper (now Guideline 1.2.i), so no amendments are needed.	None.
(21)	Guideline 1.2	When commenting on what was Guideline 1.1 of the Consultation Paper (now Guideline 1.2), some respondents suggested removing certain classification criteria. The qualitative criteria were the most often questioned ('reputational impact', 'high level of internal escalation' and 'other PSPs or relevant infrastructures potentially affected'). The motivation of most respondents to request removing them was that they were seen too subjective and burdensome and too difficult to measure with the definitions provided in the Guidelines, in particular at the beginning of the incident in the case of 'reputational impact' and 'other PSPs or relevant infrastructures potentially affected'. That is also why some respondents suggested considering them only on a best effort basis (this suggestion was also received for the quantitative criteria but from only a very limited number of respondents), and many requested that, if kept, they be more concretely	The EBA points out that qualitative criteria are widely used in current reporting frameworks at local level, and the EBA is not aware of this approach having been questioned so far. Furthermore, the EBA acknowledges their subjectivity, but this is precisely why they were chosen, since they should help provide a more accurate assessment of the incident on the basis of the PSP's past experience. Considering these criteria only on a best effort basis could not be an option, since this approach would risk introducing an uneven playing field. In any case, from the feedback received, it seems that the concerns could be addressed by enhancing the framework with more precise explanations of how to measure them, thus making them easier to assess and ensuring to a greater extent a consistent interpretation by all PSPs. In any case, an educated guess would still be possible when carrying out the assessment, as stated in Guideline 1.5.	Amendment of Guideline 1.3 to provide further explanations of how to assess the qualitative criteria (see below).

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		defined (see below).		
(22)	Guideline 1.2	When commenting on what was Guideline 1.1 in the Consultation Paper, one respondent considered that 'reputational impact' is not a consistent criterion, since it is not uncommon for minor incidents to receive wide media coverage, while major incidents may not be covered at all.	The EBA acknowledges that the 'reputational impact' criterion may not always provide an accurate measurement of the materiality of the incident, but that is why this is not a stand-alone criterion, but requires other criteria to be met as well.	None.
(23)	Guideline 1.2	When commenting on what was Guideline 1.1 in the Consultation Paper, in the case of 'other PSPs or relevant infrastructures potentially affected', one respondent mentioned that PSPs do not have enough visibility to assess whether or not it is fulfilled.	The EBA realises PSPs may not have full visibility, and they are expected not to examine the market thoroughly, but to make use of the information available regarding the source and the consequences of the incident and conclude whether or not it is likely that other PSPs or infrastructures are affected. In conclusion, and as stated above and in Guideline 1.5, educated guesses are valid.	None.
(24)	Guideline 1.2	When commenting on what was Guideline 1.1 in the Consultation Paper, regarding 'high level of internal escalation', one respondent pointed out that this criterion would be very easily fulfilled for small PSPs. There were also other marginal views, with two respondents considering that it could have a negative impact on the PSPs internal communication process, and another one pointing out that it is a consequence of the incident being major, and not the other way around. Two additional respondents considered this criterion redundant and another one was of the view that it does not capture the dimensions that are aimed at according to what was paragraph 17e of the Background and rationale section in the Consultation Paper.	The EBA acknowledges that this criterion would be easily fulfilled by small PSPs, but only at Level 1 (now Lower impact level), which means that two other criteria would still need to be reached for the incident to be classified as major. Furthermore, the EBA considers it unlikely that this criterion would prompt PSPs to change their internal procedures in order to avoid reporting. The EBA also realises that this criterion is the consequence of the incident being major from the PSP's point of view and, therefore, it would not be useful for internal classification purposes, but it would be so for reporting purposes. Although the potential redundancy is acknowledged, the EBA considers it best to risk having this redundancy in exchange for making sure that relevant incidents are not left unreported. Finally, no clarity was provided by the respondent on which dimensions of what was paragraph 17e in the Consultation Paper would not be captured by this criterion, and the EBA is still of the view that they would, so sees no reason to introduce any changes.	None.
(25)	Guideline 1.3	When commenting on what was Guideline 1.2 in the Consultation Paper, among the quantitative criteria, the 'economic impact' was questioned by almost 15% of the respondents, who considered it to be very difficult to estimate, especially at the beginning of the incident and, in particular, as regards the indirect costs. One respondent also considered that having 'clients affected' and 'transactions affected' would make	As regards the 'economic impact' criterion, the EBA considers that, although questioned, it should remain for a number of reasons. Firstly, it is consistent with the SSM's approach. Moreover, it provides an additional dimension of the relevance of the incident and the actual damage to the PSP, beyond clients (now payment service users) and transactions affected, since the cost of fixing the incident goes beyond the potential losses stemming from the	Amendment of Guideline 1.3 to explain that the focus should initially be on direct costs, and indirect costs should be considered gradually as the information becomes available (see below).

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		this other criterion redundant. Only one respondent suggested removing 'transactions affected' and 'service downtime', and 'clients affected' was not seen as a problem by anyone, although one respondent mentioned that this criterion, together with 'transactions affected', was too difficult to estimate.	number (and value) of transactions and users affected. Nevertheless, given the feedback received, the EBA considers that PSPs could initially focus their assessment on direct costs and consider only those indirect costs that are already known or very likely to materialise. The other quantitative criteria received very limited criticism and, therefore, the EBA considers they should be kept as they are.	
(26)	Guideline 1.2	When commenting on what was Guideline 1.1 in the Consultation Paper, new criteria were also suggested by one respondent, namely 'denial of staff to the PSPs premises', 'key business processes affected' and 'amount of data affected'.	The EBA considers that these potential new criteria are already reflected in those proposed in the Consultation Paper. In particular, if 'denial of staff' and 'key business processes affected' were fulfilled, there would probably be service downtime and clients (now payment service users) and transactions would be affected. Furthermore, the 'amount of data affected' would in the end be translated into, at least, 'payment service users affected' and, most likely, 'reputational impact'. In the light of this, and with the aim of simplifying the methodology as much as possible, the EBA is of the view that these additional criteria are not needed.	None.
(27)	Guideline 1.2.i & Guideline 1.3.i	When commenting on what was Guideline 1.2.a in the Consultation Paper, a few respondents requested more clarity as regards what is meant by 'transactions affected' (e.g. does it mean loss of data/loss of service/data corruption/lack of access; does it refer to actual losses or also to returned transactions or where funds were recovered; does it refer to the transactions directly affected by the breach or also those affected by a wider service disruption?) and which payments should be considered (e.g. should cheques be included, and cross-border transactions?). As far as the value of transactions is concerned, one respondent disagreed with using this measurement and another one wondered whether 'value' refers to the financial loss or to the value of the affected payment traffic. Furthermore, some respondents requested more clarity on how to calculate the percentage over the regular level of transactions, specifically on what to consider in the denominator – i.e. all transactions or only the same type of transaction (a majority favoured the latter); in the same Member State or globally? – and on what is meant by 'regular level of transactions' and whether it refers to volumes or values. As regards the latter, one respondent suggested using as a	The EBA notes that the use of the term 'affected' precisely aims to be general enough to cover all possible scenarios (loss of data, loss of service, etc.). Nevertheless, the EBA has clarified that all transactions affected directly or indirectly by the incident should be considered, regardless of whether the losses are recovered or not. This latter remark should also help clarify that 'value' refers to the value of the affected payment traffic. Furthermore, the scope has also been spelled out more clearly by saying that both domestic and cross-border transactions are included. No reference to the exclusion of cheques has been added, since the EBA is of the view that there is no need to repeat that only those payment services included in Annex I of PSD2 are under the scope of these Guidelines. Furthermore, the criterion based on the value remains, since the EBA considers that it adds value (i.e. the number of transactions affected could be low but their values very high) and this suggestion was received from only one respondent. As regards the way to calculate the percentage of transactions affected, the EBA has clarified in what was Guideline 1.1.a in the Consultation Paper (now Guideline 1.2.i) and in Table 1 that this calculation has to be made in terms of volume (i.e. number of transactions) and has specified in what was Guideline 1.2.a in the	Amendment of Guideline 1.2.i and Table 1 to clarify that the percentages need to be calculated in terms of number of transactions. Amendment of Guidelines 1.2.i and 1.3.i in order to further clarify how the criterion 'transactions affected' should be measured. *Guideline 1.2.i: 'Payment service providers should determine the total value of the transactions affected, as well as ~~and~~ the number of payments compromised as a percentage of the regular level of payment transactions carried out with the affected payment services.'* *Guideline 1.3.i: 'As a general rule, payment service providers should understand as 'transactions affected' all domestic and cross-border transactions that have been or will probably be directly or indirectly affected by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content*

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		reference the daily average transactions in the same day/week of the previous year or in the previous three months to account for seasonality.	Consultation Paper (now Guideline 1.3.i) that both domestic and cross-border transactions should be included in the denominator, but only those carried out using the same payment services as the transactions affected (e.g. if only direct debits are affected, only direct debits should be included in the denominator). Continuing with the denominator, the EBA is of the view that the concept 'regular level of transactions' is spelled out clearly enough in what was Guideline 1.2.a in the Consultation Paper (now Guideline 1.2.i), and so is the possibility of using alternative references, so the EBA has discarded the idea of introducing another metric that, although more accurate, may be more difficult to obtain.	*of the payment message was altered, and those that were fraudulently ordered (whether the funds have been recovered or not). 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 ~~for all the payment services executed by the affected payment service provider~~ carried out with the same payment services that have been affected by the incident, taking the previous year as the reference period for calculations. If payment service providers do not consider this figure to be representative (e.g. because of 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 Annex 1).'* *Table 1: '> 10% of the payment service provider's regular level of transactions (in terms of number of transactions)' and '> 25% of the payment service provider's regular level of transactions (in terms of number of transactions)'.*
(28)	Guideline 1.3.ii	As in the previous criterion, when commenting on what was Guideline 1.2.b in the Consultation Paper, several respondents requested more clarity as regards the term 'clients affected' (i.e. all clients, all clients with access to that service or only those that tried using it – and, if the latter, how it should be calculated – and all clients of the PSP or of the group?). A few others also asked about the scope (i.e. should domestic or also global clients be considered; does it mean number of merchants, or number of TPVs, or number of registered cell phones; etc.?) and whether the assessment should be for all clients taken as a whole or per segment of clients (with a majority favouring the latter). One respondent also wondered which clients should consider a PSP that offers operational services to other PSPs. In addition, almost a quarter of the respondents requested more clarity on how to calculate the percentage over the total number of clients, specifically on what to consider in the	As regards the term 'affected', the EBA has clarified that all clients (now payment service users) with access to the affected service that could have been using it during the lifetime of the incident should be considered affected and that this calculation should be made on the basis of the payment service provider's past experience. Moreover, the EBA acknowledges the existence of different user profiles (e.g. consumer, corporate, etc.) but considers that introducing a fragmentation by type of user would further complicate the assessment and risk facing different interpretations of the different types of user. Nevertheless, to cater for the worries of some respondents (e.g. the absolute thresholds are too low for corporate clients), the thresholds could be reviewed (see Question 4). Finally, the EBA agrees that the way to calculate this criterion in	Amendment of what was Guideline 1.2.b in the Consultation Paper (now Guideline 1.3.ii) to further clarify how the criterion 'payment service users affected' should be measured. *Guideline 1.3.ii: 'Payment service providers should understand as 'payment service users affected' all payment service users (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 probably suffer the consequences of the incident. Payment service providers should resort to estimations based on past activity to determine the number of payment service users that may have*

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		denominator (i.e. all clients, all clients of payment services or just those clients with access to the same type of service; and in the same Member State or globally?). In this regard, a few respondents requested that the methodology for calculating the denominator be amended by taking only active clients into consideration (i.e. excluding passive clients).	relative terms could be clarified further by explaining that the denominator should include both domestic and cross-border users with access to the payment service affected by the incident. The EBA considers, however, that there is no distinction for regulatory reasons between a passive and an active payment service user, and it should be borne in mind that a passive user can become active at any moment. If this happened during an incident, that payment service user would automatically become affected by the incident, as they would not be able to make payments.	*been using the payment service during the lifetime of the incident.* *In the case of groups, payment service providers 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.* *Furthermore, payment service providers should take as the total number of ~~clients~~ payment service users the aggregated figure of domestic and cross-border ~~clients~~ payment service users contractually bound to 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, ~~the type of service they are benefiting from~~ or whether they ~~have been classified as~~ are considered active or passive payment service users.'*
(29)	Guideline 1.3. iii	When commenting on what was Guideline 1.2.c in the Consultation Paper devoted to 'service downtime', a few respondents requested clarification of (i) what 'not being available' means (e.g. whether it refers only to total or also to partial outages and if the existence of alternative channels and/or process centres would mean that the service is available) and (ii) from when the PSP should start counting the service downtime. Furthermore, one respondent considered that the term 'service' should be defined. Suggestions on how to measure the 'service downtime' were also received, with a few respondents considering that planned outages or scheduled system maintenance should be left out of scope and a couple others being of the opinion that only business hours should be considered. Finally, three respondents suggested taking into account the timeframe when the service is down (e.g. near a	The EBA points out that the term 'service downtime' refers not to the payment service as such, but to any service offered to the user in relation to a payment service (e.g. the use of mobile banking for making payments would be a service). Since there seems to be some confusion on this, the EBA considers that it could be further clarified what is to be understood as availability. Thus, the EBA is of the view that a service should not be considered available when its primary use channel is not regardless of whether an alternative access channel may be found. On the contrary, a partial outage could be considered as the service being available. This latter aspect has been clarified by referring to the service being completely down. Furthermore, the EBA acknowledges that more guidance is needed on how to measure the service downtime, so it has been added that it should be counted from the moment it happens or, if unknown, from when it was detected. Furthermore, the EBA clarifies that the reference to maintenance	Amendment of what was Guideline 1.2.c in the Consultation Paper (now Guideline 1.3.iii) to further clarify how the criterion 'service downtime' should be measured. *Guideline 1.3.iii: '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 probably be down and, thus, prevents (i) the initiation and/or execution of a payment service and/or (ii) access to a payment 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*

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		cut-off time).	periods and closing hours was included to be considered only when relevant (e.g. instant payments), so this has been emphasised to avoid misinterpretations. Finally, the EBA considers it undesirable to include an additional dimension to take into account the timeframe when the incident takes place, since it would increase the complexity of the assessment. In any case, the EBA understands that there are other criteria that would reflect the fact that an incident takes place close to an important time window (e.g. clients affected, high level of internal escalation or reputational impact).	*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.'*
(30)	Guideline 1.3.iv	When commenting on what was Guideline 1.2.d in the Consultation Paper, one respondent requested more clarity on what 'expropriated funds' means as regards 'economic impact'. Furthermore, two respondents suggested limiting this criterion to direct costs, since indirect costs are too hard to estimate. There was also a suggestion to consider only those indirect costs that are certain and avoid estimations in this case. One respondent mentioned that inclusion of lost profits/revenues is not consistent with this term.	The EBA notes that this definition is aligned with the SSM's and, therefore, the EBA considers that it should not be changed, to ensure consistency to the greatest extent possible. However, given the feedback received about the difficulty of estimating the indirect costs, the EBA considers that PSPs could focus their assessment on direct costs and consider only those indirect costs that are already known or very likely to materialise. As regards the latter and as stated in Guideline 1.5, the PSP should resort to estimations.	Amendment of what was Guideline 1.2.d in the Consultation Paper (now Guideline 1.3.iv) to simplify the calculation of the economic impact by limiting the 'indirect costs' to those that are already known or very likely to materialise. *Guideline 1.3.iv: '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 with contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, payment service providers should consider only those that are already known or very likely to materialise.'*
(31)	Guideline 1.3.v	When commenting on what was Guideline 1.2.e in the Consultation Paper, several respondents requested more explanations of the criterion 'High level of internal escalation', to avoid different interpretations, and some suggestions were received: considering escalation at least to the Board of Directors, or to the highest level possible or an exceptional high level of escalation. Another respondent proposed considering this criterion fulfilled only if the escalation takes place to get input from the executive officers. If the figure of the CIO were to remain, one respondent considered that it should be clarified whether or not it is mandatory to have one. Furthermore, one respondent suggested specifying that the crisis mode should be	The EBA agrees that this criterion could be explained further, but does not consider it appropriate to include a reference to a higher level of escalation than the executive officers, since this would introduce an uneven playing field between larger and smaller PSPs. Furthermore, the term 'CIO' is aligned with the SSM's terminology and it is considered to be understood by the industry at large. In any case, it is just an example and nothing in the Guidelines requires PSPs to have such a position. The EBA considers that the nuance of escalating in order to receive input would be too restrictive, since the aim of the criterion is to assess whether or not the incident would be considered major for the PSP, regardless of the rest of the criteria, and input is not always sought in these cases. Finally, the	Amendment of what was Guideline 1.2.e in the Consultation Paper (now Guideline 1.3.v) to further clarify how the criterion 'high level of internal escalation' should be assessed. *Guideline 1.3.v: 'Payment service providers should consider whether or not, as a result of its impact on payment-related services, ~~the incident is reported to~~ the Chief Information Officer (or similar position) has been or will probably be informed about the incident outside any periodical notification procedure and on a continuous basis throughout*

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		considered only if it was triggered by the effect of the incident on payment services.	EBA agrees that the crisis mode, and in general the escalation, should be considered only if it was triggered by the impact of the incident on payment-related services, and has therefore clarified this.	*the lifetime of the incident. Furthermore, payment service providers should consider whether or not, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.'*
(32)	Guideline 1.3.vi	When commenting on what was Guideline 1.2.f of the Consultation Paper, a few respondents considered the definition of 'Other PSPs or relevant infrastructures potentially affected' too broad. Clarification was also sought regarding whether or not an incident in an energy supplier or network operator should always be understood as fulfilling this criterion.	The EBA acknowledges that this criterion may be considered too broad if it is not understood to be limited to the impact on financial market infrastructures but is applied to any type of infrastructure. Further clarification has therefore been added. As regards the doubt put forward, the EBA agrees that this would be the case, since an incident in an energy supplier or network operator is highly likely to affect other PSPs that have hired the same services from the affected company and, therefore, the PSP could very reasonably conclude that other PSPs may be affected.	Amendment of what were Guidelines 1.1.f and 1.2.f of the Consultation Paper (now Guidelines 1.2.vi and 1.3.vi) to clarify that only financial market infrastructures and card payment schemes should be considered. *Guideline 1.2.vi: 'Payment service providers should determine the systemic implications that the incident will probably 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 card payment schemes.'* *Guideline 1.3.vi: 'Payment service providers should assess the impact of the incident on the financial market, understood as the financial market infrastructures and/or card payment schemes that support them and the rest of the payment service providers. In particular, payment service providers should assess~~, among other things,~~ whether or not the incident ~~could be~~ has been or will probably be replicated at other payment service providers […] and whether or not the payment service provider ~~stops~~ has stopped or will probably stop fulfilling its obligations in the financial market infrastructures of which it is a member.'*
	Guideline 1.3.vii	When commenting on what was Guideline 1.2.g of the Consultation Paper, many respondents considered that 'reputational impact' is defined too broadly and should be narrowed down to avoid different interpretations. In this sense, one respondent suggested basing it only on publicly available factual information (e.g. if the incident is covered in national media) and another one suggested considering the level of media coverage and the suspected level of regulatory interest.	The EBA has taken note of the different comments and suggestions regarding the difficulty of assessing this criterion and the inconsistencies it may bring. Therefore, the Guidelines have been amended in an attempt to simplify the way it should be measured. Furthermore, the EBA points out that these Guidelines do not aim to determine how PSPs should be organised internally (e.g. to classify incidents by type or to monitor their appearance in social media); nevertheless, given that there seems to be a particular	Amendment of what was Guideline 1.2.g of the Consultation Paper (now Guideline 1.3.vii) to clarify further how the criterion 'reputational impact' should be assessed. *Guideline 1.3.vii: 'Payment service providers should consider the level of visibility that, to the best of their knowledge, the incident has gained or will*

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		Another respondent pointed out that there should be some indication of which types of incident should be recorded in order to know if the same type has occurred in the past. In addition, it was pointed out that it is particularly difficult to assess whether or not the PSP has been put at a competitive disadvantage. Finally, a couple of respondents were concerned that this criterion implies that PSPs should be tracking all media coverage in blogs and social networks, since this would be too burdensome.	concern as regards whether or not it is necessary to track all media, it has been clarified that this assessment should be based on available information (so it does not necessarily imply that the PSP is required to carry out intensive tracking of all social media).	*probably gain ~~by the incident~~ in the marketplace. In particular, payment service providers should consider the likelihood that the incident will cause harm to society as a good indicator of its potential to affect their reputation. ~~At an initial stage, p~~ Payment service providers should take into account whether or not ~~as a result of the incident: i) client account data leaked or was stolen, ii) payment instruments and/or personalised security credentials were compromised, i~~ (i) the incident has affected a visible process and is therefore likely to receive or has already received media coverage, (ii) regulatory obligations ~~were~~ have been or will probably be missed, ~~iv~~(iii) sanctions ~~were~~ have been or will probably be breached or (iv) the same type of incident has occurred before. ~~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 also bear in mind later on other criteria such as the media coverage it has received (considering not only traditional media, such as newspapers, but also blogs, social networks, etc.) or whether the payment service provider has been put in a competitive disadvantage as a result of the incident.~~*
(33)	Guideline 1.4	As regards the methodology, when commenting on what was Guideline 1.3 in the Consultation Paper one respondent considered that more levels should be introduced to identify different degrees of 'major'.	The EBA acknowledges the benefits of introducing more levels and, thus, being able to get a better view of the development of the incident, but does not think that the benefits outweigh the added complexity. Moreover, the EBA is of the opinion that the impact figures provided in the reports should be enough to achieve the desired purpose.	None.
	Guideline 1.4	When commenting on what was Guideline 1.3 in the Consultation Paper some respondents suggested swapping the terms 'Level 1' and 'Level 2', since the term 'Level 1' is generally associated with more severity.	To avoid confusion, the EBA has decided to introduce different names instead of the terms 'Level 1' and 'Level 2'.	Amendment of Table 1 (and any other reference in the Guidelines) to rename 'Level 1' and 'Level 2' as 'Lower impact level' and 'Higher impact level', respectively.
(34)	Guideline 1.4	When commenting on what was Guideline 1.3 in the	The EBA considers this proposal to be out of the scope of the	None.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		Consultation Paper one respondent proposed setting Level 1 thresholds only for 'minor incidents' and the Level 2 thresholds for 'major incidents', and subsequently requiring only for Level 2 incidents a report within a certain time limit while requiring for Level 1 incidents only a final report for data collection purposes only.	Guidelines, since the mandate in Article 96 of PSD2 requires the EBA to establish Guidelines concerning only 'major incidents'. In any case, from the EBA's point of view, incidents fulfilling three of the 'Lower impact level' thresholds should already be considered major.	
(35)	Guidelines 1. 4 and 1.5	Three respondents considered that more clarity is needed on whether the thresholds have to be actually exceeded or the mere possibility of their being exceeded at some point in the future would suffice (what were Guidelines 1.3 and 1.4 in the Consultation Paper). If it is the latter, two other respondents suggested having a second set of (higher) thresholds to be considered when assessing this 'future' impact.	As stated in Question 1, PSPs should assess whether or not the thresholds are met or reasonably expected to be met before the incident is resolved. The EBA acknowledges that more clarity is needed and therefore what was Guideline 1.3 in the Consultation Paper (now Guideline 1.4) has been amended. The suggestion to have a second set of higher criteria has not been taken into account, since the thresholds included in the Consultation Paper are already considered high enough, be they actually or potentially reached.	Amendment of what were Guidelines 1.3 and 1.4 in the Consultation Paper (now Guidelines 1.4 and 1.5) to explain that PSPs should consider both if the thresholds are reached and if it is likely that they will be reached before the incident is resolved (see Question 1).
(36)	Guideline 1.6	When commenting on what was Guideline 1.5 in the Consultation Paper, few respondents questioned why, if the threshold associated with the criterion 'transactions affected' is met, at least two more Level 1 criteria are to be met before the incident qualifies as a major incident. Similarly, one other respondent was of the opinion that the requirement to fulfil three or more criteria at Level 1 introduces more complexity than needed in the incident classification methodology.	The EBA considers that making use of Level 1 (now 'Lower impact level') and Level 2 (now 'Higher impact level') thresholds and providing for the requirement to reach at least three 'Lower impact thresholds' or one 'Higher impact thresholds' introduces proportionality in the incident classification methodology, thus striking an important and necessary balance both between smaller and larger PSPs and between quantitative and qualitative criteria. The EBA, therefore, considers the methodology appropriate for achieving the required goals and no changes have been introduced.	None.
(37)	Guideline 1.6 (previously 1.5)	When commenting on what was Guideline 1.5 in the Consultation Paper, one respondent considered that, for Level 2 criteria, the economic impact criterion should always be fulfilled (an incident is major if one or more Level 2 criteria are met, provided that the 'economic impact' is one of them).	The EBA considers that Level 2 (now 'Higher impact level') thresholds are established at a sufficiently high level to ensure that, when an incident meets any of them, it is a 'major incident'. If, for example, a PSP suffers an incident in which a large proportion of its clients (now payment service users) are affected even though the economic impact is very low, this still constitutes a major incident.	None.
	Feedback on responses to Question 3			
(38)	Guideline 1 1.2, 1.3, 1.4	The majority of respondents considered that the proposed methodology will result in significantly more incidents being considered as major, because of the use of qualitative and PSP-dependent criteria (high level of escalation for smaller PSPs, for instance). Moreover, given the low values of the proposed thresholds (static and/or relative) or the complexity of the	The EBA has taken note of the PSPs' view and has assessed the specific comments received in Questions 2 and 4 to enhance the methodology and hence reduce the potential risk of over-reporting.	See Questions 2 and 4.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		interplay of criteria and thresholds, there is a risk that even minor incidents could be considered major. This is especially true for larger payment service providers.		
	Feedback on responses to Question 4			
(39)	General remarks	Several respondents were not sure what the hyphen means in Table 1.	The EBA clarifies that the hyphen means that no threshold has been set for the corresponding criterion at the corresponding level. In those cases the criterion will therefore come into play only when assessing one of the two impact levels. To avoid misunderstandings, the EBA has replaced the hyphen with the expression 'not applicable'.	Amendment of Table 1 to replace the hyphens with the expression 'not applicable'.
(40)	Guideline 1.4	When commenting on what was Guideline 1.3 in the Consultation Paper, several respondents questioned whether the use of cumulative thresholds in Level 1 and non-cumulative in Level 2 was intentional or not. One other respondent was unsure which thresholds to apply when there are two (relative and absolute) and another one considered that the way Level 2 thresholds should be applied in the case of 'transactions affected' and 'clients affected' is not clear.	The EBA clarifies that the use of 'and' in Level 1 (now 'Lower impact level') thresholds and 'or' in Level 2 (now 'Higher impact level') thresholds as regards certain quantitative thresholds is intentional, as the EBA is of the opinion this introduces proportionality in the incident classification methodology, thus striking an important and necessary balance between smaller and larger PSPs. The EBA further explains that PSPs should assess if any of the two thresholds are met and, depending on whether the table says 'and' or 'or', both thresholds will need to be fulfilled or only one, respectively. The EBA considers this is clear enough, but the words 'and' and 'or' in the table have been highlighted to avoid misunderstandings.	Amendment of Table 1 to have the words 'and' and 'or' bold and in a separate line.
(41)	Guideline 1.4	When commenting on what was Guideline 1.3 in the Consultation Paper, one respondent proposed different thresholds for the quantitative criteria, eliminating the differentiation between Level 1 and Level 2 and including a differentiation in the criterion 'economic impact' between those PSPs that provide only money remittance or third party providers (PISP, AISP) and all other PSPs, which provide other payment services.	The EBA is of the opinion that removing the threshold differentiation between Level 1 (now 'Lower impact level') and Level 2 (now 'Higher impact level') would strike less of a balance between smaller and larger PSPs and would reduce proportionality in the incident classification methodology. It would moreover render it more difficult to strike a balance between the importance of quantitative and qualitative criteria. Furthermore, no rationale is provided for having separate thresholds for certain categories of PSPs on the basis of the type of payment service that these PSPs provide. Such a differentiation would, in the EBA's view, be unwarranted and lead only to increased and unnecessary complexity, resulting in a less level playing field.	None.
(42)	Guidelines 1.	When commenting on what were Guidelines 1.3 and 1.6 in the	The EBA underlines that the RTS on Strong Customer Authentication	None.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
	4, 1.6	Consultation Paper, wo respondents considered that the downtime of the ASPSP's dedicated interface for third party providers (PISP, AISPS) should almost automatically be a major incident for the ASPSP. To further this goal, they proposed reducing the 'transactions affected' threshold to 0.05%.	and Common and Secure Communication establish the requirements demanded of the dedicated interface to be established by an ASPSP. The EBA sees no justification for declaring any downtime of this dedicated interface automatically a major incident at the level of the ASPSP. As explained above, the criteria and thresholds ought not to differentiate between the type(s) of payment services provided or types of PSPs offering them.	
(43)	Guideline 1.4	When commenting on what was Guideline 1.3 in the Consultation Paper, a significant number of respondents proposed either significantly increasing the absolute thresholds associated with quantitative criteria ('transactions affected', 'clients affected', 'economic impact') linked to Level 1 and/or Level 2 thresholds or removing these absolute thresholds altogether. In the view of these respondents, the use of absolute thresholds places a disproportionate burden on larger PSPs and would inevitably lead to over-reporting to the NCAs. Hence, respondents felt that this would result in the Guidelines missing their stated objective of the reporting of 'major' incidents only. Four other respondents were of the same view, but in this case their concern related to the potential impact of the proposed absolute thresholds associated with the quantitative criteria for those PSPs servicing corporate clients (the so-called B2B context). They pointed out that corporate clients tend to transfer much higher volumes of money in a single transaction and argued accordingly either for the removal of absolute thresholds or for significantly increasing them. In this context, one respondent argued for replacing the absolute thresholds associated with the criterion 'transactions affected', currently expressed in euro, with an amount/number of affected transactions. Some other respondents proposed new (higher) absolute thresholds, but failed to provide any rationale for these figures.	The EBA has carefully studied the different arguments brought forward with regard to either significantly increasing or removing these absolute thresholds associated with the quantitative criteria. The EBA is of the opinion that maintaining the absolute thresholds associated with the quantitative criteria is necessary to ensure a level playing field between smaller and larger PSPs. Removing them altogether would be beneficial only to larger PSPs and place a disproportionately heavier burden on smaller PSPs, which cannot be the objective or result of any changes considered. Accordingly, as concerns the Level 1 (now 'Lower impact level') thresholds associated with the quantitative criteria, the EBA is of the opinion that precisely the requirement to meet three criteria's thresholds before an incident can be classified as 'major' provides sufficient safeguards against over-reporting or the disproportionate burdening of larger PSPs. As concerns the Level 2 (now 'Higher impact level') thresholds, the EBA concurs that the absolute threshold associated with the criterion 'transactions affected' might be too low. In particular, the EBA shares the view that PSPs operating in a B2B context are likely to meet the absolute thresholds associated with the quantitative criteria (most importantly the criteria 'transactions affected') more quickly than those PSPs operating in a B2C context. Therefore, the EBA has increased the 'Higher impact level' threshold associated with the criterion 'transactions affected', which partly responds to the industry's concern and hence should avoid over-reporting. The EBA is unconvinced that expressing the absolute threshold in 'number or amount of transactions affected' would add anything to the relative threshold that is already expressed accordingly. The differentiation initially set forth was done on	Amendment of Table 1 to raise the absolute threshold linked to the criterion 'Transactions affected' in the 'Higher impact level' from EUR 1 million to EUR 5 million, which is accordingly aligned with the 'Higher impact level' threshold established with regard to the criterion 'Economic impact'. *Table 1: '> 25% of the payment service provider's regular level of transactions (in terms of number of transactions)* ***or*** *> EUR ~~1,000,000~~ 5 million'.*

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			purpose and with the aim of capturing two parameters related to the criterion 'transactions affected', and the EBA still considers that this differentiation adds value. As regards the 'Higher impact level' thresholds associated with the criteria 'clients affected' (now 'payment service users affected') and 'economic impact', the EBA considers they are at a sufficiently high level to avoid over-reporting and no data warranting a change in these absolute figures were brought forward or could be conceived by the EBA.	
(44)	Guideline 1.4	When commenting on what was Guideline 1.3 in the Consultation Paper, one respondent proposed assigning only a Level 2 threshold to the criterion 'high level of internal escalation' and tying this to the activation of the PSP's Disaster Recovery Plan, as only this would, in the respondent's estimation, be sufficient to trigger a major incident.	The EBA considers that making use of Level 1 (now 'Lower impact level') and Level 2 (now 'Higher impact level') thresholds and providing for the requirement to reach at least three 'Lower impact level' thresholds or one 'Higher impact level' threshold introduces proportionality in the incident classification methodology, thus striking an important and necessary balance both between smaller and larger PSPs and between quantitative and qualitative criteria. The EBA is of the view that removing the 'Lower impact level' threshold associated with this criterion would indicate that a high level of internal escalation could hence exist only when the Disaster Recovery Plan is activated (or likely to be activated). In the EBA's view this is not the case. A distinction must be made between a major incident that does not require the activation of a crisis mode or equivalent (e.g. the activation of the Disaster Recovery Plan) and one that does. Not every major incident will require a crisis mode (or equivalent) to be called upon.	None.
(45)	Guideline 1.4	When commenting on what was Guideline 1.3 in the Consultation Paper, two respondents suggested not including the reference to the triggering of a crisis mode in the Level 2 threshold associated with the criterion 'High level of internal escalation', at least in the initial classification, since they considered that this is not known within 2 hours. Contrariwise, another respondent considered revising the Level 2 threshold to address the potential and likely development of an incident to a crisis mode. To do so, this respondent proposed changing the wording of the threshold to 'Yes, and a crisis mode is likely to be called upon', as the	The EBA acknowledges that the PSP may not know in the first 2 hours whether a crisis mode may be triggered or not, but that does not invalid this threshold; it only means that PSPs will need to make an educated guess. The EBA, in fact, agrees with the view that the PSP will know if a crisis is going to be called upon before this happens and consequently has amended as suggested the Level 2 (now 'Higher impact level') threshold associated with the criterion 'High level of internal escalation'.	Amendment of Table 1 to introduce a nuance in the 'Higher impact level' threshold associated with the criterion 'High level of internal escalation' to reflect the fact that it applies even if the triggering of the crisis mode is likely but has not taken place yet. Table 1: 'Yes, and a crisis mode (or equivalent) ~~was~~ is likely to be called upon'.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		necessity to call a crisis mode should be known in the lifetime of the incident before it is actually done.		
(46)	Guideline 1.4	When commenting on what was Guideline 1.3 in the Consultation Paper, two respondents suggested increasing the Level 1 threshold associated with the criterion 'service downtime' to 4 hours, with one of these proposing also keeping the 2-hour threshold but detailing further that this would apply only within normal business hours as defined by each NCA separately.	The EBA highlights that the 2-hour service downtime threshold is found in many national-level incident classification methodologies. Furthermore, in this methodology it is applicable only in Level 1 (now 'Lower impact level') precisely to ensure that at least two other thresholds associated with other criteria are met to trigger the reporting of a major incident. This establishes a level of proportionality that in the EBA's view does not require the 2-hour threshold to be raised. The EBA is of the opinion that the proposed change in terms of differentiation with regard to business hours would not only lead to undue further complexity but serve to create differentiation at the national level in the incident classification methodology and hence lead to an uneven playing field for PSPs in the European Union.	None.
	Feedback on responses to Question 5			
(47)	Annex 1 – Template	One respondent described the template as too detailed.	The EBA does not agree with this remark, but considers that the requested information is necessary for the NCA to be able to judge the impact for the national and European payment process.	None.
(48)	Annex 1 – Template	For a very large group of respondents it was not clear what should be reported in which phase of the incident. Some were of the opinion that as much of the template as possible should be filled out, which they mentioned was difficult/impossible in the timeframe of 2 hours, given that they also have to manage the incident. Others asked for more clarification. Furthermore, a majority of the respondents found it difficult to understand which fields are mandatory and which are optional, and a few respondent asked why the term 'if applicable' is used for mandatory data.	The EBA recognises that the reporting requirements for every phase of the incident were insufficiently clear and has therefore organised the template in three clear phases (initial, intermediate and final) and, together with the instructions, more clarity has been provided. Moreover, the reference to 'mandatory fields' has been removed, since all fields are in the end mandatory unless it is clearly stated otherwise (e.g. 'if applicable', 'if already known'). In any case, the EBA understands that the detail of the information to be included in the intermediate report may gradually improve from one intermediate report to the next one. Furthermore, the EBA has reviewed the use of the term 'if applicable' and it has been removed where it could led to confusion. In those cases where the term is used, the EBA notes that it simply means that the PSP does not need to fill out that field if it does not apply to its situation (e.g. 'head of group' does not need to be completed if the PSP does not belong to a banking group).	Introduction of clear sections in the template (initial, intermediate and final) and adaptation of Guideline 2 and the instructions accordingly. Furthermore, removal of 'if applicable' from the template in a few instances and clarification in the instructions that all fields are mandatory unless stated otherwise. *GL 2.10: 'Payment service providers should include headline-level information (i.e. section A of the template) in their initial reports …'.* *GL 2.12: 'Payment service providers should ~~brief~~ submit to the competent authority a first ~~in these delta/~~intermediate report~~s about~~ with a more detailed description of the incident and its consequences (section B of the template).*

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				Moreover, payment service providers should produce additional intermediate reports by updating the information already provided in sections A and B of the template~~,~~ at least, when they become aware of new relevant information or significant changes ~~they have become aware of~~ since the previous notification ~~such as,~~ (e.g. whether the incident has escalated or decreased, new causes identified or actions taken to fix the problem). In any case, payment service providers should produce an intermediate report at the request of the competent authority in the home Member State.' *GL 2.20: 'Payment service providers should aim to include in their final reports full information, ~~which comprises~~ 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 the root cause, if already known, and a summary of measures adopted or planned to be adopted to remove the problem and prevent its recurrence in the future.'*
(49)	Annex 1 – Template	Various respondents had specific comments and suggestions on dedicated fields in every section.	The EBA has evaluated and analysed every detailed comment and suggestion on the form or a field in the template and, when considered necessary, the template has been adjusted accordingly.	Various amendments of the template and throughout the Guidelines when needed to ensure consistency.
(50)	Annex 1 – Template	A respondent complained about the use of abbreviations that were not explained anywhere.	The EBA underlines that abbreviations used in the template are explained in the instruction section of the template, in the Guidelines or in PSD2. Nevertheless, the EBA has amended the template to avoid them to the extent possible.	Amendment of the template to avoid abbreviations where possible.
(51)	Annex 1 – Template	One respondent suggested using only three statuses: diagnostic, repair and closure. According to the respondent, these are the ones most commonly used by PSPs.	The EBA has no insight into the different statuses used internally by PSPs, but has streamlined the proposal by taking out those that seemed redundant (i.e. detection and closure). Recovery and restoration have been kept, since the EBA considers that they both describe a situation different from repair (i.e. they each represent one step further into the process of resolving the incident).	Amendment of the template to reduce the number of statuses to four: diagnostics, repair, recovery and restoration.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
(52)	Annex 1 – Template	A few respondents suggested adding a measure of staff impact, as this may affect the ability to maintain services.	The EBA welcomes this suggestion and the template has been modified accordingly.	Amendment of the template to include a field to state if the staff has been affected by the incident.
(53)	Annex 1 – Template	Several respondents provided suggestions as regards the taxonomy used for 'type of attack', under 'Cause of incident'. Some pointed out that there may be a potential overlap between 'infection of internal systems' and 'targeted intrusion' and others provided an array of suggestions: (i) allowing one to mark more than one attack vector, (ii) using a reference to an existing taxonomy, (iii) using the taxonomy of the SSM's cyberincident reporting, (iv) extending the list of attack vectors or (v) using an alternative taxonomy provided by the respondent.	The EBA notes that the two definitions are slightly different: 'infection of internal systems' refers only to the PSP's internal system, not visible to the user, whereas a targeted intrusion can also be spying on the user's session at the user's end. Furthermore, the EBA considers that the flexible approach followed in the Consultation Paper (i.e. a high-level list and the option 'other' for the PSP to specify, if necessary) is the most appropriate one. The taxonomy was aligned with the SSM's cyberincident reporting as much as possible, but differences can still remain, accounting for the fact that the scopes of the two reports are different. Finally, the EBA acknowledges that in this case, as well as in other parts of the template, multiple answers may be possible and has therefore clarified this in the instructions, where relevant.	Amendment of the instructions to clarify that multiple options may be possible in some parts of the template.
(54)	Annex 1 – Template	A respondent suggested including a unique identifying number. The respondent suggested using the unique identifying number system of ISO 20275. Another respondent suggested using a number generated by each PSP.	The EBA recognises that a unique number per incident based on a uniform system is useful for the administration of incidents. However, given the status of ISO 20275 at the time of drafting the Guidelines (i.e. 'under development') it has not been possible to adopt the standard. Furthermore, the EBA does not see it as appropriate to use the number generated by the PSP instead of that provided by the NCA, since this means that the information systems of the NCA would need to be flexible enough to cater for many different types of identifiers. In view of the above, the EBA prefers to leave the identification number (both whether or not to use it and its structure) to the discretion of the competent authority in the home Member State.	None.
(55)	Annex 1 – Template	Respondents suggested including a box in the template to indicate whether figures are estimated or accurate measures.	The EBA sees the benefits in this suggestion, so a tick box has been added in the relevant fields of the template to indicate whether the PSP is providing actual figures or estimations.	Amendment of the template to add a tick box to indicate whether the figures are real or estimated.
(56)	Annex 1 – Template	Respondents suggested including a separate field for 'relevant infrastructures potentially affected', as the respondents believe that these are not comparable to PSPs.	The EBA notes that, for assessing the incident to determine whether it is major or not, the two types of actors (i.e. payment service providers and relevant infrastructures) are considered together, so it makes sense that there is also a common reply in the template.	None.
(57)	Annex 1 –	A few respondents questioned the added value of distinguishing	The EBA understands that it may be difficult to establish this	Amendment of the instructions to explain that

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
	Template	between security and operational incidents and requested that this field be removed from the template.	distinction, but believes it is relevant information for the assessment of the incident by the competent authority. The EBA is, therefore, of the opinion that PSPs should mark the option that, to the best of their knowledge, is the correct one.	PSPs should indicate, to the best of their knowledge, whether it is an operational or a security incident.
(58)	Annex 1 – Template	Respondents suggested replacing 'cash placement and withdrawal from a payment account' under 'payment services affected' with 'fund transfer into & from a payment account', understanding that this other expression describes the actual payment service more accurately.	The EBA notes that the terminology is consistent with Annex 1 of PSD2 (list of payment services) and the change is, therefore, not justified.	None.
(59)	Annex 1 – Template	Respondents proposed including a choice of 'customer service' under functional areas affected, with a sub-listing to address the customer service channels affected (email, chat, etc.).	The EBA points out that 'functional areas affected' refers to the different stages of the payment process. The EBA believes that the proposed suggestion (i.e. customer service channels) is already covered under 'commercial channels affected'.	None.
(60)	Annex 1 – Template	Respondents mentioned that the template needs an additional choice of 'security infrastructure' under 'Systems and components affected' to capture hardware security modules used for authentication and transaction processing.	The EBA understands that this specific case would fall under either 'hardware' or 'application/software'. Otherwise, it would constitute an 'other' and the PSP would be requested to provide further information. The EBA is of the opinion that this approach is very clear and therefore no amendments have been introduced.	None.
(61)	Annex 1 – Template	A few respondents suggested having an option to withdraw a notification when an incident after investigation is not classified as major.	The EBA agrees with this proposal, which was already included in the Consultation Paper. Since it seems it was not very clear, the EBA has made it clearer in the Guidelines and included a tick box in the header of the template.	Amendment of current Guideline 2.21, the template and the instructions in order to make it clearer that the incident reporting may stop when incidents do not qualify as major any longer. *GL 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 ~~has been misclassified and does not, in fact, rank~~ no longer fulfils the criteria to be considered ~~as a~~ major ~~incident~~ and is not expected to fulfil them before the incident is resolved. In this case, payment service providers should send the final report as soon as this circumstance is detected and, in any case, by the estimated date for the next reporting. In this particular situation, instead of filling out section C of the template, payment service providers should tick the box 'incident reclassified as non-major' and explain the reasons justifying*

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				this downgrading.'
	Feedback on responses to Question 6			
(62)	General remarks	Respondents requested that the instructions for filling out the template be included in the Guidelines themselves.	The EBA considers that the instructions are technical and too complex to be placed in the text of the Guidelines. However, even though they are placed in an annex, they have the same legal status as the Guidelines.	None.
(63)	General remarks	Respondents recommended that other ways of communication (e.g. email and telephone) be made available to allow PSPs to clarify any doubts during review/completion of a report template.	The EBA emphasises that the way the reporting will be implemented in practice, including the resolution of doubts, is outside the scope of the Guidelines and is therefore left to the decision of the competent authorities.	None.
(64)	General remarks	A limited number of respondents requested that an information pack be provided with a briefing on incident reporting and illustrative examples.	The EBA notes that in principle it is not foreseen intended to provide examples in the Guidelines, as these could subsequently be mis-interpreted as suggesting that whatever is not listed in the examples is not allowed. Furthermore, the amendments made as a result of the public consultation aim to significantly improve the clarity of the document, so examples may not be as relevant any longer. In any case, the illustrative flow of the incident reporting has been left in the Background and rationale section, since the EBA believes it could contribute to clarify the reporting process.	None.
(65)	General remarks	Respondents requested that the Guidelines clarify whether or not reporting 'other PSPs or relevant infrastructures potentially affected' has the objective of sharing information with other PSPs such as via already existing business arrangements.	The EBA clarifies that this field has the objective of helping the authorities get an idea of the systemic importance of the incident. Any sharing of information with other PSPs is outside the scope of these Guidelines. Nevertheless, the EBA points out that, if the PSP has shared the incident with other PSPs, this should be reported in the final report (section C 3 'Additional information').	None.
(66)	General remarks	It was requested to have the possibility to leave fields empty.	As indicated in Question 5, the EBA notes that all fields are in principle mandatory, unless indicated otherwise (e.g. 'if applicable' or 'if already known'). The EBA understands, however, that the fields in section B of the template will be filled out on an incremental basis in terms of the level of detail. Furthermore, the Guidelines already explain that PSPs can provide estimations should the concrete figures not be available.	None.
(67)	Annex 1 –	Further clarification on the identification data for PSPs was	The EBA considers that the identification data of the PSP are clearly	None.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
	Instructions for filling out the template	requested (e.g. if the unique identification number can be replaced with BIC or other legal identifier, what is the authorisation number, or what the 'head of group' means).	explained in the instructions and does not think that there is room to specify them further.	
(68)	Annex 1 – Instructions for filling out the template	Respondents requested clarification of the description of 'country(ies) affected by the incident' in a case where the IT systems affected are located in another country than the branch or office where the event materialised.	The EBA acknowledges that the explanation of this field could be improved, so that it is clearly understood that in the case put forward by the respondent the country or countries affected would be the one(s) where the PSP provides payment services. The name of the field has also been amended so that there is no doubt that one or more countries may be included.	Amendment of the template to rename the field 'country(ies) affected by the incident' as 'country/countries affected by the incident' and amendment of the instructions in order to clarify that it refers to the country or countries where the impact has materialised.
(69)	Annex 1 – Instructions for filling out the template	One respondent requested clarification of whether 'discovery point time' (under 'Incident Discovery') refers to detection or to classification as major.	The EBA understands that the field the respondent refers to is 'Date and time of detection of the incident', which refers to the point in time when the incident was first identified (i.e. detection, not classification as major). The EBA is of the opinion that the instructions are clear enough in this regard. In any case, the EBA has removed the reference to 'discovery' included in the header of this subsection to avoid confusion.	Amendment of the template to refer to 'detection' instead of 'discovery'. Furthermore, amendment of Guideline 2.10 along the same lines. *Guideline 2.10: 'Payment service providers should include […] the information available immediately after it was ~~discovered~~ detected or reclassified.'*
(70)	Annex 1 – Instructions for filling out the template	Respondents mentioned that very specific details, e.g. 'start of incident', may be difficult for PSPs to report and estimated times should be accepted.	The EBA highlights that 'Date and time of beginning of an incident' should be reported, if known, and, as indicated in Guideline 2.13, estimates can be reported should actual data not be available.	None.
(71)	Annex 1 – Instructions for filling out the template	Respondents considered that the definition of operational incident is very similar to that of operational risk event used by the BIS and requested clarification of the difference between the concepts. Furthermore, one respondent requested that the expression 'acts of God' be changed to 'external event' or 'force majeure'.	The EBA confirms that the definition of operational incident is very similar to that of operational risk from the BIS ('operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk'), but this is intentional, since an incident is actually the materialisation of a risk. In the context of these Guidelines, though, the focus is not only on whether or not the PSP suffers losses, but on the disruption of payment services in general. That is also why reputational impact would be included in this case, to the extent that it could affect those services. Furthermore, the EBA agrees that a more neutral expressions than 'acts of God' could be used and has therefore modified the instructions as regards 'operational incident' accordingly.	Amendment of the instructions on how to fill out the field 'operational incident' to remove the reference to 'acts of God'.
(72)	Annex 1 – Instructions	Respondents requested more clarification of the field 'Did the PSP have to cancel or weaken some controls?'	The EBA acknowledges that there were no instructions given as regards this question and that it may not be completely clear.	Amendment of the instructions in order to clarify the field 'Did the PSP have to cancel or weaken

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
	for filling out the template		Therefore, the EBA has included an explanation in the instructions.	some controls?'
(73)	Annex 1 – Instructions for filling out the template	Respondents wondered if the field 'Was a civil complaint filed against the PSP?' also includes legal actions against the PSP before what the respondent referred to as "'ivilian' goes to court and how the PSP can answer this field.	The EBA realises that it may be too restrictive to limit this question to civil complaints, and has therefore broadened this field to include any legal action taken against the PSP (e.g. withdrawal of authorisation). The reporting PSP should provide all the relevant details, such as the status of the complaint, the courts it has been filed with, etc.	Amendment of the template, and of the instructions accordingly, to broaden the scope of the field 'civil complaints filed against the PSP'.
(74)	Annex 1 – Instructions for filling out the template	Respondents needed more clarity on what information should be provided under 'additional information' concerning possible informal communications with other PSPs.	As mentioned above, the EBA points out that PSPs are expected to state in this field if the incident has been shared, formally or informally, with other PSPs. The EBA considers that the instructions could clarify that both formal and informal interactions are included and has therefore introduced the relevant change. Furthermore, the reporting entity could provide in the free text box details about the PSPs that have been informed (i.e. names of the PSPs and countries where they are located, why the incident has been shared with them, which information has been shared with them, etc.). These examples have been added to the instructions.	Amendment of the instructions in order to clarify that the sharing of information with other PSPs may be done either formally or informally and the type of additional information that the PSP is requested to provide.
	Feedback on responses to Question 7			
(75)	General remarks	One respondent wondered what the consequences are if the template is not fulfilled in time	The EBA highlights that not fulfilling the incident-reporting requirements constitutes a breach of Article 96 of PSD2 and the PSP would have to face the corresponding sanctions. The EBA considers that there is no need to clarify this in the Guidelines.	None.
(76)	General remarks	One respondent asked for clarifications about the scenario where the incident has been identified and resolved within the 2-hour window. In particular, the respondent wondered if the EBA would expect this incident to still be reported and, if so, if it would be reported by the submission of a final report.	The EBA notes that major incidents resolved within the deadline to submit the initial report should also be notified, following the same requirements as any other major operational or security incident. In this particular case, the initial report should include information in section A and, if feasible within the submission deadline, also in section B. Potentially, the initial report could also be the last intermediate report. Furthermore, section C could be filled out as well, and thus constitute the final report, if at that time the root cause analysis has already taken place and full information is available.	Addition of a new Guideline 2.16 to clarify the first situation. *Guideline 2.16: 'Should business be back to normal before 4 hours have passed since the incident was detected, payment service providers should aim to simultaneously submit both the initial and the last intermediate report (i.e. filling out sections A and B of the template) by the 4-hour deadline.'* Addition of a new Guideline 2.19 to clarify the second situation.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				Guideline 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 4-hour window since the incident was detected, they should aim to submit in their initial report the information related to initial, last intermediate and final reports'.
(77)	General remarks	There were a couple of editorial suggestions as regards Guidelines 2.7 to 2.9, namely replacing 'incident' with 'major incident' and modifying 'initial notification' with 'initial report' for consistency.	The EBA deems the requested amendments appropriate, as they improve clarity.	Amendment of Guidelines 2.7 and 2.8 to refer to 'major operational or security incident' instead of to 'incident'. Amendment of Guidelines 2.8 and 2.9 to replace 'initial notification' with 'initial report'.
(78)	General remarks	Four respondents wondered if intermediate and/or final reports are needed when the source lays at an external provider outside of their control (e.g. a telecommunication company).	The EBA has already clarified in the Scope of application section that incidents stemming from external providers are considered 'incidents' in the context of these Guidelines and, therefore, the requirements to which they are subject do not differ from any other incident (i.e. intermediate and final reports are still required). The EBA acknowledges that in these cases PSPs may lack information on how the incident develops, and it may be the case that there is a need for longer deadlines in between reports or that some fields cannot be filled out, but these specificities need to be dealt with bilaterally between the NCA and the affected PSP. In view of the above, the EBA considers that no further clarifications are needed.	None.
(79)	General remarks	One respondent understood that Diagram 2 constitutes a requirement to set up a separate sub-process having exactly the same structure and proposed removing it.	This diagram is not part of the Guidelines so it is not a requirement but a summary of the notification process, which was included with the aim of clarifying how the different requirements relate to each other.	None.
(80)	Guideline 2.2	A few respondents proposed removing the initial report and merely sending the final report when all the information is gathered.	The EBA cannot take this suggestion on board, since it would mean that NCAs were aware of major incidents not as soon as possible but only once they have been resolved, which is not aligned with the PSD2 requirements to report major operational or security incidents without undue delay.	None.
(81)	Guideline 2.8	Most respondents disagreed with the 2-hour deadline. This deadline was considered to be difficult to meet or even counterproductive for incident resolving because of (i)	The EBA considers that the respondents' arguments for increasing the 2-hour deadline seem sensible and well founded. However, some of the deadlines proposed do not seem aligned with the	Amendment of Guideline 2.8 to replace '2 hours' with '4 hours'.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		organisational constraints, (ii) the priority to devote resources during these first hours to the resolution instead of reporting, or (iii) difficulties in gathering enough and appropriate information to assess the incident against criteria, especially in non-business hours. One respondent further pointed out that this last reason could lead to an assessment based rather on previous accumulated experience than on actual data regarding this particular case, and consequently to uneven reporting or over-reporting of incidents that are subsequently reclassified as not major. Finally, another respondent pointed out the mismatch of using a deadline of 2 hours, which is equal to the downtime Level 1 criterion. In view of the above, the vast majority of respondents requested that the timeframe to submit the initial report be increased. There were several proposals for a new deadline, some of which were based on current practices in other contexts (e.g. data protection). These proposals ranged from 3 hours to 72 hours, with 24 hours having most preferences. Two other proposals were received as regards the deadline. One respondent proposed a segmentation of PSPs in such a way that only a subgroup of PSPs (i.e significant banks) would be requested to report within 2 hours from detection. Another respondent proposed a further segmentation of major incidents, requiring an initial report within 2 hours from detection only for those incidents which match Level 2 criteria.	requirement of PSD2 for the PSPs to notify the competent authority without 'undue delay'. The EBA does not agree with introducing different deadlines for different types of PSPs, since PSD2 does not introduce this differentiation. Furthermore, the EBA considers that the 2-hour deadline needs to be equally applied to all major incidents, regardless of whether Level 1 (now 'Lower impact level') or Level 2 (now 'Higher impact level') criteria are fulfilled. As a trade-off between the PSD2 demand and the concerns raised by the respondents, the EBA has decided upon a solution which combines an increase in the deadline for the initial report notification, from 2 to 4 hours, with a simplification of the information to be provided in the initial report (see Question 5).	Guideline 2.8: 'Payment service providers should send the initial ~~notification~~ report to the competent authority within ~~the first 2~~ 4 hours from the moment the incident was first detected…'.
(82)	Guideline 2.8	Some respondents requested that only business hours be counted as regards the deadline for submitting the initial report.	The EBA considers that, if an incident is detected outside business hours and the reporting channels of the competent authority are available, it is reasonable and more aligned with the PSD2 requirements to expect the initial notification as soon as possible, be it business hours or not.	None.
(83)	Guideline 2.8	In addition, some respondents proposed starting to count the timeframe for the 2-hour deadline from the moment the incident is classified as major and not from the moment the incident is detected.	The EBA considers that the 'detection time' is more appropriate and auditable as the moment to start counting the notification deadline than the moment when the incident is classified as major, as the criticality assessment could last an undetermined amount of time from detection.	None.
(84)	Guideline 2.1	Some respondents requested more clarity on the level of detail	The EBA agrees that further clarity was needed and has updated the	Amendments in the template and in Guideline 2

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
	0	required in the initial report. They proposed to provide very basic information in the initial report, not including incident classification figures, and then provide more details in subsequent intermediate reports	template, clearly indicating which information is expected in the initial, intermediate and final reports. Information required for the initial report has been simplified and classification figures are not requested at this stage. See Question 5 for further details.	(see Question 5).
(85)	Guidelines 2. 11-2.15	Intermediate reports were considered by a few respondents to be burdensome or not to provide significant further information with respect to the information already provided in the initial report.	The EBA believes that intermediate reports are very valuable for competent authorities, who need to be aware of the development of the incident. Furthermore, as the Guidelines have been amended to require only very basic information in the initial report, the value of intermediate reports has now increased (e.g. the NCA will not receive preliminary impact and classification estimations until the first intermediate report is submitted).	None.
(86)	Guidelines 2. 11-2.15	Some respondents proposed to increase the timeframe of intermediate reports to 5-8 business days (eight responses) or 2 weeks (one response).	The EBA considers that 3 business days, as required in the Guidelines, is an appropriate period of time for the NCA to be updated on an incident that is considered major. In any case, the Guidelines provide flexibility, since, if the envisaged deadline cannot be met, PSPs are expected to contact the NCA before the deadline has lapsed, provide an explanation of the underlying causes and propose a new plausible deadline (Guideline 2.14).	None.
(87)	Guideline 2.17	Five respondents considered the timeframe of 2 weeks to send the final report from the last intermediate report too short to provide detailed and reliable information on the root cause (four respondents), and specifically the impact (two respondents). Most of them proposed either increasing the timeframe from 2 to 4 weeks or letting the PSP indicate when the final report would be available.	The EBA is of the view that the Guidelines provide enough flexibility to cover situations in which PSPs require more time to send a final report after the 2-week deadline. As stated in Guideline 2.17 (now Guideline 2.18), in such a case, the PSP should contact the NCA before the deadline has lapsed and propose a new deadline.	None.
	Feedback on responses to Question 8			
(88)	General remarks	A small number of respondents suggested that incident reporting is a formal procedure in which the PSP itself should be responsible and accountable for obtaining the right level of information in case of an incident. However, the large majority of respondents agreed with including this provision in the Guidelines, since it was seen as beneficial for small PSPs, outsourced activities and institutions which centralise at group level. Other positive comments referred to cost efficiency, better time management, more accurate and consistent reports, first-hand knowledge of the incident and its lifecycle,	The EBA takes note that the large majority of respondents confirm the rationale for this provision. Furthermore, the EBA would like to highlight that responsibility and accountability do always remain with the PSPs. This is already clarified by the current draft (Guideline 3.1.a). In any case, delegated reporting is an optional procedure that PSPs can resort to if they so wish and provided that the conditions spelled out in Guideline 3 are met. The fact that certain types of PSPs will not be able to fulfil these conditions is not seen as creating	None.

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		and reactivity.	an uneven playing field disadvantaging those that do, since the above conditions have been formulated in a technically neutral and objective manner.	
(89)	Guideline 3.1	One of the respondents that favoured delegated reporting wondered which requirements (e.g. authorisation/supervision) would apply to the third party.	The EBA would like to clarify that financial competent authorities do not regulate third parties to which services are being outsourced. As stated in current Guideline 3.1.b, the requirements to be fulfilled are those on outsourcing set forth by Article 19 of PSD2 for payment institutions, and the general rules on outsourcing of material activities laid down by the CRD and the relevant EBA Guidelines on outsourcing for credit institutions.	None.
(90)	Guideline 3.1	Another respondent stated that conditions allowing TPPs to undertake reporting must be clear and should ensure that the TPP is above a critical size. Furthermore, the respondent pointed out that the TPP's procedures for incident reporting should be regularly reviewed and monitored.	The EBA understands that by 'TPP' the respondent refers to the designated third party and not to PSPs providing payment initiation or aggregation of information services. The EBA considers that the conditions for delegated reporting are clearly spelled out in the Guidelines, and any other specific condition on the third party, as well as the reviewing of the reporting procedures, should come from the PSPs, since the responsibility and accountability for reporting incidents remain with the PSPs.	None.
(91)	Guideline 3.1	As regards the procedure for delegated incident reporting, one respondent indicated that there should be more clarity on what the procedure should be when the delegated entity is located in a different country.	The EBA is of the view that the procedures for giving information about the delegation and for actually reporting incidents should, in principle, be the same, regardless of whether the delegated entity is located in the same country or not. Nevertheless, the competent authority in the home Member State will always determine these procedures, so the Guidelines cannot specify this any further.	None.
(92)	Guideline 3.1.a	Several respondents stated that it should be allowed to rely on a third party provider established outside the Union, since external vendors may be based anywhere in the world and global PSPs may have security incident response teams outside the Union. In this sense, some respondents asked if a non-EU head office could report on behalf of the EU entity.	The EBA considers that the fact that delegated reporting is limited to third parties established in the Union does not prevent PSPs from outsourcing their services to global corporations/external vendors. It will prevent them only from appointing these third parties to perform the corresponding delegated reporting. However, the EBA acknowledges that there may be benefits from allowing that delegated reporting is carried out by a third party established outside the Union, provided that the outsourcing contract ensures the fulfilment of all technical and data protection requirements the NCA may expect. As a result, the EBA has removed former Guideline 3.1.a.	Removal of Guideline 3.1.a in order not to exclude third parties established outside the Union.
(93)	Guidelines 3.	Several respondents addressed the definition of a third party	The EBA has analysed the issue, so the Guidelines now state that, as	Amendment of Guideline 3.1.a. to reflect the

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
	1.b and 3.1.c	against the group dimension. Some of them wondered if intra-group agreements are included in the notion 'third party' and one respondent in particular pointed out that there are cooperative banking groups where the individual local or regional banks delegate the reporting obligation to a central institution owned by them; i.e. they report at group level, since this central institution also performs the payment service support for the local/regional banks. This respondent referred to the definition of group in PSD2 Article 4(40) and further to the provisions of Articles 10(1), 113(6) and 113(7) of the Capital Requirements Regulation, which state that a cooperative group or network is characterised by a system which clearly allocates the liabilities between its members. Following this, the respondent was of the opinion that reporting at group level is not reporting by a third party, but reporting by a member of the group, so the Guidelines should have less extensive rules for groups than for external third party providers (e.g. reporting at group level should be exempted from some of the requirements in Guideline 3.1, such as letter b or c).	an alternative to the existence of a formal contract, an internal arrangement within a group or equivalent scenario would be a workable solution as well.	possibility not to require a formal contract. *Guideline 3.1.a: 'The formal contract underpinning the delegated reporting or, where applicable, existing internal arrangements within a group underpinning the delegated reporting between the payment service provider and the third party […].'*
(94)	Guideline 3.1.d	One respondent requested more clarity on how PSPs can designate a third party to act as their delegated incident notification/reporting service provider to the relevant NCA.	Guideline 3 describes the requirements that a PSP needs to fulfil to delegate incident reporting to a third party. The specific procedures that need to be followed by the PSP for notifying this circumstance to the NCA will be set by the authority, as specified in current Guideline 3.1.c.	None.
(95)	Guideline 3.1.e	One respondent considered that the EBA should introduce security requirements for third parties, similar to those provided to ASPSPs and TPPs, when dealing with clients' confidential information.	The EBA considers that PSPs are responsible for securing the confidentiality of client data regardless of outsourcing or not, and this has to be part of the outsourcing contract between the PSP and the third party. Third parties' securing of confidentiality of client data in incident reports to competent authorities is included as a requirement in current Guideline 3.1.d.	None.
	Guideline 3.3	Two respondents did not agree with Guideline 3.3, i.e. they were of the opinion that having to inform the competent authority in the home Member State before delegating their reporting obligations could be against the freedom of contract and that it should be sufficient to inform the authorities after the signature of the contract.	The EBA considers that, to ensure an appropriate reporting process, it is vital for the competent authority to know in advance who will send the report in case of incidents. As a result, NCAs should be informed in advance about any incident reporting being delegated, as Guideline 3.3 lays down.	None.
	Feedback on responses to Question 9			

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
(96)	Guideline 3.2	Nearly all respondents appreciated the possibility of consolidated reporting and saw clear benefits for all stakeholders (e.g. it is more efficient, especially for smaller PSPs that outsource their IT to service providers and often do not have the full operational information to make the relevant reporting). Only one respondent mentioned not seeing any benefits from consolidated reporting and stated that the responsibility and accountability should remain with the PSPs to provide the right level of information in cases of incidents.	The EBA takes note that the large majority of respondents is in favour of consolidating reporting. Furthermore, the EBA highlights that consolidated reporting is a specific case of delegated reporting and, as stated in Question 8, responsibility and accountability always remain with the PSPs (current Guideline 3.1.a).	None.
(97)	Guideline 3.2	One respondent raised concerns that consolidated reporting may be practically impossible if absolute values for the impacts of the incident have to be calculated. The respondent considered that average values or value ranges should be sufficient instead. In this context one respondent proposed that the NCAs should be allowed to make specific arrangements with the corresponding PSP group and its service providers to find a practical solution for how to handle consolidated reports.	The EBA acknowledges that, for most incidents occurring on the side of the technical service provider, there might be slight differences among all affected PSPs regarding the financial impact of the incident and the number of clients and transactions affected. The EBA further considers that providing the NCA, the EBA and the ECB with the range of the impact (i.e. the highest and lowest values within the set of affected PSPs) may be enough for them to carry out their assessments. Nevertheless, upon request by the NCA, individual information for each PSP should be delivered. The EBA has therefore changed the template to include the possibility that, in the case of consolidated reporting, ranges are provided in the fields 'economic impact – direct costs', 'number of transactions affected' and 'total number of clients affected'. It has also amended Guideline 3.2.e accordingly to provide for this possibility.	Amendment of current Guideline 3.2.e to explain the way ranges should be used in the case of consolidated reporting. *Guideline 3.2.e: 'Ensure that, when there are fields of the template where a common answer is not possible (e.g. section ~~3, 5 and 8~~ B 2, B 4 or C 3), the third party either (i) fills them out individually […] or (ii) uses ranges, in those fields where this is an option, representing the lowest and highest values as observed or estimated for the different payment service providers.* Amendment of the instructions to include the possibility of providing ranges in the fields 'transactions affected', 'payment service users affected', 'service downtime' and 'economic impact'.
(98)	Guideline 3.2	Several respondents questioned if the thresholds for classifying an incident as major should be calculated for each single PSP or on a consolidated basis for all PSPs that would be included in the later consolidated incident-reporting template, respectively for all PSPs within a banking group. One respondent in this context was concerned that it takes too long to calculate figures for every single PSP within the given timeframe of 2 hours.	Thresholds should generally be calculated for each single PSP since the obligations set out in Article 96 of PSD2 are imposed on individual PSPs. For most incidents that may trigger a consolidated reporting, the EBA expects that it will be obvious that corresponding thresholds are reached for all corresponding PSPs which are affected by a common incident. The EBA expects that a detailed analysis and time-consuming assessment for each single PSPs is therefore not necessary in most cases. In cases of doubt, a PSP should be included in the consolidated initial report. If new information is available, the list of PSPs can be modified with the intermediate or final report.	New Guideline 3.2.d to clarify that the assessment has to be carried out on an individual basis. *Guideline 3.2.d: 'Ensure that the third party assesses the materiality of the incident for each affected payment service provider and includes in the consolidated report only those payment service providers for which the incident is 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 that it should not'.*

No	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
(99)	General remark	One respondent proposed expanding the possibility of consolidated reports to payment schemes.	The EBA underlines that payment schemes are outside the scope of these Guidelines and, therefore, this suggestion cannot be taken on board.	None.
(100)	Guideline 3.2. b	Some respondents criticised the limitation of consolidated reporting only to incidents which result from a disruption of technical services.	The wording 'technical services' was not intended to limit the scope of consolidated or delegated reporting. The incidents that may be in the scope of consolidated reporting do usually result from a disruption of technical services. Therefore, in practical terms, this is not a limitation. Any incident that fulfils the relevant criteria under Guideline 1.3 can be reported in a consolidated way.	Remove the word 'technical' from Guideline 3.2 b.
(101)	Guideline 3.2. c	Some respondents criticised the limitation of consolidated reporting only to incidents where all affected entities are located in the same Member State. In this context, one respondent proposed expanding the possibility to banking groups (with subsidiaries in different Member States).	The EBA highlights that, according to PSD2, reports have always to be sent to the national competent authority of the PSP and this requirement needs to be fulfilled at all times, even for consolidated reporting. Including in the consolidated reporting PSPs established in several Member States would increase organisational complexity for NCAs as well as for PSPs: for the PSPs, because the incident report would have to be sent to all NCAs (with different contact points) that are responsible for at least one of the PSPs mentioned in the report; for NCAs, because the relevant information for the Member State in question would have to be extracted from the consolidated report. In view of the above, the EBA considers that Guideline 3.2.c should remain.	None.