cssf

Commission de Surveillance
du Secteur Financier

Circular CSSF 21/787

Application of the EBA Guidelines (EBA/GL/2021/03) on Major Incident Reporting under PSD2

Commission de Surveillance du Secteur Financier

Circular CSSF 21/787

RE: Application of the EBA Guidelines (EBA/GL/2021/03) on Major Incident Reporting under PSD2

Luxembourg, 17 December 2021

To all payment service providers

Ladies and Gentleman,

The purpose of the present circular is to inform you that the CSSF, in its capacity as competent authority, applies the revised guidelines of the European Banking Authority (EBA) on the notification of major operational or security incidents of 10 June 2021 (i.e. EBA/GL/2021/03; hereafter "**the Guidelines**"), in accordance with article 96 of the Directive (EU) 2015/2366 (hereafter "**PSD2**"), replacing as from 1 January 2022 the EBA guidelines EBA/GL/2017/10.

Consequently, the CSSF has integrated the Guidelines into its administrative practice and regulatory approach with a view to promote supervisory convergence in this field at European level.

This circular also provides certain details concerning the reporting obligations, in particular the notification process to the CSSF, related to major operational or security incidents (hereafter "**major incidents**") as provided by Article 105-2(1) of the amended law of 10 November 2009 on payment services (hereafter "**Law**"), which stipulates that payment services providers (hereafter "**PSP**") shall notify the CSSF without undue delay of major incidents.

I. The Guidelines

The Guidelines apply to PSPs as defined in article 1(37) of the Law.

The Guidelines specify, in particular, the criteria for the classification of major incidents by PSPs, as well as the format and procedures the latter should follow to communicate such incidents to the competent authority in the home Member State. The Guidelines apply to all incidents included under the definition of "operational or security incident", according to point 15 of the Guidelines, which covers both external and internal events that could be either malicious or accidental.

Compared to the EBA guidelines EBA/GL/2017/10, the revised Guidelines aim at:

- optimising and, where possible, simplifying the reporting of major incidents under PSD2 and the underlying reporting templates, in order to ease the reporting burden on PSPs and to improve the meaningfulness of the reports received;
- capturing additional security incidents that would not qualify as major under the criteria set in the original guidelines but that experience has shown are material;
- reducing the number of operational incidents that will be reported but that do not have a significant impact on the operations of PSPs.

The **Guidelines** are attached in annex 2 of the present circular, and published on the EBA's website under the following link:

https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

II. Deadlines for classification and notification of major incidents

Please find here below the main deadline requirements:

- PSPs should **classify** the operational or security incident within 24 hours of its detection.
- PSPs should submit an **initial report** to the CSSF within 4 hours from the moment the operational or security incident has been classified as major.

  The CSSF will **acknowledge** to the PSP the receipt of the initial report and communicate to the PSP a **unique reference code**, which the PSP shall indicate in any subsequent reports related to the same incident.
- PSPs should submit the **intermediate report** when regular activities have been recovered and business is back to normal, or in case where regular activities have not yet been recovered, within three working days from the submission of the initial report.
- PSPs should deliver the **final report** to the CSSF a maximum of 20 working days after business is deemed back to normal.

III. Delegation of reporting obligations to a third party

The delegation of reporting obligations of major incidents to a third party is not accepted.

IV. Technical instructions on the notification process to the CSSF

The detailed **technical instructions** for sending the data related to the major incidents to the CSSF are laid down in annex 1 of the present circular.

The PSP shall use for the notification of a major incident to the CSSF the **standard reporting template** as published on the CSSF's website under the following link:

https://www.cssf.lu/en/Document/major-incident-reporting-1/

PSPs should use the same template when submitting the initial, intermediate and final reports related to the same incident, and should therefore complete a single template

in an incremental manner and update, where applicable, the information provided with previous reports.

V. Date of application

This circular, by which the CSSF adopts the Guidelines, **applies with effect on 1 January 2022**.

Circular CSSF 18/704, applying the EBA guidelines "EBA/GL/2017/10" on major incident reporting, is repealed with effect on 1 January 2022, and replaced with the present circular.

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur général

Annex 1: Technical instructions for sending the files

Annex 2: The EBA Guidelines on major incident reporting under PSD2 (EBA/GL/2021/03)

Annex 1: Technical instructions for sending the files

For the transmission of the data to the CSSF, the PSPs have to use the template available on the CSSF website at:

https://www.cssf.lu/en/Document/major-incident-reporting-1/

Delivery instructions

The initial, intermediate and final incident reports must be a duly filled copy of the above template in ".xlsx" format. The Excel file above is pre-formatted and its structure shall not be changed in any way by the PSPs.

Annexes to the initial, intermediate and final incident reports may be in typical "office" application formats (".pdf", ".docx", etc).

All production files must be sent to the CSSF via the file channel system introduced in circular CSSF 08/334. The naming convention to be used is the reporting type "OTH" and the file naming described below must be fully respected to guarantee an automated processing.

The mandatory structure of the file name is in general:

TYRDIR-ENNNN-MAJINCREP-YYYYMMDDHHMM-TYR-AAAA.ext

Examples:

- OTHREP-B0999-MAJINCREP-202201301700-INI-0000.xlsx

  for the initial report generated by the Bank B0999 for the incident detected on 30 January 2022 at 17:00

- OTHREP-B0999-MAJINCREP-201901301700-INI-0001.pdf

  for an annex in PDF format giving additional information to the initial report above

- OTHREP-W0999-MAJINCREP-201901301700-INT-0000.xlsx

  for the intermediate report generated by the electronic money institution W0999 in the version created on January 30th 2019 at 17:00

Remark:

If an **updated version** of the incident template or one of the annexes has to be sent by the PSP to replace an older version of that template or annex, or if an **additional intermediate** report has to be sent by the PSP, then the same annex number (AAAA) as before has to be reused.

Here below are the details of the file naming convention:

Code	Signification	Structure	Values authorised
TYR	Type of reporting	Char(3)	Constant “OTH”
DIR	Direction	Char(3)	“REP” for Report → file to CSSF “FBR” for feedback receipt → file returned, confirming reception by CSSF
-	Separator → DASH	Char(1)	Constant “-” (dash !)
E	Reporting entity	Char(1)	Any type of entity assigned by CSSF, e.g. “B” for Banks, “P” for PFSs, “W” for EMIs (Electronic Money Institutions), “Z” for PIs (Payment Institutions), …
NNNN	CSSF entity ID	Number(4)	0001…9999: the entity ID assigned by CSSF
-	Separator → DASH	Char(1)	Constant “-” (dash !)”
TYPE	TYPE	Char(9)	The only value allowed is the report code “MAJINCREP” which characterizes the Major Incident Reporting
-	Separator → DASH	Char(1)	Constant “-” (dash !)
TIMESTAMP	Creation date & time of the report	Creation date & time of the report	A timestamp representing the **date & time of detection of the incident**, e.g. ‘202201301700’ for the incident detected on 30 January 2022 at 17h00 (this timestamp will serve as a key / identifier of the incident and be reused for all annexes of the report submission)
-	Separator → DASH	Char(1)	Constant “-” (dash !)
TYR	Type of report	Char(3)	“INI” for initial report, “INT” for intermediate report and “FIN” for final report
-	Separator → DASH	Char(1)	Constant “-” (dash !)

AAAA	Annex number	Number(4)	0001…9999 0000 must be used for the main Excel template, 0001 to 9999 may be used for any supplementary annexes
.ext	Extension	Char(5)	For Annex 0000, the only extension value allowed is ".xlsx" For supplementary annexes, "office" extensions are allowed (".pdf", ".docx", etc.)

Annex 2: The EBA Guidelines on major incident reporting under PSD2 (EBA/GL/2021/03)

EBA/GL/2021/03

10 June 2021

Final Report

Revised Guidelines

on major incident reporting under PSD2

Contents

1. Executive Summary

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

Article 96(4) of PSD2 requires the EBA, in close cooperation with the European Central Bank (ECB), to review the Guidelines on a regular basis and in any event at least every two years. To that end, the EBA assessed more than 6000 incident reports it received in 2018 and 2019 and the reporting practices established by PSPs and CAs during that time and decided to review the Guidelines. The objectives of the review were to optimise and simplify the reporting of major incidents under PSD2 and the underlying reporting templates, to capture additional security incidents and to reduce the number of reported operational incidents that are required to be reported but that do not have a significant impact on the operations of PSPs. These, in turn, are expected to decrease the reporting burden for PSPs and at the same time improve the meaningfulness of the incident reports received.

The EBA published a Consultation Paper (CP) with its proposals for a two-month consultation period that ran from 14 October to 14 December 2020. The EBA received 29 responses to the CP raising 82 distinct concerns. The EBA assessed the responses to decide what, if any, changes should be made to the Guidelines. In the light of the comments received, the EBA agreed with some of the proposals and their underlying arguments, and has introduced changes to the Guidelines. The most substantive change related to the new classification criterion, which was changed from 'Breach of security measures' to 'Breach of security of network or information systems'. This change aimed, inter alia, at narrowing down the scope of the criterion, avoiding any overlap with other classification criteria and providing a more tangible criterion that does not require complex assessment and implementation.

The EBA also clarified the process and timeline for classification of major incidents, the meaning of the term duration of an incident and other aspects in the Guidelines, mainly in the instructions on how to fill out the incident reporting template.

Next steps

The Guidelines will be translated into the official EU languages and published on the EBA website. The deadline for CAs to report on whether they comply with the Guidelines will be two months after the publication of the translations. The Guidelines will apply from 1 January 2022.

The EBA acknowledges the ongoing negotiations on the European Commission's proposal for an EU regulatory framework on digital operational resilience (DORA), which contains inter alia a proposal to harmonise and streamline the reporting of ICT-related incidents across the EU finance sector. Depending on the outcome of those negotiations, the EBA Guidelines may eventually be repealed when the DORA Regulation applies, which is currently estimated to be in 2024 or later.

2. Abbreviations

CA	Competent authority
CP	Consultation Paper
EBA	European Banking Authority
ECB	European Central Bank
EU	European Union
DORA	EU legislative proposal for an EU regulatory framework on digital operational resilience
ICT	Information and communications technology
PSD2	Payment Services Directive (EU) 2015/2366
PSP	Payment service provider

3. Background and rationale

3.1 Background

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

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

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

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

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

4. In addition, PSD2 assigned to the EBA and the ECB a central coordination role in relation to other relevant EU and national authorities. The Directive provides that the national CA in the home Member State should, without undue delay, share with the EBA and the ECB relevant details of the incident, that a collective assessment of its significance for these other Union and national authorities is performed and that, where appropriate, the EBA and the ECB notify them accordingly.

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

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

7. In 2020, the EBA therefore decided to review the Guidelines by assessing the incident reports received by then. Following this assessment, the EBA decided to revise the Guidelines and published a Consultation Paper (CP) in October 2020 with proposed amendments to the Guidelines, which aimed at:

   - optimising and, where possible, simplifying the reporting of major incidents under PSD2 and the underlying reporting templates, in order to ease the reporting burden on PSPs and to improve the meaningfulness of the reports received;

   - capturing additional security incidents that would not qualify as major under the criteria set in the original Guidelines but that experience has shown are material;

   - reducing the number of operational incidents that will be reported, in particular those that are currently classified as major but are related to the failure of less significant tasks or single processes and are therefore not that material.

8. The public consultation closed on 14 December 2020, at which point the EBA had received 29 responses raising 82 distinct concerns. The EBA assessed the responses to decide what, if any, changes should be made to the Guidelines. The feedback table in Chapter 5 provides an exhaustive and comprehensive list of all the responses and their respective analysis by the EBA. The Rationale section below, in turn, summarises a key subset of the concerns raised by respondents and changes made to the Guidelines as a result.

9. The revised Guidelines will apply from 1 January 2022.

10. In issuing these Guidelines, the EBA acknowledges that the European Commission published, on 24 September 2020, a proposal for an EU regulatory framework on digital operational resilience (DORA), which contains inter alia a proposal for incident reporting in relation to all financial services provided by all financial institutions in the banking, insurance and investment sector. While the scope therefore extends beyond the incident reporting established under PSD2, which is limited to major incidents impacting payment services provided by PSPs, the EBA takes comfort from the fact that the substance of the proposal is very much aligned with the requirements on incident reporting under PSD2 and the EBA Guidelines.

11. The EBA is therefore looking forward to the DORA negotiations being concluded and to the DORA Regulation applying, which the EBA currently estimates to be some time in 2024/25. The revised Guidelines on major incident reporting under PSD2 issued today will apply until the application date of DORA.

3.2 Rationale

12. The key concerns raised and requests for clarification made by respondents relate to the newly introduced classification criterion, the standardised file for submission of incident reports and the timeline for classification of incidents.

3.2.1 New classification criterion

13. The EBA proposed in the CP to include in the Guidelines an additional classification criterion, 'Breach of security measures', aimed at capturing additional security incidents that would be of interest to CAs. More specifically, the CP proposed that the criterion cover cases where one or more security measures, as referred to in Guideline 3.4.1 of the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04), have been violated, with impacts on the availability/integrity/confidentiality/authenticity of payment services-related data, processes and/or systems of the PSP, its payment service users or a third party to which operational functions have been outsourced.

14. However, a large number of the respondents to the public consultation were of the view that the formulation of the proposed new criterion was too broad. These respondents also sought clarification on how and when PSPs should consider that the criterion can trigger a major incident report. Some of them argued that the criterion does not provide any objective indicators to assess whether the security incident is 'material'.

15. In addition, a few respondents raised the concern that the criterion partly overlaps with already existing criteria, namely 'High level of internal escalation', 'Reputational impact', 'Transactions affected' and 'Payment service users affected'. A few other respondents were of the view that the new criterion is cause-based while all other criteria are impact-based.

16. Finally, some respondents were of the view that the new criterion introduced more complexity into the assessment process and an additional reporting burden for PSPs due to the difficulty in the implementation of the criterion, the need for additional time for classification and reporting, as well as the need for additional resources on the side of PSPs.

17. After assessing these responses, the EBA arrived at the view that the proposal of the new criterion should be reconsidered, since the criterion is indeed rather broad and may cover unintentional operational incidents. This would result in additional incidents to be reported by PSPs that would be of limited use to CAs, which in turn would be contrary to the objective of the revision of the Guidelines.

18. The EBA, therefore, assessed a few options on how to proceed:

    a) retain the currently proposed criterion and introduce further clarifications;

    b) try narrowing down the criterion to intentional 'breach of security measures' only;

    c) focus the criterion on 'breach of security of network or information systems';

d) discard the idea of including a new classification criterion.

19. With regard to option a) above, the EBA considered clarifying that the criterion 'breach of security measures' covers cases where the security measures have been breached due to non-compliance from the PSP and that it does not cover cases where the PSP has complied with its security policies but, for instance, has been a victim of an external attack. In the latter cases, the EBA would have viewed this as a weak policy that needs to be assessed in view of the requirements of the EBA Guidelines on ICT and security risk management. However, the EBA discarded this option for the reasons stated in paragraphs 14-17 above.

20. With regard to option b) above, the EBA arrived at the view that it may be difficult to distinguish between intentional and unintentional breaches of security measures since the motivation is often times not clear from the beginning of the incident and that further investigation is required from that perspective. Therefore, taking into account that the disadvantages of option a) would still apply, the EBA discarded this option.

21. The EBA considered option d) above by also taking into account that some additional security incidents would be covered by the changes introduced in the criteria 'Transactions affected' and 'Payment service users affected '. However, the EBA came to the view that the objective of the review of the Guidelines of capturing the security incidents that may be of interest to CAs would not be achieved fully. For these reasons, the EBA discarded this option as well.

22. Eventually, the EBA decided that option c) above is the most appropriate way to address the concerns raised by the respondents and to meet the objective of capturing additional security incidents that may be of interest to CAs. A detailed description of the criterion has therefore been introduced in Guideline 1.3.

3.2.2 Standardised file for submission of incident reports

23. The EBA proposed in the CP the introduction of a standardised file for submission of incident reports from PSPs to CAs in order to ensure consistent reporting for all PSPs across the EU while facilitating an automated processing and timely assessment of the information received by CAs and subsequently by the EBA and the ECB.

24. While many of the respondents to the public consultation supported the proposed approach, some respondents were of the view that CAs should have the discretion to decide on the most suitable format for communication with their respective national industry and that existing national reporting channels must be maintained since they allow for more efficient submission of incident reports and PSPs in the respective jurisdictions have adapted to these reporting channels. These respondents highlighted further that there will be a short-term but significant adaptation effort, which is likely to be repeated again when DORA applies.

25. Having assessed these concerns, the EBA reassessed the merits of introducing a standardised file for the submission of incident reports between PSPs and CAs and arrived at the view that the disadvantages outweigh the advantages, for the following reasons:

- A change in the established national approaches for reporting major incidents under PSD2 would lead to significant changes to IT systems and processes for PSPs, which are accustomed to national solutions and means for submission of incident reports.

- Changing the established approaches would bring additional cost for CAs to redesign their systems for reporting of major incidents and for PSPs to adapt to these new systems.

- Changing the established approach would introduce an additional administrative burden for PSPs, and possibly also for CAs, and it is likely to require further amendments in several years' time when DORA applies.

- The standardisation of a single file would be difficult to achieve since some incidents need to be submitted in the national languages of the Member State, therefore internationally operating PSPs would not benefit from any significant reduction in their respective reporting burden.

- Some CAs have already developed very sophisticated systems for reporting major incidents at national level, which are also compatible with other incident reporting frameworks.

- Harmonisation of the major incident reporting under PSD2 is already achieved by standardising the template for reporting of these incidents.

26. Nevertheless, while the EBA arrived at the view that the file for submission of incidents from PSPs should not be standardised, the EBA finds merit in standardising the file for submission of incident reports between CAs and the EBA/ECB since it will allow for quicker and more efficient assessment of the incident reports received. To reflect these changes, the EBA amended Guidelines 2.1 and 7.1 accordingly.

3.2.3 Timeline for classification of incidents

27. The EBA proposed in the CP changes in the Guidelines in order to clarify that the four-hour deadline for submission of an incident report from PSPs to CAs applies after the incident has been classified as major against the criteria set in the Guidelines.

28. A few respondents commented on the timeline for classification of the incidents and that additional clarity is needed on the deadline that should apply to the classification of the incidents after they are detected.

29. To address these concerns, the EBA further clarified in Guideline 2.9 that the classification of the incident should take place within 24 hours of its detection, inter alia to avoid situations where PSPs might take an excessively long time to classify the incidents. The EBA also clarified in the same Guideline that, on the rare occasions when the incident cannot be classified within 24 hours, the PSP should justify to the CA why this has been the case.

4. Guidelines

EBA/GL/2021/03

10 June 2021

Revised Guidelines

on major incident reporting under PSD2

1. Compliance and reporting obligations

Status of these Guidelines

1. This document contains Guidelines issued pursuant to Article 16 of the EBA Regulation[1]. In accordance with Article 16(3) of the EBA Regulation, competent authorities and financial institutions must make every effort to comply with the Guidelines.

2. Guidelines set the EBA view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of the EBA Regulation to which Guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where Guidelines are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of the EBA Regulation, competent authorities must notify the EBA as to whether they comply or intend to comply with these Guidelines, or otherwise with reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website with the reference 'EBA/GL/2021/03'. 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 foreseen in Article 96(1) of PSD2, 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 PSD2, 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 PSD2.

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

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

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

Addressees

13. The first set of Guidelines (Section 4) is addressed to payment service providers as defined in Article 4(11) of PSD2 and as referred to in Article 4(1) of Regulation (EU) 1093/2010.

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

Definitions

15. Unless otherwise specified, terms used and defined in PSD2 have the same meaning in the Guidelines. In addition, for the purposes of these Guidelines, the following definitions apply:

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

16. These Guidelines apply from 1 January 2022.

Repeal

17. The following Guidelines are repealed with effect from 1 January 2022:

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

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

Guideline 1: Classification as a major incident

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

a. one or more criteria at the 'higher impact level'; or

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

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

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

i. Transactions affected

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

ii. Payment service users affected

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

iii. Breach of security of network or information systems

Payment service providers should determine whether any malicious action has compromised the security of network or information systems related to the provision of payment services.

iv. Service downtime

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

v. 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).

vi. High level of internal escalation

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

vii. Other payment service providers or relevant infrastructures potentially affected

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

viii. Reputational impact

Payment service providers should determine how the incident can undermine 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 likely be directly or indirectly impacted by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content of the payment message was altered, and those that were fraudulently ordered (have the funds been recovered or not) or where proper execution is prevented or hampered in any other way by the incident.

For operational incidents affecting the ability to initiate and/or process transactions, payment service providers should report only those incidents with a duration longer than one hour. The duration of the incident should be measured from the moment the incident occurs to the moment when regular activities/operations have been recovered to the level of service that was provided prior to the incident.

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

ii. Payment service users affected

Payment service providers should understand as 'payment service users affected' all customers (either domestic or from abroad, consumers or corporates) that have a contract

with the affected payment service provider that grants them access to the affected payment service, and that have suffered or will likely suffer the consequences of the incident. Payment service providers should recur to estimations based on past activity in order to determine the number of payment service users that may have been using the payment service during the lifetime of the incident.

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

For operational incidents affecting the ability to initiate and/or process transactions, payment service providers should report only those incidents that affect payment service users with a duration longer than one hour. The duration of the incident should be measured from the moment the incident occurs to the moment when regular activities/operations have been recovered to the level of service that was provided prior to the incident.

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

iii. Breach of security of network or information systems

Payment service providers should determine whether any malicious action has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) related to the provision of payment services.

iv. Service downtime

Payment service providers should consider the period of time that any task, process or channel related to the provision of payment services is or will likely be down and, thus, prevents i) the initiation and/or execution of a payment service and/or ii) access to a 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.

v. 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 only consider those that are already known or very likely to materialise.

vi. *High level of internal escalation*

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

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

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

viii. *Reputational impact*

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

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

Table 1: Thresholds

Criteria	Lower impact level	Higher impact level
Transactions affected	> 10% of the payment service provider's regular level of transactions (in terms of number of transactions) **and** duration of the incident > 1 hour* **or** > EUR 500,000 **and** duration of the incident > 1 hour*	> 25% of the payment service provider's regular level of transactions (in terms of number of transactions) **or** > EUR 15,000,000
Payment service users affected	> 5,000 **and** duration of the incident > 1 hour* **or** > 10% of the payment service provider's payment service users **and** duration of the incident > 1 hour*	> 50,000 **or** > 25% of the payment service provider's payment service users
Service downtime	> 2 hours	Not applicable
Breach of security of network or information systems	Yes	Not applicable
Economic impact	Not applicable	> Max (0.1% Tier-1 capital**, EUR 200,000) **or** > EUR 5,000,000
High level of internal escalation	Yes	Yes, and a crisis mode (or equivalent) is likely to be triggered
Other payment service providers or relevant infrastructures potentially affected	Yes	Not applicable
Reputational impact	Yes	Not applicable

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

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

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

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

Guideline 2: Notification process

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

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

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

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

2.5. Any additional information contained in the documents provided by payment service providers to the competent authority, either on the initiative of the payment service provider or upon the request of the competent authority in line with Guideline 2.4, should be reflected by the payment service provider in the template under Guideline 2.1.

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

Initial report

2.7. Payment service providers should submit an initial report to the competent authority in the home Member State after an operational or security incident has been classified as major. Competent authorities should acknowledge the receipt of the initial report without undue delay and assign a unique reference code unequivocally identifying the incident. Payment service providers should indicate this reference code when submitting an update either to

the initial report or to the intermediate and final reports related to the same incident, unless the intermediate and final reports are submitted jointly with the initial report.

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

2.9. Payment service providers should classify the incident in accordance with Guidelines 1.1 and 1.4 in a timely manner after the incident has been detected, but no later than 24 hours after the detection of the incident, and without undue delay after the information required for the classification of the incident is available to the payment service provider. If a longer time is needed to classify the incident, payment service providers should explain in the initial report submitted to the competent authority the reasons why.

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

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

Intermediate report

2.12. Payment service providers should submit the 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 business is back to normal when activity/operations are restored with the same level of service/conditions as defined by the payment service provider or laid out externally by a service level agreement (processing times, capacity, security requirements, etc.) and when contingency measures are no longer in place. The intermediate report should contain a more detailed description of the incident and its consequences (section B of the template).

2.13. If regular activities have not yet been recovered, payment service providers should submit an intermediate report to the competent authority within three working days from the submission of the initial report.

2.14. Payment service providers should update the information already provided in sections A and B of the template when they become aware of significant changes since the submission of the previous report (e.g. whether the incident has escalated or decreased, new causes identified or actions taken to fix the problem). This includes the case where the incident has not been resolved within three working days, which would require payment service providers to submit an additional intermediate report. In any case, payment service providers should submit an additional intermediate report at the request of the competent authority in the home Member State.

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

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

Final report

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

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

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

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

2.21. Payment service providers should also send a final report when, as a result of the continuous assessment of the incident, they identify that an already reported incident 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, within the deadline for the submission of the next report. In this particular situation, instead of filling out section C of the template, payment service providers should check the box 'incident reclassified as non-major' and provide an explanation of the reasons justifying this reclassification.

Guideline 3: Delegated and consolidated reporting

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

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

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

d. The confidentiality of sensitive data and the quality, consistency, integrity and reliability of the information to be provided to the competent authority are 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 referring to several payment service providers affected by the same major operational or security incident) should inform the competent authority in the home Member State, provide the contact information included under 'Affected PSP' in the template and ensure the following conditions are satisfied:

a. include this provision in the contract underpinning the delegated reporting;

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

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

d. provide a list of all payment service providers affected by the incident;

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

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

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

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

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

3.5. Payment service providers should materially fulfil 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. Payment service providers

should also ensure that an incident is not reported twice, individually by said payment service provider and once again by the third party.

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

Guideline 4: Operational and security policy

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

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

Guideline 5: Assessment of the relevance of the incident

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

a. The causes of the incident are within the regulatory remit of the other domestic authority (i.e. their field of competence).
b. The consequences of the incident have an impact on the objectives of another domestic authority (e.g. safeguarding of financial stability).
c. The incident affects, or could affect, payment service users 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, so as to identify any possible change that could make relevant an incident that was previously not considered as such.

Guideline 6: Information to be shared

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

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

- Date and time of classification of the incident as major.

- Date and time of detection of the incident.
- Date and time of beginning of the incident.
- Date and time when the incident was restored or is expected to be restored.
- Short description of the incident (including non-sensitive parts of the detailed description).
- Short description of measures taken or planned to be taken to recover from the incident.
- Description of how the incident could affect other payment service providers 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 the relevant domestic authorities. Nevertheless, competent authorities should provide the relevant domestic authorities with the name and address of the reporting payment service provider when said domestic authorities can guarantee that the information will be treated confidentially.

6.4. Competent authorities should at all times preserve the confidentiality and integrity of the information stored and exchanged and their proper authentication towards the 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 for assessing 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 by using a standardised file made available on the website of the EBA.

Guideline 8: Communication

8.1. Competent authorities should at all times preserve the confidentiality and integrity of the information stored and exchanged and their proper authentication towards 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. In order 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 – Reporting template for payment service providers

Initial report

Initial report	within 4 hours after classification of the incident as major					Reset dropdown selections	
Report date (DD/MM/YYYY)				Time (HH:MM)			
Incident reference code							
	A - Initial report						
	A 1 - GENERAL DETAILS						
Type of report							
Type of report							
Affected payment service provider (PSP)							
PSP name							
PSP national identification number							
Head of group, if applicable							
Country / countries affected by the incident	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ GR ☐ HR ☐ HU ☐ IE	☐ IS ☐ IT ☐ LI ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK	
Primary contact person		Email		Telephone			
Secondary contact person		Email		Telephone			
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)							
Name of the reporting entity							
National identification number							
Primary contact person		Email		Telephone			
Secondary contact person		Email		Telephone			
	A 2 - INCIDENT DETECTION and CLASSIFICATION						
Date and time of detection of the incident (DD/MM/YYYY HH:MM)							
Date and time of classification of the incident (DD/MM/YYYY HH:MM)							
The incident was detected by		If 'Other', please specify:					
Type of Incident							
Criteria triggering the major incident report	☐ Transactions affected	☐ Payment service users affected	☐ Service downtime	☐ Breach of security of network or information systems	☐ Economic impact	☐ High level of internal escalation	☐ Other PSPs or relevant infrastructures potentially affected	☐ Reputational impact
A short and general description of the incident							
Impact in other EU Member States, if applicable							
Reporting to other authorities		If 'Yes', please specify:					
Reasons for late submission of the initial report							

Intermediate report

Intermediate report	maximum of 3 working days from the submission of the initial report	Reset dropdown selections
Report date *(DD/MM/YYYY)*		Time *(HH:MM)*
Incident reference code		

B – Intermediate report			
B 1 - GENERAL DETAILS			
More detailed description of the incident:			
What is the specific issue?			
How did the incident start?			
How did it evolve?			
What are the consequences (in particular for payment service			
Was the incident communicated to payment service users?		If 'Yes', please specify:	
Was it related to a previous incident/s?		If 'Yes', please specify:	
Were other service providers/third parties affected or involved?		If 'Yes', please specify:	
Was crisis management started (internal and/or external)?		If 'Yes', please specify:	
Date and time of beginning of the incident (if already identified) *(DD/MM/YYYY HH:MM)*			
Date and time when the incident was restored or is expected to be restored *(DD/MM/YYYY HH:MM)*			
Functional areas affected	☐ Authentication/Authorisation ☐ Communication ☐ Clearing ☐ Direct settlement ☐ Indirect settlement ☐ Other	If 'Other', please specify:	
Changes made to previous reports			
B 2 - INCIDENT CLASSIFICATION / INFORMATION ON THE INCIDENT			
Transactions affected [2]	Impact level Number of transactions affected As a % of regular number of transactions Value of transactions affected in EUR Duration of the incident (only applicable to operational incidents) Comments:		
Payment service users affected [3]	Impact level Number of payment service users affected As a % of total payment service users		
Breach of security of network or information systems		Describe how the network or information systems have been affected	
Service downtime	Total service downtime:	Days: Hours: Minutes:	
Economic impact	Impact level Direct costs in EUR Indirect costs in EUR		
High level of internal escalation		Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe	
Other PSPs or relevant infrastructures potentially affected		Describe how this incident could affect other PSPs and/or infrastructures	
Reputational impact		Describe how the incident could affect the reputation of the PSP (e.g. media coverage, publication of legal actions or infringements of law...)	
B 3 - INCIDENT DESCRIPTION			
Type of Incident			
Cause of incident	☐ Under investigation ☐ Malicious action ☐ Process failure ☐ System failure ☐ Human errors ☐ External events ☐ Other	If 'Other', please specify:	
Was the incident affecting you directly, or indirectly through a service provider?		If 'Indirectly', please provide the service provider's name:	
B 4 - INCIDENT IMPACT			
Overall impact	☐ Integrity ☐ Availability ☐ Confidentiality ☐ Authenticity		
Commercial channels affected	☐ Branches ☐ E-banking ☐ E-commerce ☐ Telephone banking ☐ Mobile banking ☐ ATMs ☐ Point of sale ☐ Other		
	If 'Other', please specify:		
Payment services affected	☐ Cash placement on a payment account ☐ Cash withdrawal from a payment account ☐ Operations required for operating a payment account ☐ Acquiring of payment instruments ☐ Credit transfers ☐ Direct debits ☐ Card payments ☐ Issuing of payment instruments ☐ Money remittance ☐ Payment initiation ☐ Account information services		
B 5 - INCIDENT MITIGATION			
Which actions/measures have been taken so far or are planned to recover from the incident?			
Have the Business Continuity Plan and/or Disaster Recovery Plan been activated?			
If so, when? *(DD/MM/YYYY; HH:MM)*			
If so, please describe			

Final report

Major Incident Report

Please select the type of report: (within 20 working days after the submission of the intermediate report)

Please describe: (applicable for incidents reclassified as non-major)

Reset dropdown selections

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

Incident reference code

C - Final report

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

C 1 – GENERAL DETAILS

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

C 2 – ROOT CAUSE ANALYSIS AND FOLLOW UP

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

C 3 – ADDITIONAL INFORMATON

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

INSTRUCTIONS TO FILL OUT THE TEMPLATE

Payment service providers (PSPs) 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. PSPs should use the same template when submitting the initial, intermediate and final reports related to the same incident. All fields are mandatory, unless it is clearly specified otherwise.

Headline

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

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

Final report: it is the last report the PSP will send on the incident since i) a root cause analysis has already been carried out and estimates can be replaced with real figures or ii) the incident is no longer considered major and needs to be reclassified.

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

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

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

A – Initial report

A 1 – General details

Type of report:

Individual: the report refers to a single PSP.

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

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

Head of group: in the case of groups of entities as defined in Article 4(40) of PSD2, please indicate the name of the head entity.

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

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

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

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

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

Secondary contact person: name and surname of an alternative person that could be contacted by the competent authority to inquiry about an incident when the primary contact person is not available. In the case of a third service provider reporting on behalf of the affected PSP, 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 through which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate telephone number.

Reporting entity: this section should be completed in the case of a third party fulfilling the reporting obligations on behalf of the affected PSP, if applicable.

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

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

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

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

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

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

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

A 2 – Incident detection and classification

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

Date and time of classification of the incident: date and time when the security or operational incident was classified as major.

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

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

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

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

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

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

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

Reasons for late submission of the initial report: please explain the reasons why you required longer than 24 hours to classify the incident.

B – Intermediate report

B 1 – General details

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

Was it related to a previous incident(s)?: please indicate whether or not the incident is related to previous incidents, if this information is available. If the incident has been related to previous incidents, please specify which ones.

Were other service providers/third parties affected or involved?: please indicate whether or not the incident has affected or involved other service providers/third parties, if this information is available. If the incident has affected or involved other service providers/third parties, please list them and provide more information.

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

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

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

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

Authentication/authorisation: procedures which allow the PSP to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials and the payment service user (or a third party acting on behalf of that user) giving their consent in order to transfer funds.

Communication: flow of information for the purpose of identification, authentication, notification and information between account servicing PSPs and payment initiation service providers, account information service providers, payers, payees and other PSPs.

Clearing: a process of transmitting, reconciling and, in some cases, confirming transfer orders prior to settlement, potentially including the netting of orders and the establishment of final positions for settlement.

Direct settlement: the completion of a transaction or of processing with the aim of discharging participants' obligations through the transfer of funds, when this action is carried out by the affected PSP itself.

Indirect settlement: the completion of a transaction or of processing with the aim of discharging participants' obligations through the transfer of funds, when this action is carried out by another PSP on behalf of the affected PSP.

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

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

B 2 – Incident classification / Information on the incident

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

Payment service users affected: PSPs should indicate which thresholds are or will likely be reached by the incident, if any, and the related figures: total number of payment service users that have been impacted and percentage of payment service users affected in relation to the total number of payment service users. PSPs should provide concrete values for these variables, which may be either actual figures or estimates. 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 PSP that grants them access to the affected payment service, and that have suffered or will likely suffer the consequences of the incident. PSPs should recur to estimates based on past activity in order to determine the number of payment service users that may have been using the payment service during

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

Breach of security of network or information systems: PSPs should determine whether any malicious action has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) related to the provision of payment services.

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

Economic impact: PSPs should indicate whether the threshold is or will likely be reached by the incident and the related figures: direct costs and indirect costs. PSPs should provide concrete values for these variables, which may be either actual figures or estimates. 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 only consider those that are already known or very likely to materialise. In the cases where the costs are in non-Euro currencies, when calculating the threshold and reporting the value of the economic impact PSPs should convert the amount of the costs in a non-Euro currency to Euro by using the ECB daily reference exchange rate for the day preceding the submission of the incident report.

> **Direct costs:** costs (Euro) directly caused by the incident, including cost for the correction of the incident (e.g. expropriated funds or assets, replacement costs of hardware and software, fees due to non-compliance with contractual obligations).
>
> **Indirect costs:** costs (Euro) indirectly caused by the incident (e.g. customer redress/compensation costs, potential legal costs).

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

Other PSPs or relevant infrastructures potentially affected: PSPs should assess the impact of the incident on the financial market, understood as the financial market infrastructures and/or payment schemes that support it and the rest of the PSPs. In particular, PSPs should assess whether the incident has been or will likely be replicated at other PSPs, whether it has affected or will likely affect the smooth functioning of financial market infrastructures or whether it has compromised or will likely compromise

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

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

B 3 – Incident description

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

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

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

Malicious action: actions intentionally targeting the PSP. These cover malicious code, information gathering, intrusions, distributed/denial of service attack (D/DoS), deliberate internal actions, deliberate external physical damage, information content security, fraudulent actions and others. For more details, please refer to section C2 of this template.

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

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

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

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

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

Was the incident affecting you directly, or indirectly through a service provider?: please indicate whether or not the incident has targeted directly the PSP or affects it indirectly through a third party, if this information is available. In the case of an indirect impact, please provide the name of the service provider(s).

B 4 – Incident impact

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

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

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

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

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

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

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

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

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

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

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

Point of sale: physical premises of the merchant at which the payment transaction is initiated.

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

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

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

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

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

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

Acquiring of payment instruments: a payment service consisting of 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 PSP or to the payer's own PSP.

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

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

Money remittance: a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another PSP acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.
Payment initiation services: a payment service to initiate a payment order at the request of the payment service user with respect to a payment account held at another PSP.
Account information services: an online payment service to provide consolidated information on one or more payment accounts held by the payment service user with either another PSP or with more than one PSP.

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 are planned to be taken in order to temporarily address the incident.
Have the Business Continuity Plan and/or Disaster Recovery Plan been activated?: please indicate whether this has been the case and, if so, provide the most relevant details of what happened (i.e. when they were activated and what it consisted of).

C – Final report

C 1 – General details

Update of the information from the initial report and the intermediate report(s) (summary): please provide further information on the incident, including the specific changes made to the information provided with the intermediate report. Please also include any other relevant information.
Are all original controls in place?: please indicate whether or not the PSP had to cancel or weaken some controls at any time during the incident. If so, please indicate whether all controls are back in place and, if not, explain in the free text field which controls are not back in place and the additional period required for their restoration.

C 2 – Root cause analysis and follow up

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

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

Malicious code: e.g. a virus, worm, Trojan, spyware.
Information gathering: e.g. scanning, sniffing, social engineering.
Intrusions: e.g. privileged account compromise, unprivileged account compromise, application compromise, bot.
Distributed/Denial of service attack (D/DoS): an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
Deliberate internal actions: e.g. sabotage, theft.
Deliberate external physical damage: e.g. sabotage, physical attack of the premises/data centres.
Information content security: unauthorised access to information, unauthorised modification of information).
Fraudulent actions: unauthorised use of resources, copyright, masquerade, phishing.
Others (please specify): the cause of the incident is none of the above. Further details should be provided in the free text field.

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

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

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

Improper operations: e.g. no exchange of certificates, cache is full.

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

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

Recovery issues: e.g. contingency management, inadequate redundancy.

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

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

Hardware failure: failure of physical technology equipment that runs the processes and/or stores the data needed by PSPs to carry out their payment-related activity (e.g. failure of hard drives, data centres, other infrastructure).

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

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

Software/application failure: failures of programs, operating systems, etc. that support the provision of payment services by the PSP (e.g. malfunctions, unknown functions).

Physical damage: e.g. unintentional damage caused by inadequate conditions, construction work.

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

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

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

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

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

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

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

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

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

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

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

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

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

C 3 – Additional information

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

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

Assessment of the effectiveness of the action taken: please include, where available, a self-assessment of the effectiveness of the actions taken during the duration of the incident, including any lessons learnt from the incident.

5. Accompanying documents

5.1 Draft cost-benefit analysis / impact assessment

Article 96(4) of PSD2 mandates the EBA to review the Guidelines on major incident reporting developed under the mandate in Article 96(3) of PSD2.

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

A. Problem identification

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

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

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

The current criteria triggering a major incident report result in reporting of some operational incidents which have low impact on the institutions and the financial system. At the same time, the reported incidents do not capture some of the relevant security incidents. Furthermore, the current reporting process results in part of the information reported not being useful for supervisory purposes, which leads to an unnecessary reporting and monitoring burden for PSPs and CAs respectively. Lastly, the current reporting template collects information which can be improved for an effective classification of major incidents. To address these issues, after carrying out a public consultation, the EBA revised the Guidelines on major incident reporting as outlined in this final report.

B. Policy objectives

In general, the outlined revisions to the Guidelines contribute to the EBA's objective of fostering regulatory and supervisory convergence and the development of a single market for payment services in the Union. It further contributes to the EBA's objective to create efficient, secure and easy retail payments.[3]

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

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

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

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

C. Options considered

Criteria triggering a major incident report and their thresholds

The revised Guidelines addressed to PSPs respond to the need to optimise the classification of major incidents under PSD2. With regard to the individual criteria and thresholds used, the EBA was of the view that amendments in the criteria and some thresholds may be beneficial in order to (i) avoid capturing operational incidents without a significant impact and thereby reduce CAs' and PSPs' administrative burden and (ii) capture additional security incidents.

Under the original Guidelines, a major incident needed to be reported when the incident affected payment transactions of an amount higher than EUR 5 million. This would trigger the criterion 'transaction affected' on the 'higher impact' level. The EBA assessment shows that this threshold is

[3] EBA Annual Report 2019; EBA 2020 work programme.

too low and results in the reporting of insignificant operational incidents. Thus, the following options were considered to increase the threshold:

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

In addition, the EBA assessment showed an disproportionately large number of operational incidents reported under the 'lower impact' threshold for the same criterion and the 'lower impact' threshold for the criterion 'payment service users affected'. Furthermore, these thresholds did not allow relevant security incidents to be captured. The EBA therefore introduced in the final report an amendment to the assessment of the lower impact thresholds for the 'transactions affected' and 'payment service users affected' criteria and considered the following options:

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

The EBA is also of the view that in order to capture to a greater extent relevant security incidents that would be of interest to CAs, a new, targeted criterion could be included in the Guidelines. After assessing the responses to the public consultation where the inclusion of a criterion 'breach of security measures' was proposed, the EBA considered four options:

> **Option 3.1:** add to the Guidelines the criterion 'breach of security measures' with a 'lower impact' level only.
>
> **Option 3.2:** add to the Guidelines the criterion intentional 'breach of security measures' with a 'lower impact' level only.
>
> **Option 3.3:** add to the Guidelines the criterion 'breach of security of network or information systems' with a 'lower impact' level only.
>
> **Option 3.4:** keep the original criteria for determining whether an operational or security incident is major and do not include a specific criterion for capturing additional relevant security incidents.

Causes of major incidents

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

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

Option 4.1: change the reporting template by amending the causes of incidents 'process failure', 'human error', 'system failure' and 'external events' as introduced in the original Guidelines in the following way:

- **Processes failure:** deficient monitoring and control, communication issues, improper operations, inadequate change management, inadequacy of internal procedures and documentation, and recovery issues;
- **Human error:** unintended errors, inaction and insufficient resources;
- **System failure:** hardware failure, network failure, database issues, software/application failure and physical damage;
- **External events:** failure of a supplier/technical service provider and force majeure.

Option 4.2: change the reporting template by amending the causes of incidents 'process failure', 'human error', 'system failure' and 'external events' as introduced in the original Guidelines in the following way:

- **Operational cause – procedural dimension:** deficient change management, deficient capacity planning, deficient vulnerability management, deficient monitoring, in breach of internal procedures, lack of internal procedures and human error;
- **Operational cause – technical dimension:** application failure, database failure, software failure, network/infrastructure failure, hardware failure and data centre/physical damage.

Option 4.3: change the reporting template by amending the causes of incidents 'process failure', 'human error', 'system failure' and 'external events' as introduced in the original Guidelines in the following way:

- **Processes failure:** deficient monitoring and control, communication issues, operations, change management, inadequacy of documentation, and recovery;
- **Human error:** unintended errors, insufficient resources, lack of information knowledge and abuse behaviour;
- **System failure:** hardware failure, custom and off-the-shell software failure, and inadequate or unavailable premises;
- **External events:** malevolence, failure of service providers and force majeure.

Finally, the EBA came to the view that the information collected under the causes of incidents 'internal attacks' and 'external attacks' can be further improved by adding additional granularity and aligning the terminology to other incident reporting frameworks. Therefore, the EBA introduced a new cause of incident – 'malicious actions', which contains the following subcategories of causes: malicious code, information gathering, intrusions, distributed/denial of service attack, deliberate internal actions, deliberate external physical damage, information content security and fraudulent actions.

Notification process

The revised Guidelines addressed to PSPs aim to improve the incident notification process between PSPs and CAs. To that end, the EBA proposes to further harmonise the format of communication and considered the following options:

> **Option 5.1:** PSPs should use a common standardised file for reporting major incidents to CAs made available on the website of the EBA.
>
> **Option 5.2:** CAs have discretion to decide on the file formats PSPs should use to report major incidents to them but a standardised file should be used when CAs submit the incident reports to the EBA.

D. Cost-benefit analysis and preferred options

Criteria triggering a major incident report and their thresholds

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

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

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

In term of major incident reports based on the criterion 'transactions affected' only, the number of incidents reported is expected to decrease by 21% under Option 1.1, which will insufficiently decrease the number of reports submitted. Under Option 1.3, 47% of the major incidents only due to the criterion 'transaction affected' are expected to not be reported. This threshold is therefore too high, as it cannot ensure that all significant incidents are captured. Option 1.2 strikes the correct balance in reducing the number of operational incidents reported while still capturing the significant incidents. Furthermore, it also strikes a balance between the different size of institutions across Member States. While the threshold may be considered low for large credit institutions, it can equally be considered high for smaller institutions. **Option 1.2** is the preferred option.

Under Option 2.1, a simple threshold based on a percentage of the PSP's regular level of transactions / payment users affected is considered. This option has the advantage to provide one simple quantitative threshold, which facilitates the application by PSPs. However, without a

threshold for the total absolute amount of transactions affected and total number of payment service users affected, significant incidents, especially from larger PSPs, might not be captured.

Under Option 2.2, the two-level approach is retained, while the precise quantitative threshold for the criterion 'transactions affected' is increased, and operational and security incidents are separately considered. This option has the benefit that it reduces the number of operational incidents reported, by increasing the threshold from EUR 100,000 to EUR 500,000 and by applying a time dimension of one hour to operational incidents, which is expected to be an appropriate duration to cover relevant major incidents, while reducing the number of reported operational incidents of lesser significance. The Guidelines further introduced a clear clarification of the term 'duration of an incident' for a harmonised application. In addition, the absolute amount threshold, which applies to all incidents, allows the capture of significant security incidents, both from smaller and larger PSPs.

Option 2.2 has the disadvantage of being more complex and requires PSPs to monitor the duration of incidents. However, PSPs already need to monitor any service downtime under the current framework and it is therefore expected that the increase in monitoring costs is small. At the same time, it will achieve the objectives of reducing the number of reported operational incidents and capturing relevant security incidents with an overall decrease in the reporting burden for PSPs. **Option 2.2** is the preferred option.

Under Option 3.4, the number of criteria to determine whether an operational or security incident is major remains the same. Under this option, PSPs and CAs are expected to have no additional direct costs such as costs related to the implementation of a new criterion. However, the rise of security risk in recent years[4] makes PSPs more vulnerable towards security breaches, especially when no precautionary measures are in place to address them in a timely and adequate manner. Even with related changes in other criteria, retaining the same criteria may not allow the identification of relevant major security incidents.

PSPs need to update their current systems to identify and report major incidents in order to implement the additional criterion. While initially considered the preferred option, the public consultation disclosed drawbacks to Option 3.1. The criterion is considered to have a relatively broad scope and may include unintentional incidents and external attacks with no fault on the part of the PSP after following its security policy. The former may not be distinguishable from operational incidents and thereby might go against the objectives of these revised Guidelines. The broad scope introduces more complexity into the assessment process and an additional reporting burden for PSPs.

The EBA considered narrowing the definition of security measures, to focus only on intentional incidents. Under Opinion 3.2. the reporting of non-relevant security incidents is lower than under Option 3.1 and would avoid overlap with operational incidents. However, the intention (motivation) can often not be clear at the beginning of the incident and thus require further assessment. Option 3.2 therefore does not narrow down the scope of reported incidents at the

[4] EBA Guidelines on ICT and security risk management.

stage of initial and possibly intermediate reporting compared to Option 3.1 and provides room for interpretation, which may hinder the harmonised implementation of this criterion, introduce more complexity into the assessment process and place an additional reporting burden on PSPs.

Option 3.3 also narrows the scope of the criterion by focusing on the security of network or information systems and whether it has been compromised by a malicious action. In comparison to Option 3.2 and 3.1, Option 3.3 focuses on the impact on the network or information systems of the PSP, rather than on the breach of security measures. Including the defined criterion in the Guidelines addressed to PSPs is expected to increase the number of reported major security incidents, which will improve PSPs' preparedness for such incidents and thereby positively affect the abilities of PSPs to provide services. **Option 3.3** is the preferred option.

Causes of major incidents

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

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

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

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

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

Notification process

The EBA considered the introduction of a standardised file for submission of incident reports from PSPs to CAs to ensure consistent reporting for all PSPs across the EU while facilitating automated

processing and timely assessment of the information received by CAs. Moreover, Option 5.1 aims to address concerns that PSPs which are part of a cross-border group face different national approaches for submitting the reporting template in the different Member States, which in turn increases their reporting burden.

On the other hand, PSPs may under current practices submit incident reports following national approaches. The consultation highlighted that the introduction of a standardised file will lead to significant changes to the current reporting approach in several Member States, such as the change in file format and IT solutions currently used. Those changes come with additional costs for CAs and PSPs to adapt their systems and an additional administrative burden for PSPs and CAs. Those costs are expected to outweigh the benefits from using a common reporting file, considering also that the notification approach will likely change again with the introduction of the proposed EU regulatory framework on digital operational resilience (DORA). **Option 5.2** is the preferred option.

5.2. Feedback on the consultation

The EBA publicly consulted on the draft proposal contained in this paper.

The consultation period lasted for two months and ended on 14 December 2020. A total of 29 responses were received, of which 18 were published on the EBA website.

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

In many cases several industry bodies made similar comments or the same body repeated its comments in the response to different questions. In such cases, the comments and EBA analysis are included in this section where the EBA considers them most appropriate.

Changes to the draft Guidelines have been incorporated as a result of the responses received during the public consultation.

Summary of responses to the consultation and the EBA's analysis

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
Feedback on responses to general questions			
1	One respondent was of the view that the incident reporting should be further harmonised and streamlined by requiring international PSPs to submit the incident report only once.	The EBA is of the view that when it comes to individual PSPs providing services directly or through agents/branches in other Member States, this should not be possible since the process envisaged in the EBA Guidelines is based on Article 96 of PSD2, which in turn requires the incident to be reported to the relevant CA in the country where the affected PSP is authorised/registered. Nonetheless, in the specific case of delegated and consolidated reporting, it is possible for PSPs to delegate reporting obligations under PSD2 to a third party on the basis of a formal contract or, where applicable, existing internal arrangements within a group. Such delegation is specified in Guideline 3 of the revised Guidelines on major incident reporting and is subject to permission by the relevant CA.	None.
2	One respondent was of the view that the 'reputational impact' criterion is one of the factors that in combination with others (e.g. 'high level of internal escalation level') acts as a trigger for escalation of the incident as major. Although the update to the definition helps, there should be a more tangible value association when reputational impact plays a role in ruling an incident as major. A binary value continues to be too subjective. Another respondent also requested further clarification of the 'reputational impact' criterion.	The EBA is of the view that the nature of the criterion is subjective and would require an interpretation from the side of PSPs. Furthermore, the EBA already introduced specific examples of what could or could not be considered as falling under the criterion, as well as additional minor changes to the explanation. Moreover, it is difficult to introduce a tangible value as suggested by the respondent because the criterion depends on the size of the PSP, the market it operates in and its specific circumstances. Nevertheless, the EBA has introduced additional minor amendments to Guideline 1.3. to address some of the concerns raised by the respondent.	*Guideline 1.3.viii* *[…] iii) ~~regulatory and/or~~ contractual obligations have been or will likely be missed, resulting in the publication of ~~regulatory measures~~ legal actions against the payment service provider, iv) regulatory requirements have not been complied with, resulting in the imposition of supervisory measures or sanctions that have been or will likely be ~~imposed or~~ made publicly available, and v) a similar type of incident has occurred before.*
3	One respondent was of the view that the EBA should clarify further	The EBA is of the view that no additional clarification is needed because the EBA already introduced some additional changes to the explanation of the criterion.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	the criterion 'high level of internal escalation'.	In addition, the criterion depends on the type of PSP and its size, and therefore is to some extent subjective since it is linked to the internal process of PSPs for the classification of incidents.	
4	One respondent requested further alignment in the use of the term 'third parties' throughout the Guidelines to ensure consistency, namely in the Annex to the Guidelines, parts 'B – Intermediate report' and 'B 3 – Incident description'.	The reference to 'third parties' in the scope of the Guidelines (paragraph 12) was included to clarify that major incidents affecting third parties to which operational functions have been outsourced by the PSP should also be reported. The EBA is of the view that the term has been used consistently and clearly. Therefore, no changes have been introduced in the Guidelines.	None.
5	One respondent suggested clarification on whether payments related to lending products (e.g. paying out initial loan amounts, payments in relation to loan top-ups) fall within the scope of the major incident reporting under the Guidelines.	The EBA is of the view that in the cases where payment transactions related to 'lending products' are considered as payment services as defined in PSD2, the PSPs have to report any major incident related to these services. Therefore, the EBA has not introduced any changes to the Guidelines in response to this comment.	None.
6	A few respondents were of the view that harmonisation in European reporting requirements (EBA, ECB, DORA) is needed on the classification schemes of incidents, reporting processes and procedures.	The EBA is of the view that the revised Guidelines already achieve significant harmonisation between the applicable incident reporting frameworks (PSD2, NIS Directive, SSM cyber security incident reporting framework). As highlighted in paragraph 33 of the CP 'the *proposed new category and its subcategories are aligned with the terminology used in other incident reporting frameworks, such as the Cybersecurity Incident Taxonomy developed by the European Union Agency for Cybersecurity, and also to a significant degree to the Cyber Incident Taxonomy of the Single Supervisory Mechanism in the Eurozone (SSM). This approach is also consistent with the Joint Advice of the European Supervisory Authorities on the information and communication technology risk management and cybersecurity.*" The EBA is not in a position to align the incident reporting frameworks further because of the dependencies and differences stemming from level-1 texts (PSD2) and other frameworks (SSM), which differ in scope and objectives.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
		Finally, since no specific suggestions for further harmonisation were proposed by the respondent, it is not clear which part of the EBA Guidelines may need further amendment.	
7	Two respondents were of the view that the EBA should align its Guidelines with the EU legislative proposal on digital operational resilience (DORA) in order to fully harmonise the reporting processes and procedures.	The EBA is not in a position to align the Guidelines on major incident reporting under PSD2 with the proposal for the DORA Regulation because the latter is still in the process of being negotiated and its final impact on major incident reporting under PSD2 is not yet known.	None.
8	One respondent suggested that the requirements of the revised Guidelines should be taken into account in the DORA proposal, for example with regard to alignment of criteria, templates and reporting processes.	The suggestion by the respondent goes beyond the capacity of the EBA since the EBA is not part of the legislative process in the DORA negotiations.	None.
9	One respondent was of the view that the application date of the Guidelines should be postponed to 1 January 2022 because of the DORA negotiations.	The EBA is mandated by Article 96(4) of PSD2 to review, in close cooperation with the ECB, the Guidelines on a regular basis and in any event at least every two years. Therefore, the current revision of the Guidelines is in fulfilment of that requirement and is not dependent on other factors, including DORA. In addition, the application date of EBA legal instruments cannot be based on other acts that are in the process of still being negotiated. Nevertheless, to allow CAs and PSPs to adapt their IT systems and incident reporting processes, the EBA has accepted the proposal to postpone the application date of the revised Guidelines to 1 January 2022.	*Date of application* *These Guidelines apply from 1 ~~October 2021~~January 2022.*
10	One respondent suggested differentiating between the type of payments, such as SEPA payments and instant payments, because of the difference in their potential impact.	The EBA is of the view that the Guidelines have been developed based on the principle that no differentiation between types of payments should be made and therefore has not incorporated the suggestion. In addition, if such a proposal were to be incorporated, it is likely to add further complexity in the reporting and, thus, to an increase in the reporting burden for PSPs and CAs that need to differentiate between different types of payments. This will go contrary to one of the objectives of the revision of the Guidelines – to simplify the incident reporting process.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
		Finally, it should be noted that additional information about types of payments can be provided by PSPs in the general fields of the incident reports.	
11	One respondent was of the view that there is an issue with the current methodology on calculating the value of 'payment service users affected' because the user has to have a contract with the PSP and thus the PSP would not include in their incident reporting cases where there is no contract between the customer and the PSP.	The respondent did not provide specific examples of incidents that would be excluded and any negative impact they may have, therefore it is unclear to the EBA how the concern can be addressed. Nevertheless, the EBA considered two possibilities that the respondent may have had in mind – execution of a single payment transaction and acquiring of a payment transaction. With regard to the execution of a single payment transaction, it should be noted that these are also based on a contract between the PSP and the payment service user, in line with the requirements of Title III, Chapter 2 of PSD2. When it comes to acquiring of payment transactions, it should be noted that the acquiring PSP has a contractual relationship with merchants that are its payment service users. Therefore, the acquiring PSP should include in the calculation of the criterion 'payment service users affected' only the affected merchants. Since the acquiring PSP does not have any contractual relationship with the payer, the number of payers should not be taken into account in said calculation. It should also be noted that, if the acquiring PSP considers it necessary, and if available, it can assess and provide information also on the number of affected payers on a voluntary basis. For the reasons stated above, the EBA has not introduced changes to the Guidelines.	None.
12	One respondent questioned why the term 'availability' is mentioned twice in the definitions (once within 'operational or security incident' and once on a stand-alone basis).	The EBA would like to clarify that the two definitions have a specific meaning within and purpose for the EBA Guidelines. They cover different concepts – more generally what is an operational or security incident that needs to be reported under the EBA Guidelines and more narrowly what should be understood by the term 'availability'. It should also be noted that these are terms used in other related legal instruments, e.g. the EBA Guidelines on ICT and security risk management, and any change should be considered within the context of these legal instruments. For the reasons stated above, the EBA has not introduced changes to the Guidelines.	None.
13	One respondent was of the view that the availability of a system is already captured under the criterion 'service downtime',	The EBA would like to clarify that availability is related to services being accessible and usable by payment service users. While service downtime may affect the availability of services for	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	therefore 'availability' should be removed from the criterion 'breach of security measures'.	the end user, it can also affect systems that do not have a direct impact on payment service users. However, since the comment made by the submitter is relevant to the way the EBA amended the newly introduced criterion (from 'breach of security measures' to 'breach of security of network or information systems'), the EBA would like to clarify that service downtime may be due to operational reasons and not necessarily related to a breach of the security of network or information systems. Similarly, it should be noted that not all breaches of the security of network or information systems have an impact on the availability. Finally, even in the very limited cases where an incident affecting the availability would trigger both criteria 'service downtime' and 'breach of security of network or information systems', there needs to be a third criterion with a lower impact level in order to classify an incident as major under the Guidelines. In relation to the above, the EBA has not considered it necessary to remove 'availability' from the criterion 'breach of security of network or information systems'.	
14	One respondent suggested to exclude the reference to 'crisis mode' from the criterion 'high level of internal escalation' in the submission of the initial report due to the difficulty in assessing it within the four-hour deadline.	The criterion 'high level of internal escalation' is subjective and dependent on the internal processes within each organisation. However, the reference to 'crisis mode' is one of the more tangible aspects of this criterion that allow institutions to identify whether an incident should be considered within the higher impact level of the criterion or not. Therefore, the EBA is of the view that this is an integral part of the explanation of the criterion. In addition, the Guidelines are developed in such a way to allow for PSPs to indicate whether a criterion can potentially be breached but also allow for the reclassification of an incident from major to non-major. Therefore, the Guidelines provide flexibility to PSPs in case they are unsure whether a crisis mode should or should not be called upon. In relation to the above, no changes have been introduced in the Guidelines.	None.
Responses to questions in Consultation Paper EBA/CP/2020/22			
Question 1. Do you agree with the change proposed in Guideline 1.4 to the absolute amount threshold for the criterion 'transactions affected' in the higher impact level?			
15	Several respondents were of the view that the proposed increase of the absolute amount threshold for the criterion 'transactions affected'	The EBA does not see merit in increasing the threshold any further in order to address the specific situation of a particular subset of payment service providers. The EBA is of the view that the EUR 15 million absolute amount threshold for the criterion 'transactions affected' in the higher impact level strikes the right balance between the	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	in the higher impact level to EUR 15 million could still be considered too low for wholesale/investment banks, which process a much higher daily volume of payment transactions. In their view, there is still margin to increase this threshold to EUR 20-30 million.	objectives of reducing the number of reported operational incidents and still capturing those incidents that have a major impact on the operation of payment service providers. Increasing the threshold further may lead to underreporting of major incidents. Furthermore, the threshold of EUR 15 million also strikes a balance between the different size of institutions across Member States. While the threshold may be considered low for large credit institutions, it can equally be considered high for smaller institutions.	
16	Several respondents suggested that the criterion should refer exclusively to the percentage threshold, so that its potential breach is not linked to the size and operations of the reporting PSP.	The EBA is of the view that having a percentage threshold only will lead to some relevant incidents with high impact not being reported if they affect larger PSPs that execute payment transactions of very large amounts. The EBA therefore has not incorporated the suggestion.	None.
17	One respondent proposed to increase the absolute amount threshold for the criterion 'transactions affected' in the higher impact level to e.g. EUR 50 million where two or more legal entities of the same banking group are involved, in order to limit the number of reports to be submitted.	See the response in row 15 above. In addition, it should be noted that in the case of groups (delegated reporting), each PSP should only consider their own payment transactions that are affected by the incident.	None.
18	One respondent was of the view that the criterion 'high level of internal escalation' should be removed.	The respondent did not provide sufficient rationale for considering their proposal and, taking into account that a removal of a criterion may have a negative outcome on the balance between the classification criteria, the EBA has not introduced the suggestion.	None.
Question 2. Do you agree with the changes proposed in Guideline 1.4 to the assessment of the criteria 'transactions affected' and 'payment service users affected' in the lower impact level, including the introduction of the condition that the operational incidents must have a duration longer than one hour?			
19	One respondent was of the view that the EBA should clarify whether thresholds for transaction values	The EBA is of the view that no additional change in the Guidelines is needed since Guideline 1.3 already clarifies that it relates to transactions that are directly or indirectly affected. Said Guideline also refers to the daily annual average of transactions. Therefore, the	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	and volumes relate to the outage period or the entire day.	transactions affected during the outage period should be divided by the daily annual average of domestic and cross-border transactions, in order to calculate the required ratio.	
20	A few respondents disagreed with the proposed change in the lower impact level of the criteria 'transactions affected' and 'payment service users affected'. They were of the view that the thresholds of the criteria 'transactions affected' and 'payment service users affected' should be triggered when both the absolute *and* the percentage threshold are met. In their opinion, this would lead to a more accurate reporting of major incidents to avoid reporting of relatively minor operational and security incidents, especially for larger institutions.	The EBA has not amended the proposal in the Guidelines based on the suggestions by the few respondents because their concerns are mitigated by complementary changes to the Guidelines – in particular, the fact that a condition related to the duration of operational incidents was added, as well as the fact that the absolute amount threshold for the lower impact level of the criterion 'transactions affected' was increased. It should be further noted that the change in the revised Guidelines is consistent with the objectives of the review – to capture additional security incidents that were not captured by the original Guidelines on major incident reporting. Finally, the EBA would like to highlight that in order for an incident to qualify as major, two other low-level criteria should be met in accordance with Guideline 1.1.	None.
21	A few respondents sought clarification (and potentially some examples) on the term 'duration of the incident', in particular in relation to the interplay with the term 'service downtime'.	The EBA agrees with the respondents that further clarification on the term 'duration of the incident' would be useful. Therefore, the EBA has introduced changes in the Guidelines to clarify that the duration of the incident means the time between the moment the incident occurs and the moment when regular activities have been recovered to the levels of service as before the incident. While the duration of the incident and service downtime may overlap to some extent, it should be noted that the duration is a more generic term, which also covers situations where the PSP is affected by an incident without any downtime of the service, e.g. incidents with an impact on confidentiality. Furthermore, the duration of the incident is a condition for the thresholds set in the lower impact level of the criteria 'transactions affected' and 'payment service users affected' and is not a separate classification criterion. 'Service downtime' is not inherently linked to the specific number of transactions or number of payment service users affected and could trigger major incident classification/reporting in combination with other criteria.	*Guideline 1.3(i)* *…For operational incidents affecting the ability to initiate and/or process transactions, payment service providers should report only those incidents with a duration longer than one hour. The duration of the incident should be measured from the moment the incident occurs to the moment when regular activities/operations have been recovered to the level of service that was provided prior to the incident. […]* *Guideline 1.3(ii)*

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
			…For operational incidents affecting the ability to initiate and/or process transactions, payment service providers should report only those incidents that affect payment service users with a duration longer than one hour. The duration of the incident should be measured from the moment the incident occurs to the moment when regular activities/operations have been recovered to the level of service that was provided prior to the incident. […]
22	One respondent suggested adding the condition of the duration of the incident for operational incidents being longer than one hour also to the higher impact level. In their view, the change related to the 'duration' will not have an effect on the reporting of major incidents for larger banks if it is only applicable to the lower impact level.	The EBA does not find merit in introducing a condition of the duration of operational incidents in the higher impact level for the criteria 'transactions affected' and 'payment service users affected' because by doing so some major incidents may be missed.	None.
23	One respondent suggested increasing the threshold for 'transactions affected' to EUR 1 million.	The EBA does not see merit in increasing the threshold any further. The EBA is of the view that the EUR 500,000 absolute amount threshold strikes the right balance between the objectives of reducing the number of reported operational incidents and allowing to capture additional relevant major security incidents that have an impact on the operation of PSPs. Increasing the threshold further may lead to underreporting of major incidents.	None.
24	One respondent suggested deleting the condition concerning the duration of the incident or replacing	See the response in row 21 above.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	the term with 'service downtime' and aligning the timeframe to more than two hours.	In addition, taking into account that the terms 'duration of the incident' and 'service downtime' have different scope and purpose, alignment in the timeframe of the two is not necessary.	
25	One respondent suggested to increase the timeframe of the duration of operational incidents from 1 to 1.5 hours.	The respondent did not provide sufficient rationale for considering the extension of the timeframe. Since the EBA is of the view that the one-hour duration provides a good balance between covering relevant major incidents and reducing the number of reported operational incidents of lesser significance, the EBA has not introduced the suggestion.	None.
Question 3. Do you agree with the inclusion of the new criterion 'breach of security measures' in Guidelines 1.2, 1.3 and 1.4?			
26	Around half of the respondents shared the view that the new criterion 'breach of security measures' is too broad and high-level. They also sought clarification on how and when PSPs should consider that the criterion is triggered. Some argued that it does not provide any objective indicators to assess whether the security incident is 'material'. Some of the respondents asked the EBA to give examples. A few respondents also argued that the criterion partly overlaps with already existing criteria, namely 'high level of internal escalation', 'reputational impact', 'transactions affected' and 'payment service users affected'. A few respondents were of the view that the new criterion 'breach of security measures' is cause-based while all others are impact-based.	The EBA reassessed the new criteria in the light of the responses received and agreed with the comments from the respondents and their rationale. In addition, the EBA took into account that the relatively broad scope of the suggested criterion 'breach of security measures' and the fact that it may cover unintentional incidents would contribute to receiving additional operational incidents, which was contrary to the objective of its introduction. Therefore, the EBA has narrowed down the scope of the new criterion to 'breach of security of network or information systems', which should allow additional security incidents to be covered that would be of interest to supervisory authorities, while avoiding the reporting of additional operation incidents that would not be of interest.	*Guideline 1.2(iii) Breach of security ~~measures~~of network or information systems* *Payment service providers should determine whether any malicious action has compromised the security of network or information systems related to the provision of payment services~~one or more security measures have been violated~~.* *Guideline 1.3(iii) Breach of security ~~measures~~ of network or information systems* *~~Payment service providers should determine whether one or more security measures, as referred to in Guideline 3.4.1 of the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04), have been violated with impacts on the availability/integrity/confidentiality/authenticity of payment service related data, processes and/or systems of the payment service provider, its payment service users or a third party to which operational functions have been outsourced. This also includes~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	A few respondents were of the view that the new criterion 'breach of security measures' introduces more complexity into the assessment process and creates an additional reporting burden for PSPs. The arguments provided in support of this referred to the difficulty in the implementation of the criterion, the need for additional time for classification and reporting, as well as the need for additional resources on the side of PSPs.		~~*internal and external unauthorised access as well as data leakages.*~~ *Payment service providers should determine whether any malicious action has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) related to the provision of payment services.* *Guideline 1.4, Table 1: Thresholds* *Breach of security ~~measures~~ of network or information systems*
27	Two respondents were of the view that breaches of payment security data within the context of the breach of security measures can be highly relevant and therefore suggested that the new criterion should be considered in the context of the higher impact level.	See the response in row 26 above. In addition, since the comment from the respondent would also apply to the amended criterion, the EBA is of the view that placing the criterion 'breach of security of network or information systems' in the higher impact level will lead to capturing some incidents that are not major, which in turn will result in over-reporting of incidents. At the same time, as highlighted in the CP on the revision of the Guidelines on major incident reporting under PSD2, the EBA observed that some important security incidents of relevance to CAs are currently not being captured because they trigger only two criteria from the lower impact level. The proposed additional criterion should fill this gap, albeit only in the lower impact level.	None.
28	A few respondents indicated that the combination of the new criterion 'breach of security measures' with the criteria 'high level of internal escalation' and 'reputational impact' may lead to the reporting of a high number of	The EBA would like to highlight that one of the objectives of the review of the Guidelines was to cover incidents that were not captured by the classification criteria of the Guidelines. It should also be noted that if the new classification criteria (now 'breach of security of network or information systems') would trigger an incident report together with the criteria 'high level of internal escalation' and 'reputational impact', then the chance of having a critical incident is very high so it would be useful for such an incident to be reported as major under the Guidelines.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	insignificant incidents that are not major.	The EBA has not introduced any changes to the Guidelines.	
29	One respondent sought clarification on whether the assessment of security incidents should take into account the non-compliance with security measures.	See the response in row 26 above.	See row 26 above.
30	One respondent questioned whether information on unintentional deeds should be taken into account in the new criterion 'breach of security measures', since the categories 'malicious actions', 'information gathering' and 'information context' do not clearly express intent as such and could be understood as unintentional actions.	See the response in row 26 above.	See row 26 above.
31	One respondent sought clarification on whether PSPs also have the responsibility of reporting incidents when the security breach is suffered not by the PSP itself but by the payment service user (which may represent a potential fraud that is already reported under EBA/GL/2018/05) or by other parties, such as financial market infrastructures.	See the response in row 26 above. However, since the comment made by the submitter may be relevant to the way the EBA has amended the newly introduced criterion (from 'breach of security measures' to 'breach of security of network or information systems'), the EBA would like to highlight that the criterion intends covering the breach of the security of network or information systems of the PSPs. Any additional incidents related to financial market infrastructures or technical service providers that have an impact on the PSP or its customers should be assessed on the basis of all classification criteria set in the revised Guidelines on major incident reporting under PSD2.	None.
32	Two respondents suggested that the new criterion 'breach of security	See the response in row 26 above.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	measures' should be based on the measurement of the actual or potential adverse effect an incident has on payment services users and payment institutions.	In addition, the EBA is of the view that PSPs should take into account the actual or potential impact of the event. As specified in Guideline 1.5, PSPs should resort to estimations if they do not have actual data.	
33	One respondent sought clarifications on whether data breaches which do not impact payment transactions should be reported.	The EBA has narrowed down the scope of the new criterion to breaches of security of network or information systems. For further details see row 26. Nevertheless, the EBA is of the view that the definition of the 'operational or security incident' clearly provides that the incident is 'a singular event or a series of linked events unplanned by the payment service provider which has or will likely have an adverse impact on the integrity, availability, confidentiality and/or authenticity of payment-related services'. Therefore, if the incident is not related to the payment-related services or data related to payment service users, it should not be reported under the Guidelines.	None.
34	One respondent was of the view that further clarity is needed on whether impactful breaches of security measures which do not meet any of the other lower impact level criteria should also be reported.	The EBA is of the view that Guideline 1.1 clarifies that an incident should only be reported if it is triggered by three or more criteria from the lower impact level (or one or more criteria from the higher impact level). In addition, please see row 26 above. In relation to it, impactful breaches of security of network or information systems should only be reported together with two or more criteria from the lower impact level. The EBA has therefore not introduced any changes to the Guidelines.	None.
35	One respondent suggested deleting the criterion 'breach of security measures' and reflecting its description in the definition of 'operational or security incident'.	The EBA disagrees with the proposal since it may narrow down the scope of the definition of 'operational or security incident'. In addition, modifications of the definition may have an unintended consequence on other parts of the Guidelines. In addition, please see row 26 above. The EBA would also like to highlight that one of the objectives of the review of the Guidelines was to cover incidents that were not captured by the classification criteria of the original Guidelines. Retaining an addition criterion on the breach of security of network or information systems would allow that.	None.
Question 4. Do you agree with the proposed changes to the Guidelines aimed at addressing the deficiencies in the reporting process?			

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
36	Two respondents were of the view that further clarification is needed on the meaning of the term 'classification'.	The EBA suggested changes in the CP on the revision of the Guidelines in order to clarify that the moment of classification of the incident, which includes the assessment of the incident against the criteria set in the Guidelines and the conclusion on whether said criteria are breached, is the starting point for calculation of the deadline for submission of the major incident report to the CA. However, since there seems to be a lack of clarity, the EBA has introduced additional clarifications in the Guidelines.	*Guideline 2.9* *Payment service providers should classify the incident in accordance with Guidelines 1.1 and 1.4 in a timely manner after the incident has been detected, but no later than 24 hours after the detection of the incident, and without undue delay after the information required for the classification of the incident is available to the payment service provider […]*
37	One respondent asked whether, in the case of all reports (initial, intermediate and final) related to the same incident being submitted together (in the cases where the incident is resolved in e.g. one hour), the reporting entity should wait to receive the unique reference number (after submitting the initial report) before submitting the intermediate and final report?	The EBA would like to clarify that in the case described by the submitter where the incident is resolved before the four-hour deadline for submission of the initial report set out in Guideline 2.8, all incident reports related to the same incident could be submitted together. The EBA has introduced minor amendments in the Guidelines to clarify this aspect.	*Guideline 2.7* *[…] Payment service providers should indicate this reference code when submitting an update either to the initial report or to the intermediate and final reports related to the same incident, unless the intermediate and final reports are submitted jointly ~~they are submitted together~~ with the initial report.*
38	One respondent requested clarification on whether the final report should be submitted with updated and complete information if the incident is reclassified as minor.	The EBA is of the view that Guideline 2.21 clearly articulates that, in the cases where the incident report is being reclassified as minor, instead of filling out section C of the template (with updated and complete information about the incident), PSPs should only check the box 'incident reclassified as non-major' and elaborate briefly on the reasons for the reclassification.	None.
39	One respondent asked whether a copy of the communication to users should be provided with the	The information provided from PSPs to the payment service users in line with Guideline 2.3. and Article 96(1) of PSD2 has not been standardised by the Guidelines since the latter focus on the reporting from PSPs to their CAs.	Amendments in section B1 of the template.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	template or separately as an attachment. The respondent suggested that it may be useful to introduce in the reporting template a box where the PSP can copy the text of the end client communication.	Therefore, it is left to CAs' discretion to decide whether attachment of the communication with the payment service users is required. The EBA has nevertheless clarified in the template that information about communication with payment service users can be included in the field 'More detailed description of the incident' in Intermediate report, B 1 – General details from the template set out in the Annex to the Guidelines.	
40	One respondent suggested adding to Guideline 2.8. that *PSPs* 'should send their reports during the CA's working hours.' The respondent highlighted this principle stands for all similar reporting frameworks.	The EBA disagrees with the respondent. It should be noted that many CAs have implemented processes allowing for reporting 24/7, including on online platforms.	None.
41	One respondent suggested that CAs should report back to PSPs if they identify any issues related to the information provided in the incident report.	The EBA is of the view that it is the responsibility of the PSP to ensure that the reports are populated correctly. Nevertheless, this does not prevent CAs from introducing validation and data quality checks of the information reported by PSPs and communicating back any identified issues with the data. Finally, introducing such a requirement would be an additional administrative burden for CAs. Therefore, the EBA has not amended the Guidelines.	None.
42	One respondent suggested that it should be left to the discretion of the PSP to use 'delegated reporting' in the case of banking groups sharing the same outsourcer/information system, irrespective of whether or not the banking group opts for consolidated reporting. Therefore, the reporting to the CAs could be delegated	The EBA is of the view that the suggestion put forward is possible when adhering to the procedure already set out in Guideline 3.1. Therefore, the EBA has not introduced any amendments to the Guidelines.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	completely to the outsourcer (i.e. initial, intermediate and final reports), or to each of the entities affected by the incident belonging to the same banking group (or to the parent company in the case of consolidated reporting) that share the same outsourcer/information system.		
43	PSPs should legally ask their outsourcer to report incidents as opposed to reporting itself those major incidents affecting functions outsourced by PSPs to third parties.	The EBA would like to clarify that PSPs have discretion to decide whether the PSP would report major incidents directly to their respective CA or whether they will outsource this function to a third party. Outsourcing of the incident reporting to third parties should be included within a written outsourcing agreement in line with the EBA GL on outsourcing arrangements. The EBA would also like to highlight that, in line with Guideline 3.1, the affected PSP 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 CA in the home Member State.	None.
44	One respondent suggested that the Guidelines should clarify that incidents caused by a disruption in the services provided by an infrastructure should also be reported. The respondent suggested reflecting this in the section with the scope of the Guidelines, in particular that the Guidelines apply to those incidents which are caused by both external and internal events.	The EBA is of the view that this is clearly articulated in the definition of operational and security incident and has, therefore, not introduced any changes to the Guidelines.	None.
45	One respondent suggested removing the requirement for submission of intermediate reports. In their view, intermediate reports	The EBA disagrees with the respondent on the fact that intermediate reports do not have added value. Initial reports serve the function of a warning signal, while intermediate reports provide substantial information about the incident itself to the CA. Therefore, they are crucial for the CA's assessment of the incident.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	do not bring any added value regarding the management of the incident itself while they create substantial administrative burdens for PSPs, in particular smaller PSPs like some co-operative banks.	The EBA has not amended the Guidelines.	
46	One respondent was of the view that the initial report should be provided within 12-24 hours after it has been classified as 'major' using a simplified version of the template in the Annex to the Guidelines. In the view of the respondent, the first hours after the detection of the incident are crucial for a PSP to concentrate resources on containing the incident and its effects rather than spending them on fulfilling reporting obligations.	The EBA would like to highlight that in accordance with the amendments to/clarifications in Guideline 2.8, the four-hour timeframe for submission of incidents from PSPs to CAs applies after the incident has been classified as major. Taking into account that there may be a small time gap between the moment of detection and the moment of classification of the incident, the amendment proposed in the CP should address the concern raised by the respondent. Nevertheless, for greater clarity about applicable deadlines and in line with the proposal from the respondent, the EBA has clarified in the Guidelines that the classification of the incident should take place within 24 hours of its detection, inter alia to avoid situations where PSPs might take an excessively long time to classify the incidents. The EBA also clarified in the Guidelines that on the rare occasions when the incident cannot be classified within 24 hours, the PSP should justify to the CA why this has been the case.	*Guideline 2.9* *Payment service providers should classify the incident in accordance with Guidelines 1.1 and 1.4 in a timely manner after the incident has been detected, but no later than 24 hours after the detection of the incident, and without undue delay after the information required for the classification of the incident is available to the payment service provider. If a longer time is needed to classify the incident, payment service providers should explain in the initial report submitted to the competent authority the reasons why.*
47	One respondent suggested clarifying that 'service downtime' applies from the moment of classification of the incident and not the moment of its detection, since incidents sometimes start as non-major and then evolve to major over time (e.g. login issues for a small portion of customers that grow into issues for a large portion of customers).	The EBA does not agree with the suggestion by the respondent. Guideline 1.3 clearly articulates that 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 and times when they are closed. Since service downtime is a criterion for the classification of incidents under these Guidelines, it cannot be measured from the moment of classification of the incident.	None.
48	One respondent was of the view that the Guidelines should clarify further the timeline for	For greater clarity about applicable deadlines and in line with the proposal from the respondent, the EBA has clarified in the Guidelines that the classification of the incident should take place in a timely manner after the incident has been detected, but no later than 24 hours after the detection of the incident, and without undue delay after the information	*Guideline 2.8* *Payment service providers should send the initial report to the competent authority*

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	classification of incidents after their detection.	required for the classification of the incident is available to the PSP. This is also to avoid situations where PSPs take a long time to classify the incidents. The EBA has also clarified in the Guidelines that, on the rare occasions when the incident cannot be classified within 24 hours, the PSP should justify to the CA why this has been the case.	*within four hours from the moment the operational or security incident has been classified as major~~, but no later than 24 hours after the detection of the incident. If longer time is needed to classify the incident, payment service providers should justify in the initial report submitted to the competent authority why~~.* See also the change in Guideline 2.9 in row 46 above.
49	One respondent suggested ensuring that all CAs can provide PSPs with the unique incident reference code (referenced in Guideline 2.7) immediately upon submission of the initial report to improve incident traceability.	The EBA is of the view that the generation and submission of the incident reference code should be left to the discretion of CAs because it is related to their internal procedures and the established channels for collecting incident reports. Nevertheless, the EBA has clarified in the Guidelines that the reference code should be provided from CAs to PSPs without undue delay.	*Guideline 2.7* *[…] Competent authorities should acknowledge the receipt of the initial report without undue delay and assign a unique reference code unequivocally identifying the incident. […]*
Question 5. Do you support the introduction of a standardised file for submission of incident reports from payment service providers to national competent authorities? If so, what type of structured file format would you support (e.g. 'MS Excel', 'xbrl', 'xml') and why?			
50	The majority of respondents supported the introduction of a standardised file for submission of incident reports from PSPs to CAs. It was indicated that by doing so the EBA will save time and effort of PSPs, in particular those that report in different countries. A few respondents shared the opposite view that CAs should have discretion to decide the most suitable format for communication	The EBA reassessed the merits of introducing a standardised file for the submission of incident reports between PSPs and CAs based on the feedback from the public consultation and came to the view that the disadvantages outweigh the advantages. A change in the current approach for reporting major incidents under PSD2 would lead to significant changes to IT systems and processes for PSPs, which are accustomed to national solutions and means for submission of incident reports. Changing the approach will bring additional cost for CAs to redesign their systems and for PSPs to adapt their reporting to these new systems. Changing the approach would introduce an additional administrative burden for PSPs, and possibly also for CAs, which may require further amendments in several years' time when DORA applies.	*Guideline 2.1* *Payment service providers should collect all relevant information, produce an incident report by completing the template in the Annex and submit it to the competent authority in the home Member State ~~by using a standardised file made available on the website of the EBA~~.* *Guideline 7.1* *Competent authorities should always provide the EBA and the ECB with all reports received*

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	with their industry without risking loss of any data element that is to be reported uniformly across Europe. Some of these respondents expressed a view that existing national reporting channels must be maintained since they are effective for the providers in the respective jurisdictions. Otherwise, there will be a high, short-term adaptation effort, which is likely to be repeated again when DORA applies.	The standardisation of a single file would be difficult to achieve since some incidents need to be submitted in the national languages of the Member State, therefore internationally operating PSPs would not benefit from any significant reduction in their respective reporting burden. Some CAs have already developed very sophisticated systems for reporting major incidents at national level, which are also compatible with other incident reporting frameworks. Harmonisation of the major incident reporting under PSD2 is already achieved by standardising the template for reporting of these incidents. Nevertheless, while the EBA has arrived at the view that the file for submission of incidents from PSPs should not be standardised, the EBA finds merit in standardising the file for submission of incident reports between CAs and the EBA/ECB since it will allow quicker and more efficient assessment of the incident reports received. The EBA has amended the Guidelines to reflect the above.	*from (or on behalf of) payment service providers affected by a major operational or security incident by using a standardised file made available on the website of the EBA*.
51	With regard to the structured file format to be used for the reporting of major incidents under PSD2, the majority of the respondents supported the use of MS Excel because in their view it is: - common, simple, easy to use, flexible and most institutions and individuals are familiar with it; - widely used and supported by PSPs, especially for regulatory reporting; - most appropriate since the template is populated manually; - allows for all types and sizes of PSPs to use it;	Following the public consultation, the EBA has changed the approach on the standardisation of the file for submission of major incident reports under PSD2. Based on the approach taken, the standardised file will be used for the submission of incident reports between CAs and the EBA/ECB (see row 50 above). Nevertheless, the EBA understands that some CAs may want to use the same standardised file for collecting incidents from PSPs in their jurisdiction. Therefore, in line with the suggestion by the majority of the respondents to the public consultation, the EBA has decided to use MS Excel as the standardised file format for incident reporting from CAs to the EBA. In addition to the arguments put forward by the respondents to the public consultation, the EBA took into account that said file format would not require additional resources from CAs and, where applicable, PSPs to implement significant IT changes and would allow maintaining the currently established process at national level to which PSPs are accustomed.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	- is already being used and works well. A few respondents supporting MS Excel as a file were against the introduction of more complex file formats because they will require resources for development of IT systems and may impact negatively on the simplicity and speed of the reporting process. Several other respondents supported the use of 'xml' mainly because of its capabilities to integrate into reporting processes and systems of PSPs, which also allow the data to be exported into other formats. Finally, a few respondents suggested the use of 'xbrl' with the main argument being that it is used for reporting.		
52	A few respondents suggested the use of additional and alternative file formats for the reporting of major incidents under PSD2.	The EBA is of the view that the concern of the respondents would be addressed by the amendments introduced as a result of the public consultation (see the two rows above). With the approach taken in the revised Guidelines on major incident reporting under PSD2, CAs are to have discretion to decide on the file formats.	None.
53	A few respondents supported the use of a dedicated portal by the EBA where PSPs can submit the incident report directly. Some acknowledged that due to the constraints of the reporting process this may not be feasible.	The EBA is of the view that the suggestion by the respondents is not possible since the process envisaged in Article 96 of PSD2 and as implemented in the EBA Guidelines on major incident reporting under PSD2 requires the incident to be reported to the relevant CA in the country where the affected PSP is authorised/registered first and then, as a second step, for the CA to forward the incident to the EBA and the ECB.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
		In addition, while carrying out the assessment of the practices for reporting major incidents under PSD2 that informed the revision of the Guidelines, the EBA has not found any deficiencies that would require such a change.	
54	One respondent was of the view that the notification process should allow for supporting material to be attached.	The EBA is of the view that the information relevant for the respective incident should be submitted to the CA with the standardised template provided in the Annex to the Guidelines. If CAs allow PSPs to submit attachments, these should be in support of the information provided in the standardised template. If the attachments contain substantial information not included in the incident reporting template, CAs should, in line with the requirements of Article 96(2) of PSD2, require PSPs to include the relevant details in the template and then for CAs to submit the updated template to the EBA and to the ECB. The EBA has amended the Guidelines to reflect that. These changes should ensure consistency of the data received and that the incident reporting process and its assessment are more efficient.	*New Guideline 2.5* *Any additional information contained in the documents provided by payment service providers to the competent authority, either on the initiative of the payment service provider or upon the request of the competent authority in line with Guideline 2.4, should be reflected by the payment service provider in the template under Guideline 2.1.*
Question 6. Do you agree with the proposed changes to Guidelines 2.4, 2.7, 2.12, 2.14 and 2.18 that are aimed at simplifying the process of reporting major incidents under PSD2?			
55	One respondent was of the view that there is a contradiction between provisions of para. 24 of the CP and Guideline 2.13 on removal of the PSP obligation to submit intermediate reports every three working days.	The EBA was not able to identify such a contradiction. The requirement to provide an update of the intermediate report every three days until the major incident is being resolved was removed from the Guidelines. In accordance with Guideline 2.13 (previous Guideline 2.12), the PSP should submit an intermediate report to the CA within three working days from the submission of the initial report, or earlier if regular activities have been restored and business is back to normal, in line with Guideline 2.12 (previous Guideline 2.13). In accordance with Guideline 2.14, in the event that the PSP becomes aware of significant change to the information provided with an intermediate report (including the specific case where the incident has not been resolved in three working days but at a later stage), the PSP should submit another intermediate report. This additional intermediate report has no specific deadline for its submission and is based on the assessment of the PSP.	*Change in Guidelines 2.12 and 2.13.* *Payment service providers should submit the intermediate report ~~within the timeframe specified in Guideline 2.12~~ when regular activities have been recovered and business is back to normal, informing the competent authority of this circumstance. Payment service providers should consider business is back to normal when activity/operations are restored with the same level of service/conditions as defined by the payment service provider or laid out externally by a service level agreement (processing times,*

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
		The EBA has swapped the place of Guidelines 2.12 and 2.13 and has introduced minor editorial amendments to clarify the interplay between the two Guidelines.	*capacity, security requirements, etc.) and when contingency measures are no longer in place. The intermediate report should contain a more detailed description of the incident and its consequences (section B of the template).* *If regular activities have not yet been recovered, payment service providers should submit an intermediate report to the competent authority within three working days from the submission of the initial report.* ~~*The intermediate report should contain a more detailed description of the incident and its consequences (section B of the template).*~~
56	One respondent was of the view that the unique reference code should be assigned by the PSP and not by the CA. In their view a naming convention (e.g. <country code>-<PSP identification>-<yyyy>-<incidentID>) can be introduced.	The EBA agrees that following a specific naming convention would allow for a more harmonised approach for generating reference codes and that this would be an easier process from the perspective of PSPs. However, it should be noted that the proposal for CAs to generate reference codes was put forward because of the following reasons: - CAs often have a standardised process and reference codes of incoming communications from external stakeholders, which are not necessarily related to incident reporting under PSD2. - Keeping track of a particular naming convention for generating these reference codes may introduce an additional burden for PSPs, especially the smaller institutions. - There is a risk that some PSPs would not follow a specific naming convention, which will undermine the entire process.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
		- The generation of the reference code by CAs and its submission to PSPs also serves the purpose of acknowledgement of receipt of the notification. For the reasons stated in the previous paragraph, the EBA is of the view that the advantages for generating a reference code by CAs outweigh the advantages of introducing a standardised naming convention for generation of these codes by PSPs. Therefore, the EBA has not introduced changes to the Guidelines.	
57	One respondent sought clarification about how the initial reporting in four hours should be managed in case of bank holidays or during the weekends. The respondent suggested to allow sending the incident report the next working day.	The EBA would like to clarify that the four-hour deadline set in Guideline 2.8 for the submission of the initial report relates to the moment of classification of the incident, not the moment when the incident started (or when the incident was detected). Nevertheless, the EBA would like to highlight that the reporting deadlines do not distinguish between working hours, weekends and bank holidays, which follows the requirement of Article 96(1) of PSD2 that prescribes that 'in the case of a major operational or security incident, payment service providers shall, without undue delay, notify the competent authority in the home Member State of the payment service provider.'	None.
58	One respondent suggested that the Guidelines should allow for an additional intermediate report to be submitted when the payment service affected by the major incident has been restored.	The EBA is of the view that this has already been addressed in the Guidelines. Guideline 2.12 (previous Guideline 2.13) prescribes that PSPs should submit the intermediate report when regular activities have been recovered and business is back to normal, but no later than the timeframe specified in Guideline 2.13 (previous Guideline 2.12). Payment service providers should consider business is back to normal when activity/operations are restored with the same level of service/conditions as defined by the payment service provider or laid out externally by a service level agreement (processing times, capacity, security requirements, etc.) and when contingency measures are no longer in place. The EBA has swapped the place of Guidelines 2.12 and 2.13 and has introduced minor editorial amendments to clarify the interplay between the two Guidelines.	*See row 55 above.*
59	Several respondents requested an extension of the deadline for submission of the final report in order to have more time for the root	The EBA is of the view that sufficient time has been provided for the development and submission of the final report. It should be noted that the proposal in the CP already extended the timeline from two weeks (10 working days) to 20 working days. Finally, it should be noted that the 20 working days timeline for submission of the final report was deemed sufficient for most incidents. For the small subset of incident reports that will	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	cause analysis (up to 30 working days). One respondent supported the extension of the deadline to send the final report to 20 working days generally but considered it insufficient for the submission of information on the 'assessment of the effectiveness of the actions taken'. The majority of the other respondents supported the extension of the timeline for submission of the final report from two weeks (10 working days) to 20 working days.	require more time for the submission of the final incident report, the EBA has arrived at the view that Guideline 2.18 already allows for the possibility of a further extension, based on communication between the PSP and the respective CA. Therefore, the EBA has not introduced any changes to the Guidelines.	
60	One respondent was of the view that Guidelines 2.12-2.14 are difficult to navigate through.	The EBA has swapped the place of Guidelines 2.12 and 2.13 and has introduced amendments to the two Guidelines in order to address the concern raised by the respondent.	*See row 55 above.*
61	One respondent was of the view that Guideline 2.13 should be amended in order to clarify that it refers to the last intermediate report (e.g. 'Payment service providers should submit the last intermediate report when regular activities have been recovered and business is back to normal […]').	This suggestion is contrary to the intention of the EBA to reduce the reporting burden on PSPs by limiting the number of reported intermediate reports to one. The EBA is of the view that the intermediate report should be submitted once regular activities have been recovered and business is back to normal in line with Guideline 2.12 (previous Guideline 2.13), which in almost all cases would be within the timeframe specified in Guideline 2.13 (previous Guideline 2.12) – three working days. Introducing a reference to a 'last intermediate report' would envisage at least a two-step process for the submission of intermediate reports and may bring confusion to reporting agents. In the very limited number of specific cases where the incident is not resolved within three working days, Guideline 2.14 requires PSPs to submit an updated intermediate report.	*See row 55 above.*

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
		The EBA has not introduced the suggested change but, as highlighted in the row above, the EBA has introduced editorial amendments clarifying the interplay between Guidelines 2.12-2.14.	
62	One respondent was of the view that there is a contradiction between Guideline 2.17 and Guideline 2.18 with regard to the reference to root cause.	The EBA has not found any contradiction between the two Guidelines. Guideline 2.18 clearly introduces the situation when the root cause of the incident has not been identified as an example of a situation when the PSP can request from its respective CA to extend the deadline for submission of the final report. Therefore, the EBA has not introduced any changes to the Guidelines.	None.
63	One respondent suggested that the deadlines for submission of the initial report should be longer in order to allow the more comprehensive information to be provided.	The EBA is of the view that the initial report does not contain detailed information. It also serves the purpose of a warning signal. For these reasons, the EBA has not introduced any changes to the Guidelines.	None.
Question 7. Do you agree with the proposed changes to the templates in the Annex to the Guidelines?			
64	One respondent was of the view that CAs have introduced templates with minor discrepancies to the template set in the Guidelines. The respondent was concerned that such approaches have a negative effect on the ability of PSPs to introduce a standardised escalating and reporting process across borders.	The EBA would like to highlight that the template set out in the Guidelines is uniform and must be adhered to by all CAs without any changes. The EBA has been made aware of different communication channels used by CAs to collect incident reports, which was the reason to put forward a suggestion about standardisation of the file for submission of incident reports from PSPs to CAs, but the EBA has not been informed of differences in the reporting templates. Since the concern of the respondent is not with the requirement of the Guidelines but with their application, the EBA has not introduced any changes to the Guidelines.	None.
65	One respondent was of the view that not all fields of the template should be mandatory. In the view of the respondent, it is not possible to fill in all fields of the template for all types of incidents. Therefore, they suggested that it should be possible	The EBA would like to highlight that population of all fields is mandatory. Nevertheless, the EBA understands that the information in some of the fields may not be available, unknown at the time of submission of the incident or not applicable. Therefore, the EBA has introduced changes in the template to reflect that.	Amendments in sections A1, A2, B1, B3 and C3 of the template.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	either to leave a field empty or to mark it as 'not available', 'unknown' or 'not applicable' (e.g. 'Incident related to previous incident?' (B1) and 'Incident affecting other service providers/third parties' (B1)).		
66	One respondent was of the view that the reporting templates should allow tracking of the updates of information provided with previous reports.	The EBA is of the view that since NCAs have discretion on how to collect incident reports from PSPs in their respective jurisdictions, the technological solutions and their functionalities cannot be prescribed in the Guidelines. In addition, the EBA proposed in the CP a change in the template to include a field in the intermediate and final reports allowing the PSP to summarise the changes made to previous reports, where applicable. Therefore, the EBA has not introduced any changes to the Guidelines.	None.
67	A few respondents suggested to rely more on 'free comments sections' to facilitate reporting agents when completing the template. These respondents were also of the view that it would be highly beneficial to reduce the restrictions in the reporting template that allow for detailed description.	The EBA disagrees with these respondents. Increasing the number of free comment sections and removing restrictions from the reporting template would go against the objective of achieving a more efficient and standardised reporting process and incidents assessment. In addition, it would not allow for automated processing of the provided information. Finally, it is likely to have a negative impact on the quality of the data collected.	None.
68	One respondent was of the view that the fields seeking information on whether the incident 'has been reported to other authorities' and what their decisions/ recommendations for said incident may be (e.g. 'Reporting to other authorities' (A2)) provide very little added value, as a very limited	The EBA is of the view that this information is relevant for competent authorities in order to understand whether and which other relevant authorities have been informed. This, in turn, would allow the respective authorities to cooperate with each other if needed. EBA is also of the view that since this requirement would apply to a very limited number of cases, it will not increase the reporting burden on the industry. Therefore, the EBA has not introduced any changes to the Guidelines.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	number of cases are to be reported to other agencies.		
69	One respondent sough clarification on paragraph 30 of the CP, i.e. 'Assessment of the actions taken during the duration of the incident'. In particular, the respondent was of the view that it was not clear if the assessment targets the adequateness or effectiveness of the actions. The same respondent was of the view that the fields 'Assessment of the actions taken during the duration of the incident' (C3) and 'Lessons learnt' (C1) are time consuming and suggested making them optional. The respondent also noted that the 'Lessons learnt' references seem to have been removed from the instructions part C1.	On the first point related to the assessment of the actions taken and whether they have been adequate or effective, the EBA is of the view that it is already clearly specified in the template (C3) and in the instruction part (C3) that the assessment is related to the effectiveness of the actions taken. The EBA did not introduce any changes to the Guidelines as a result. With regard to the remark on the required time to complete the fields covering the assessment of the actions taken during the duration of the incident and lessons learnt and the suggestion to make these complementary, the EBA reassessed those fields and took the view that they overlap slightly. The EBA therefore merged them into a single field 'Assessment of the effectiveness of the actions taken' during the duration of the incident. On the timeline for submission of the final report, see row 59. On the suggestion to make the fields optional, see row 65.	Amendments in sections C1 and C3 of the template.
70	One respondent was of the view that the field 'Time' may be deleted from all reports since the 'Time of Report' corresponds to the time of the upload of the report (or date email sent).	The EBA is of the view that the field 'Time' for submission of the report is needed for completeness of the report and how the respective timelines are being met. This would also be relevant for aggregated and automated assessments of incident reports. Furthermore, the EBA is of the view that the field 'Time' is particularly relevant when the incident is submitted to the EBA and ECB and forwarded to other CAs that may not have access to the system logs or the email containing the respective incident report.	None.
71	One responded suggested that the EBA clarify the exact scope of the subcategory 'Information context	The EBA agrees the correct reference should be to 'Information content security' as it is indicated in the 'Cyber incident taxonomy' and introduced the editorial amendment.	Amendments in section C2 of the template.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	security', and also amend the term used to 'Information content security' to be consistent with the Cyber incident taxonomy.	With regard to the request for further clarification, the EBA sees the examples provided as sufficient and at the same time consistent with other incident reporting frameworks, such as the 'Cyber incident taxonomy' (point 7.1) of the NIS Cooperation Group. Therefore, the EBA did not introduce further clarifications.	
72	One respondent was of the view that the scope of the reported countries that have been affected by the incident may change over the life cycle of the incident and consequently the PSP would have to report such changes in section B, field 'Changes made to previous reports'.	The EBA would like to clarify that any changes related to the information contained in any of the previously submitted reports should be reflected in the respective report and summarised in the field 'Changes made to previous reports'. For example, if the PSP has specified in the initial report that the incident affected PSPs in two other jurisdictions but in the intermediate report the PSP specifies that PSPs from all EU Member States have been impacted by the incident, the initial report should be amended to reflect that change and the intermediate report should contain a summary of this change (and others that may apply). It should be noted that this is in line with Guideline 2.14, which specifies that PSPs 'should update the information already provided in sections A and B of the template when they become aware of significant changes since the submission of the previous report'. Finally, it is worth clarifying that the changes made relate to the information provided with the previous report. For example, if the information provided with the initial report changed and this was reflected in the intermediate report, and no other changes have occurred after the submission of the intermediate report, the final report should not reflect any changes. The EBA has introduced minor changes to the reporting template to reflect the above.	Amendments in sections B1 and C1 of the template.
73	One respondent sought clarification on the purpose of the field 'Impact in other EU Member States, if applicable' (A2).	The EBA would like to point out that the information from the field 'Impact in other EU Member States, if applicable' would be useful to identify whether other institutions/authorities may be affected by the same incident. This is in line with the requirements of Article 96(2) of PSD2, which states 'EBA and the ECB shall, in cooperation with the competent authority of the home Member State, assess the relevance of the incident to other relevant Union and national authorities and shall notify them accordingly'. Finally, the EBA is of the view that the instruction document in the Annex to the Guidelines already contains some examples to clarify this aspect. Therefore, the EBA has not introduced changes to the Guidelines.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
74	One respondent suggested deleting the field 'Date and time when the incident was restored or is expected to be restored (DD/MM/YYYY, HH:MM)' (B1) because such an expectation is not easy to assess.	The EBA is of the view that the information about the time when the incident has been restored is important for the assessment of the incident and the measures taken. Therefore, the EBA has not incorporated the suggestion from the respondent.	None.
75	A few respondents were of the view that the subcategories for causes of incidents are too granular. In their view, it is at times difficult to differentiate between the subcategories for causes of incidents. The respondents therefore suggested that the EBA provide more precise and unambiguous definitions in order to make sure incidents are properly categorised in practice. One respondent provided the following examples: - the subcategories called 'Malicious action' and 'Process failure' would require some examples in their description of B3. - the subcategory 'Fraud', as it is currently defined, may overlap with other subcategories of malicious action. For instance, phishing (currently included in the definition of fraud) could also be said to fall within the subcategory 'Information gathering'. 'Fraud' should be 'an unauthorised use (e.g.	The EBA is of the view that the level of granularity of the subcategories of causes of incidents is appropriate and would be required for the purposes of supervision and oversight. Furthermore, it ensures consistency and harmonisation with other incident reporting frameworks. The EBA would like to highlight that the subcategories are not mutually exclusive, in the sense that more than one cause of the incident may apply. PSPs would therefore be able to select multiple subcategories of causes of incidents. With regard to the comment on fraud, to avoid ambiguity with the exact meaning of the term under PSD2, the EBA has amended the name of the subcategory to 'Fraudulent actions'. In addition, on fraud it should be noted that not all fraud should be reported under the Guidelines but only the fraud that falls within the scope of the definition of operational and security incident and that breaches the classification criteria and their thresholds.	Amendments in sections B3 and C2 of the template.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
	unauthorised use of resources, copyright infringements)'. One responded proposed the subcategories 'Malicious action' and 'Process failure' be consistently presented, i.e. either describe the process failures as 'monitoring and control, communication, operations, etc.', or by adding an adjective to specify what kind of failure, e.g. deficient monitoring and control, communication issues, improper operations. In the view of the respondent, the suggestions presented in the CP are a combination of both, therefore inconsistent.		
76	One respondent suggested to add to the root cause 'System failure' the category 'Infrastructure failure'.	The EBA is of the view that the infrastructure failures are already covered by either 'Hardware failure' or 'Network failure'. If failure of an infrastructure does not qualify in either of the referred categories, PSPs would be able to include it in 'Other (please specify)'. In addition, the EBA took into account that introducing the suggested new category 'Infrastructure failure' would lead to a situation where the categories of the root cause 'System failure' are not mutually exclusive, which is not desirable. Therefore, the EBA has not introduced changes to the Guidelines.	None.
77	One respondent was of the view that the reference in template B2 to 'Describe how the security policy was violated' is not consistent with the definition of the criterion 'Breach of security measures' in the Guidelines.	See row 26.	None.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
78	One respondent commented on the economic impact (B2), in particular the reference to 'Missed business opportunities, potential legal costs'. In the view of the respondent, this is not in line with the reporting requirements of operational risk events, where financial impact should be considered in actual terms and should not include opportunity costs (except near miss events).	The EBA agrees with the respondent and, as a result, deleted the reference to revenues lost due to missed business opportunities from the examples given for economic impact under 'Indirect costs' (B2).	Amendment in section B2 of the template.
79	The reputational impact in Guideline 1.3. viii and B2 specifies that certain incidents could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement). However, mixing the reputational and regulatory impact of an event could prove to be difficult in the internal classification of incidents, as well as in the reporting process and record keeping.	The EBA is of the view that actions from PSPs that are based on regulatory requirements or infringement of the legal basis may have a reputational impact to the institution. The EBA also acknowledges that not all regulatory and/or supervisory actions (e.g. fines, administrative sanctions) entail a reputational risk, unless when these actions are made public. The EBA has clarified the above in the Guidelines.	Amendments to section B2 of the template. *Guideline 1.3. viii* *…iii) ~~regulatory and/or~~ contractual obligations have been or will likely be missed, resulting in the publication of ~~regulatory measures~~ legal actions against the payment service provider, iv) regulatory requirements have not been complied with, resulting in the imposition of supervisory measures or sanctions that have been or will likely be ~~imposed or~~ made publicly available, and v) a similar type of incident has occurred before.*
80	One respondent sought clarification on the interplay between the criterion 'breach of security measures' and the 'overall impact' (B4) on the reference to the impact on the integrity, availability, confidentiality and/or authenticity.	The EBA, as a result of the public consultation, has introduced changes to the criterion 'breach of security measures' (please see row 26). Nevertheless, since the comment would be applicable to the changes introduced to the criterion 'breach of security measures', the EBA has introduced minor amendments in the 'overall impact' field to reflect that it applies to all incident reports and not only to the security-related incidents. It should be further noted that the breach of security of network or information systems and the overall impact are different by nature since one is a cause of an incident and the other is related to the impact of the incident.	Amendment in section B4 of the template.

Comments	Summary of responses received	EBA analysis	Amendments to the proposal
81	One respondent suggested the Guidelines need to distinguish clearly between operational/technical incidents and security incidents.	The EBA is of the view that the instructions to fill out the template as part of the Annex to the Guidelines allow such a distinction between operational and security incidents to be made. The descriptions of the fields in 'Type of incident' in sections A2 and B3 clearly elaborate on both 'operational' and 'security' incidents. Therefore, the EBA has not introduced changes to the Guidelines.	None.
82	One respondent was of the view that cybersecurity-related changes proposed in the CP should be removed from the Guidelines since they do not add much information and are already subject to other reporting obligations.	The EBA would like to highlight that cybersecurity incidents are part of the security incidents, which are explicitly referred to in PSD2. The EBA cannot narrow down the scope of a level-1 text with its Guidelines.	None.

Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu