EBA/CP/2016/23

07 December 2016

Consultation Paper

on draft Guidelines on major incidents reporting under the Payment Services Directive 2

Contents

1. Responding to this consultation

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

Comments are most helpful if they:

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

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 07.03.2017. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

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

Data protection

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

2. Executive Summary

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

These draft Guidelines set out the criteria, thresholds and methodology to be used by payment service providers in order to determine whether an operational or security incident should be considered major and, therefore, be notified to the competent authority in the home Member State. Moreover, these draft Guidelines establish the template that payment service providers will have to use for this notification and the reports they have to send during the lifecycle of the incident, including the time frame to do so.

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

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

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

Next steps

The consultation period will run from 07 December 2016 to 07 March 2017. The final Guidelines will be published after this consultation.

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 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 in order to ensure that damage to users, other payment service providers or payment systems is kept to a minimum, Article 96 foresees that payment service providers shall report major operational or security incidents to the competent authority in their home Member State without undue delay. It is also expected that this competent authority, after assessing the relevance of the incident to other relevant domestic authorities, notifies them consequently.

   .

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

   a. payment service providers, on the classification of major operational or security incidents and on the content, the format, including standard notification templates, and the procedures for notifying such incidents;

   b. competent authorities, on the criteria on 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, the PSD2 assigns to the EBA and the ECB a central coordination role in this context towards other relevant Union and national authorities. The Directive provides that the competent authority in the home Member State swiftly shares with the EBA and the ECB relevant details of the incident, that a collective assessment of its significance for these other Union and national authorities is performed and that, where appropriate, the EBA and the ECB notify them accordingly

5. In what follows in the rationale section below, this Consultation Paper explains the reasoning for some of the options the EBA has considered and the decisions the EBA has taken.

3.2. Rationale

6. Access to reliable, up-to-date and comparable data on operational or security incidents provides many benefits. On the one hand, it proves critical in order to develop a clear understanding of the nature and extent of the actual problems at stake. As a result, it also helps define the best actions that are potentially required to address them in a satisfactory manner. Over and above, incident reporting contributes to assessing the success of applicable legal, regulatory, organisational and technical measures as well as to identify good practices across the market. Effective notification procedures enable also a coordinated response and ultimately ensure that competent authorities can follow up with payment service providers in their regulatory capacity, if necessary.

7. Given the existing experience on incident reporting practices of both, national banking supervisors and central banks acting in their capacity as overseers of payment systems, schemes and instruments, prior to starting to develop the substance of the draft Guidelines, the EBA and ECB sought initial input from these authorities. For this purpose, a stock-taking exercise was carried out amongst them, which helped map the current landscape across the Union and identify its strengths and shortcomings. This approach provided a solid foundation for the development of a new reporting scheme, by narrowing down the set of best practices that could inform a proportionate and harmonised reporting framework as laid down in the PSD2 mandate.

8. While this exercise confirmed that compulsory reporting procedures for payment-related incidents were already in place across the European Union, it also confirmed the need for a common approach, due to the growing cross-border dimension of operational or security incidents, the disparity in the criteria presently applied by competent authorities for the fulfilment of reporting obligations, the prevalence of individual payment service provider's judgments about the appropriateness of a notification and the non-structured nature of most reporting procedures currently in place (e.g. contents, formats and reporting deadlines). Likewise, standardised data should cater for sophisticated statistical analyses and facilitate the reporting flow, thus minimising the need for complementary information to be delivered by payments service providers to the authorities. Lastly, standardisation should make it possible for payment service providers to install interfaces that align their internal reporting procedures with those established in these draft Guidelines.

9. In order to enhance the resulting framework, the EBA and the ECB further liaised with the European Union Agency for Network and Information Security (ENISA). Their standards, specifications and extensive expertise on incident reporting in the telecommunications sector and, more recently, with so-called trusted service providers were also taken into account for the completion of these draft Guidelines, with a focus on the provision of payment services.

10. Along the same lines, the ECB, in its capacity as competent authority for prudential supervision of credit institutions, was actively engaged in the present work, given that significant credit institutions are under the direct supervision of the above-mentioned authority and that these draft Guidelines apply to them as well when acting in their condition of payment service providers. Seeking consistency with any of the ongoing work at the ECB in this field was thus deemed relevant.

11. Furthermore, in the specific case of the Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), the provisions contained in the PSD2 on the notification of incidents are considered to be one particular case of a sector-specific Union legal act as foreseen in Article 1(7) of the NIS Directive. Therefore, as regards incidents affecting the provision of payment services, only those requirements laid down in the PSD2 on the reporting process will apply to credit institutions under the scope of the aforementioned Directive.

12. The EBA and the ECB arrived at the view that no general exemption based on the nature or size of the payment service provider was permissible under the Directive and that its legal provisions apply to payment service providers located within the Union and to all payment services they provide as listed in Annex I of the PSD2, regardless of the currency, yet only for those parts of the payment transaction that are carried out in the Union. Moreover, in the case of international banking groups, each affected payment service provider will have to submit an incident notification to the competent authority in the Member State where they have been granted authorisation.

13. Given the above, the requirements proposed in the draft Guidelines below set out a consistent and transparent framework for the notification by payment service providers of major operational or security incidents falling under the scope of the PSD2, namely incidents with an impact on payment services (i.e. incidents affecting transactions, processes, data or funds, among other things). It attempts to balance comprehensiveness and simplicity while still meeting the expectations of all stakeholders by leveraging current practices. It does so by applying a limited set of basic indicators related to the targeted business and by acknowledging the complexity of the situations as well as the limitations faced by payment service providers both at the time an incident occurs and during its lifecycle. Hence, these draft Guidelines are aimed at preventing payment service providers from being overburdened with reporting duties while responding to an incident as well as avoiding to create undue distortions between the smaller and the bigger players in the market.

14. As a first step, these draft Guidelines complement the PSD2 with a workable definition of what a major operational or security incident is, by focusing on the scope of the Directive and outlining all the different aspects that could potentially be affected by such a disruption: i.e. the integrity, availability, confidentiality, authenticity and/or continuity. Explanations of all the relevant elements of the definition are further provided.

Q1. Do you consider the definitions included in the draft Guidelines to be sufficiently clear?

15. The draft Guidelines also set the methodology that payment service providers should use in order to assess an incident when first detected and, if concluded to be major, notify it to the competent authority in the home Member State.

16. In particular, the draft Guidelines establish the qualitative and quantitative criteria that payment service providers should use to assess the materiality of an operational or security incident. These criteria have been chosen on the basis of their present level of use among both banking supervisors and central banks acting in their oversight capacity. Moreover, they reflect the experience with incident classification and reporting of ENISA and the ECB, in its capacity as competent authority for prudential supervision of credit institutions. These criteria take further into account the nature of the incidents to be reported (major operational or security incidents under the scope of the PSD2) as well as the size of the various types of payment service providers and their legal status. In addition, other features such as the capacity of the criteria to ensure a proper and proportionate metric of the severity of the incident, as well as the possibility of standardisation and automation of the data or their prompt availability and collection, have also been pondered.

17. Specifically, the rationale below was followed for choosing each criterion:

a. *Transactions affected* – the severity of an incident may be assessed by the number of payment transactions compromised and/or the value of the payments involved. On a general basis, the more the transactions or the higher the values, the more severe the incident is likely to be. It should be noted that this criterion is not applicable to account information service providers, since they do not carry out payment transactions.

b. *Clients affected* – the number of clients affected is, by itself and regardless any other considerations, a good indicator of the materiality of a payment service-related incident, as it is connected to other relevant factors such as potential complaints, indemnities, etc.

c. *Service downtime* – an event that disrupts the normal flow of business processes usually leads to delays or outages in standard performance metrics. As a general rule, the longer it takes to recover regular activities, the more clients and transactions are likely to be impacted, the greater the implications for the brand image, etc.

d. *Economic impact* – incidents oftentimes bear an effect on the payment service provider's financial statements, thus providing an objective and measurable reference of its relevance for both the institution itself and the economy at large.

e. *High level of internal escalation* – incidents raising the attention of the Chief Information Officer (or equivalent position) outside of the regular reporting procedures provide a meaningful indication of the potential significance of the underlying event. By means of this indicator, other relevant dimensions are indirectly captured such as, e.g. the criticality of the business process affected, the impact on a security goal, the relevance of the clients affected, the fact that it happened close to bank holidays or during a particularly critical time window, the degree of repetition of a given incident, etc.

f. *Reputational impact* – despite its intangible nature, high-profile incidents altering the public perception of a payment service provider can cause short-term effects leading to greater long-term consequences including reduced profits, loss of clients and key employees, sudden drops in stock price or the withdrawal of a license.

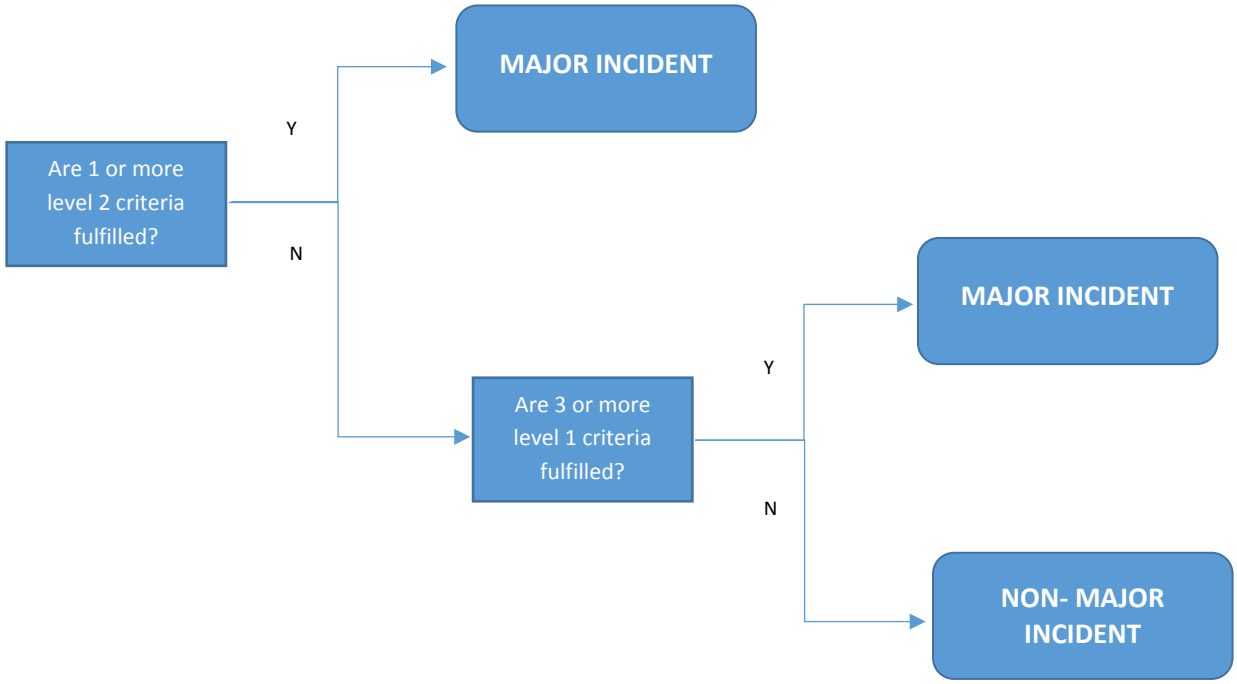
g. *Potential to affect other payment service providers or relevant infrastructures* – this criterion gives an indication of the seriousness of the incident not only for the payment service provider which is directly affected, but also for the market as a whole, the payments industry and/or other parties; the criterion assesses and reflects the possibility of the incident spilling over into other entities or sectors.

18. For an incident to be classified as major it must have significant disruptive effects on the business activity of a payment service provider. Therefore, there is a need to measure the actual size of an incident's impact. In order to to do so, the draft Guidelines establish a set of thresholds for each individual criterion. As a result an incident would only be ranked as major when a certain number of these thresholds are reached or exceeded.

19. The thresholds mainly echo the current practices as reflected in the initial fact-finding exercise carried out across supervisors and overseers. They do also take into account the experience gained by the ECB as a result of the pilot exercise on cyber-incident reporting they launched in their capacity as competent authority for prudential supervision of credit institutions. Moreover, they care for the legal status and size of the various types of payment service providers, mainly by combining absolute and relative thresholds. There are cases, however, where certain thresholds may not be applicable. In particular, the reference to Tier-1 capital, under "economic impact", is not suitable for account information service providers, since they do not have to fulfil capital requirements. As a result, account information service providers should only assess this criterion against the 200,000 EUR threshold.

20. The thresholds are structured along two potential levels of severity, one lower than the other, since it was considered that some criteria would, by themselves, be an indication that the incident is major once they attained a certain level. The more stringent level (level 2) is only featured in four out of the seven classification criteria. Thus, when any of these four criteria reaches this level, the incident should be considered major. Should none of these criteria reach level 2, payment service providers should analyse all seven criteria against the less stringent thresholds (level 1). In this case, it was considered that the fact that 3 or more criteria met or surpassed the level 1 thresholds would be a good indication of the incident being major. Diagram 1 schematically depicts the methodology explained above.

Diagram 1: Decision tree for assessing the severity of an operational or security incident



Legend:
- If an incident meets 1 or more level 2 thresholds, it should be qualified as major.
- If an incident does not meet any level 2 thresholds, but meets 3 or more level 1 thresholds, it should be qualified as major.
- If an incident does not meet any level 2 thresholds and does not meet at least 3 level 1 thresholds, it should not be qualified as major.

Q2. Do you consider the criteria and methodology applicable for the assessment and classification of an incident as major to be sufficiently clear? If not, what should be further clarified?

Q3. Do you consider that the methodology will capture all of / more than / less than those incidents that are currently considered major? Please explain your reasoning.

Q4. In particular, do you propose to add, amend and/or remove any of the thresholds referred to in Guideline 1.3? If so, please explain your reasoning.

21. Payment service providers will still be able to preserve their internal incident categorisation rules provided the reporting of incidents to competent authorities takes place in line with these draft Guidelines. Moreover, payment service providers may voluntarily report other operational or security incidents not falling under the category of major but considered significant according to their internal classification scheme. In such a case, an explanation of the underlying rationale should be provided to the competent authority as well.

22. Homogeneity is further ensured by foreseeing the use of a common template for the notification of incidents. This template is specifically conceived for reporting those incidents that are classified

as major, but its use is also advisable for the voluntary reporting of other incidents that payment service providers may deem relevant to notify. The template (see Annex 1) has been structured along eight basic sections which follow a logical sequence in the analysis and handling of an incident, namely: a) general details, b) incident discovery, c) incident classification, d) incident description, e) incident impact, f) incident mitigation, g) root cause analysis and follow up and h) additional information.

23. The use of a standardised template will enable greater comparability and automation in the management of information. This will be further ensured by using the same template throughout the various stages of the investigation process on an incremental basis (i.e. adding more and more quality information as the incident evolves). Three types of reports are foreseen on the basis of the different phases of an incident:

    a. Initial reports are not expected to provide very detailed information or accurate figures, but rather a high-level overview of what has happened and the impact it has had or may have. Balancing the need of competent authorities to be aware of an incident without undue delay and the importance of not interfering with the management of the situation by the payment service provider, a maximum limit of 2 hours from the moment the incident was detected has been considered, as a general rule, a good deadline for delivering the initial report.

    b. Intermediate reports are not seen as something that should be produced with a fixed periodicity, but rather every time there is relevant information about the evolution of the incident. Aiming at balancing the need of competent authorities to be regularly informed of how the incident develops and the fact that payment service providers are those in the best position to determine when the next update could reasonably be expected, the periodicity of intermediate reports has been left to the discretion of payment service providers, with a maximum limit of 3 business days.

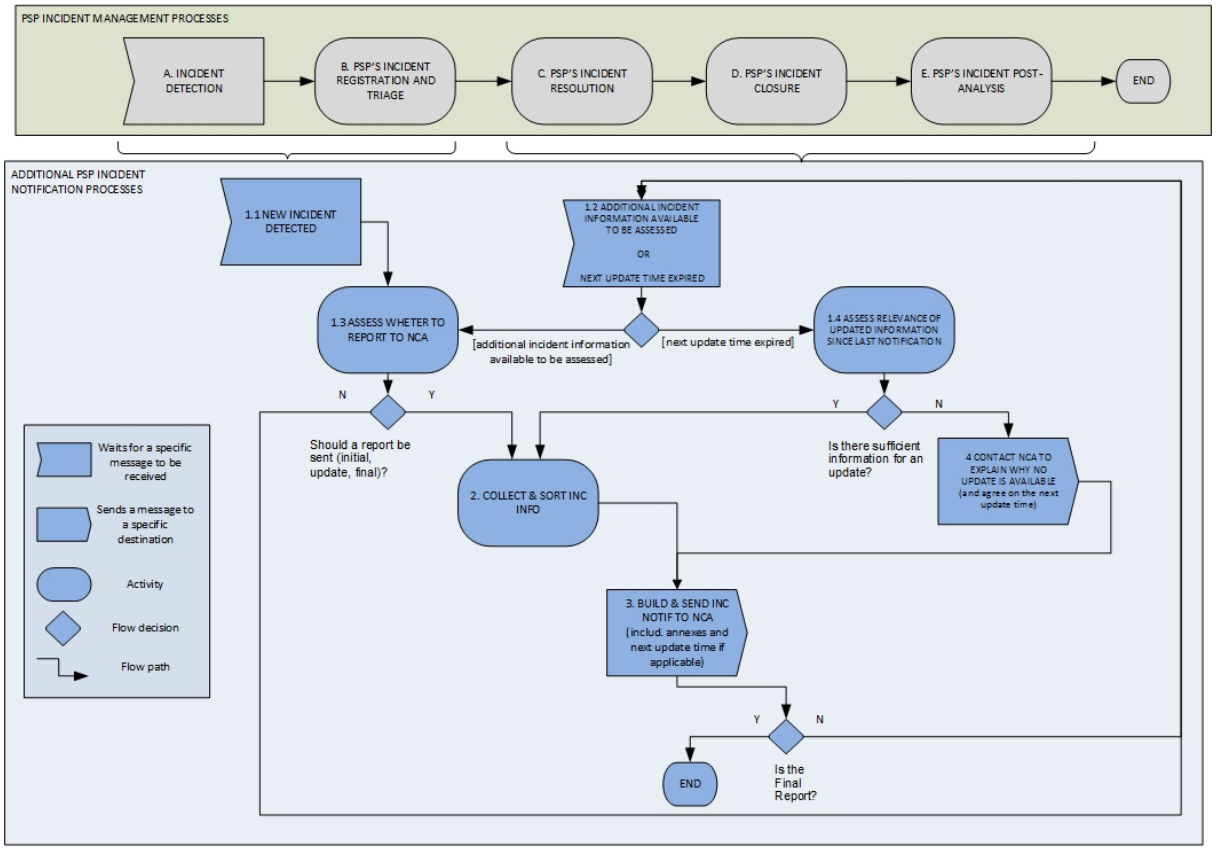
    c. Final reports should aim at providing full information (unless this final report is the result of an incident ceasing to qualify as major), including a detailed and accurate description of what happened, the impact it had and how it was solved. Two weeks since business is deemed back to normal is regarded as enough time for payment service providers to gather all this information, although, in order to ensure the delivery of a quality report, the possibility of a delay has also been foreseen. Moreover, it is acknowledged that the analysis of the root cause and the design of the corrective actions/measures could take quite a long time, and it has therefore not been considered appropriate to request full information as regards these two aspects.

24. Despite the benefits of using a common template, a certain degree of flexibility is, nevertheless, introduced by allowing payment service providers to attach as an annex additional explanatory documents they may have available and deem relevant for the competent authority. These documents do not need to follow any specific format or contents. In particular, internal incident reports or those facilitated by a third party technical service provider could be provided along with other more general reports that

may go beyond the actual incident: e.g., statistics about typical failures or most common threats as well as references to best practices.

25. A summary view of the procedure for the notification of major operational or security incidents, as explained above, is illustrated by Diagram 2, which clearly depicts the different steps in the notification process.

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



Q5. Do you think that the information depicted in the template in Annex 1 is sufficient to provide competent authorities in the home Member State with a suitable picture of the incident? If not, which changes would you introduce? Please explain your reasoning.

Q6. Are the instructions provided along with the template sufficiently clear and helpful to remove any doubts that could arise when completing the required fields? If not, please explain your reasoning.

Q7. As a general rule, do you consider the deadlines and circumstances that should trigger the submission of each type of report (i.e. initial, intermediate and final) feasible? If not, please provide a reasoning and justify any alternative proposal.

26. As an attempt to reflect current practices, the draft Guidelines also open up the possibility for payment service providers to rely on a third party established in the Union to fulfil their reporting obligations, provided certain conditions are met and the competent authority in the home Member State is informed. In jurisdictions where this option is presently a common practice, it has proved useful for reducing the reporting burden on small payment service providers (in particular when they rely on the technical services provided by external parties). In these cases, the reporting procedure benefits from the notification being carried out by the third party, since its overview and understanding of the circumstances surrounding the incident are much more accurate than those of the payment service provider.

27. The delegation of administrative tasks described above can, under no circumstance, imply that payment service providers are relieved from their regulatory responsibilities in relation to the notification of major operational or security incidents. Therefore, in line with the outsourcing of important operational functions as set forth by Article 19 of the PSD2 for payment institutions and the general rules on outsourcing laid down by the Capital Requirements Directive (CRD) and the Committee of European Banking Supervisors (CEBS) Guidelines on outsourcing for credit institutions, payment service providers remain fully responsible and accountable for fulfilling all the requirements set forth in these draft Guidelines regarding the assessment and notification of major incidents. Moreover, the competent authority in their home Member State always retains the right to address them directly at any time with the purpose of requesting additional information or clarifications.

Q8. Do you consider that the delegated reporting procedure proposed in the draft Guidelines will provide added value to the market? Please explain your reasoning.

28. Practical experience also shows that the delegation of reporting obligations is most commonly used by groups of payment service providers (be they legal groups or not) that rely on one common IT-group service centre or one common technical service provider offering them the same services / processes / infrastructures. In these cases, an incident at the level of the IT-group service centre or technical service provider typically affects all or a part of these payment service providers and does so in a similar way. Hence, and as confirmed by several jurisdictions, there are efficiency gains in having the notification of these incidents being carried out not only in a delegated manner, but also in a consolidated way. As a result, the designated third party may be able to generate and forward directly to the corresponding competent authority one single incident report on behalf of multiple payment service providers within the same Member State, as opposed to a collection of detailed individual reports.

29. In order to reflect this current practice to the extent possible, the draft Guidelines also offer payment service providers the possibility of making use of this consolidated reporting option. As a precondition, the draft Guidelines envisage that incidents arise in a technical service provider and affect several payment service providers that have their reporting obligations delegated on such third party. In this case, and as long as there are no divergences among the information related to the different payment service providers, the designated third party may be able to fill out one single report, specifying in the dedicated table of the template the list of payment service providers such report refers to. Nevertheless, as soon as a common reply valid for the different

payment service providers is no longer possible, the third party would have to provide -from then onwards- the corresponding divergent information on an individual basis for each payment service provider.

Q9. Do you consider that the consolidated reporting procedure proposed in the draft Guidelines will provide added value to the market? Please explain your reasoning.

30. Acknowledging the broad diversity of payment service providers, the draft Guidelines do not prescribe the way these market players should organise internally in order to ensure the assessment and notification of operational or security incidents along with the foreseen methodology and process. Instead, payment service providers are simply requested to ensure that their general operational and security policy clearly defines all the responsibilities and processes required to notify incidents under the scope of the PSD2.

31. Likewise, the draft Guidelines do not prescribe the way payment service providers should communicate with the competent authority in the home Member State, since this would be determined by each competent authority ensuring, inter alia, the availability and accessibility of the channels, the secure bilateral identification of the parties involved in the information exchange, the safeguarding of data confidentiality and integrity as well as the provision of the corresponding timestamping.

32. Although these draft Guidelines on classification and notification of incidents are exclusively addressed to payment service providers, they could also be used as a basis by other authorities when designing the incident reporting framework to be complied with by other addressees. In particular, central banks acting in their capacity of overseers of payment systems, schemes and instruments could consider applying these same or similar requirements for the reporting of operational or security incidents by the entities they oversee.

33. Sharing incident information with other domestic authorities is also relevant in order to ensure a coordinated approach when the consequences or the source of an incident fall within their remit. Moreover, it enables the pooling of experience and knowledge, thus facilitating the identification of good practices in responding to specific types of incidents and the decision-making process on the potential actions to be taken in each situation. The benefits of granting other domestic authorities access to such information are evidenced by the fact that this is nowadays a common practice among European supervisors and overseers alike, as the initial stock-taking exercise carried out among these national authorities had shown.

34. In order to gain a better insight into the various approaches taken across countries on the above practice, supervisors and overseers were approached for a second time requesting more detailed information. The results of this exercise revealed that incident-related information is often shared with domestic authorities, such as ministries, supervisory authorities or telecommunications authorities. Additionally, the questionnaire allowed identifying some best practices, such as the documentation of the routines for information exchange, including a description of what triggers the flow of information towards the different domestic authorities.

35. The input gained formed the basis for determining the criteria that should govern the sharing of incident-related information with other domestic authorities, in terms of the types of incident and the details thereof that should be provided. These criteria are to be seen as minimum requirements that do not preclude competent authorities from going further when deciding what, when and with whom to share such information. All of this has to be done bearing in mind the need to ensure that the required confidentiality and/or intellectual property rights are preserved at all times, as well as the integrity of the information and the proper authentication of the parties involved in the exchange.

36. These draft Guidelines also harmonise the reporting process envisaged in Article 96(2) between competent authorities in the home Member State and the EBA/ECB. The related requirements address the issue of which information to be further distributed and the way it should be transmitted. Considering that the more the information, the better positioned the EBA and the ECB are to decide on the interest of a given incident for other authorities, a maximalist approach has been followed. As a result, competent authorities should share with the EBA and the ECB all reports received on major operational or security incidents. Moreover, competent authorities could potentially decide to include in their notifications any additional documentation they may have received, and even share information on non-major incidents they may have been reported, should they consider them critical to other Union or national competent authorities (e.g. due to their potential geographical scope across the Union).

37. As regards the communication process, no specific channels are foreseen, since they will have to be agreed upon together with the EBA/ECB. Practical experience shows that secure e-mail and secure on-line document management systems are the most common channels, although others are also used due to the complexity of the content, the urgency of the notification, or the severity of the incident. All in all, the approach followed in the draft Guidelines aims at allowing an expedited and secure communication flow and ensuring full transparency, thus providing the EBA and the ECB with a fair picture of the circumstances surrounding the incident. As a result, both the EBA and the ECB will have a good basis for determining the relevance of such incident to other relevant Union and national authorities so as to ensure a timely and effective delivery of the required information.

38. In this regard, it should be noted that the voluntary cooperation among competent authorities is a principle embedded in the Union directives. As such, the competent authority in the home Member State could always consider the possibility of, in addition to notifying the EBA/ECB, directly forwarding incident-related information to a competent authority of a different Member State (i.e. to the competent authority of the host Member State) if a swifter communication is deemed necessary (e.g. where a payment service provider's main business happens to take place in the host Member State or when an incident particularly impacts a geography different from that of the home Member State).

39. The draft Guidelines are organised in three sets: the first set (Section 4) comprises Guidelines addressed to payment service providers on the classification of major operational or security incidents as well as on the content, the format (including standard notification templates) and the procedures for notifying such incidents to the competent authorities in their home Member State. The second set (Section 5) consists of Guidelines addressed to competent authorities, on the

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

40. Lastly, the third set (Section 6) of the draft Guidelines delineates the information to be shared with the EBA and the ECB in order to notify them those incidents they were reported about by payment services providers operating in their jurisdictions.

41. Together, these draft Guidelines will contribute to a consistent, efficient and effective implementation of the provisions of the PSD2 and foster supervisory convergence across Member States, in line with the EBA's overall objective of bringing about regulatory and supervisory convergence, as set out in Article 1(5) of Regulation (EU) No 1093/2010.

4. Draft Guidelines on incident reporting

EBA/GL-REC/20XX/XX

DD Month YYYY

Draft Guidelines

on incident reporting under the Payment Services Directive 2

1. Compliance and reporting obligations

Status of these Guidelines

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

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

Reporting requirements

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

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

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

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

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

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

10. These draft Guidelines apply also where the major operational or security incident originates outside the Union (e.g. when an incident impacts the services provided via a parent or a subsidiary established outside the Union) and affects, either directly or indirectly, the payment services provided by a payment service provider located in the Union.

Addressees

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

12. 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

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

Major operational or security incident	A singular event or a series of linked events which have or may have a material adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.
Integrity	The property of safeguarding the accuracy and completeness of assets (including data).
Availability	The property of payment-related services being accessible and usable upon demand by authorised clients.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Authenticity	The property of a source being what it claims to be.
Continuity	The property of an organisation being capable of delivering its payment-related services at acceptable predefined levels after disruptive incidents occur.
Payment-related services	Any business activity in the meaning of Article 4(3) of the PSD2, and all the necessary technical supporting tasks for the correct provision of the payment services.

3. Implementation

Date of application

14. These Guidelines apply from 13.01.2018.

4. Draft 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: Incident classification

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

a. *Transactions affected*

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

b. *Clients affected*

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

c. *Service downtime*

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

d. *Economic impact*

Payment service providers should determine the monetary costs associated to the incident holistically and take into account both the absolute figure and, when applicable, the relative importance of these costs in relation to the size of the payment service provider (i.e. to the payment service provider's Tier-1 capital).

e. *High level of internal escalation*

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

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

Payment service providers should determine the systemic implications the incident may have, i.e. its potential to spill over beyond the initially affected payment service provider.

g. *Reputational impact*

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

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

a. Transactions affected:

As a general rule, payment service providers should understand the regular level of payment transactions to be the daily annual average of payment transactions for all the payment services executed by the affected payment service provider, 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 Annex 1).

b. Clients affected

Payment service providers should take as the total number of clients the aggregated figure of clients contractually bound with them at the time of the incident or, alternatively, the most recent figure available, regardless of their size, the type of service they are benefiting from or whether they have been classified as active or passive.

c. Service downtime

Payment service providers 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 applicable.

d. 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 of contractual obligations, sanctions, external liabilities and lost revenues.

e. *High level of internal escalation*

Payment service providers should consider whether the incident is reported to the Chief Information Officer (or similar) outside any periodical notification procedure.

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

Payment service providers should assess, among other things, whether the incident could be replicated at other payment service providers, whether it could affect the smooth functioning of financial market infrastructures or whether it could compromise the solidity 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 stops fulfilling its obligations in the infrastructures it is a member of.

g. *Reputational impact*

Payment service providers should consider the level of visibility gained by the incident in the marketplace. At an initial stage, payment service providers should take into account whether as a result of the incident: i) client account data leaked or was stolen, ii) payment instruments and/or personalised security credentials were compromised, iii) regulatory obligations were missed, iv) sanctions were breached or v) the same type of incident has occurred before. In particular, payment service providers should consider the likelihood of the incident to cause harm to the society as a good indicator of its potential to impact their reputation. Payment service providers should also bear in mind later on other criteria such as the media coverage it has received (considering not only traditional media, such as newspapers, but also blogs, social networks, etc.) or whether the payment service provider has been put in a competitive disadvantage as a result of the incident.

1.3. Payment service providers should establish the materiality of an incident by determining, for each individual criterion, whether the relevant thresholds in Table 1 are met or surpassed.

Table 1: Thresholds

Criteria	Level 1	Level 2
Transactions affected	> 10 % of the payment service provider's regular level of transactions and > EUR 100,000	> 25 % of the payment service provider's regular level of transactions or > EUR 1,000,000
Clients affected	> 5,000 and	> 50,000 or

	> 10 % of the payment service provider's clients	> 25 % of the payment service provider's clients
Service downtime	> 2 hours	-
Economic impact	-	> 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) was called upon
Other payment service providers or relevant infrastructures potentially affected	Yes	-
Reputational impact	Yes	-

*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.

1.4. Payment service providers should resort to estimations should they not have actual data to support their judgments as to whether a given threshold is met or surpassed (e.g. during the initial investigation phase).

1.5. Payment service providers should classify as major those incidents that fulfil either i) one or more criteria at Level 2 or ii) three or more criteria at Level 1.

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).

Guideline 2: Notification process

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

2.2. Payment service providers should leverage the same template to inform the competent authority throughout the life of the incident (i.e. payment service providers should use the same template for initial, intermediate and final reports, as described in paragraphs 2.7 to 2.19). Payment service providers should complete the template in an incremental manner, on a best effort basis as more information becomes readily available in the course of their internal investigations.

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

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

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

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

Initial report

2.7. Payment service providers should submit an initial report to the competent authority in the home Member State when an incident is first detected.

2.8. Payment service providers should send the initial notification to the competent authority within the first 2 hours from the moment the incident was first detected, or if the reporting channels of the competent authority are known not to be available or operated at that time, as soon as they become available/operational again.

2.9. Payment service providers should also submit an initial report to the competent authority in the home Member State when a previous non-major incident becomes a major incident. In this particular case, payment service providers should send the initial notification 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/operated again.

2.10. Payment service providers should facilitate in their initial reports headline-level information, thus featuring some basic characteristics of the incident and its foreseen consequences based on the information available immediately after it was discovered or reclassified. Payment service providers should resort to estimations when actual data are not available. Payment service providers should also include in their initial report the date for the next update, which should be as short as possible and under no circumstance go beyond 3 business days.

Intermediate report

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

2.12. Payment service providers should brief the competent authority in these delta/intermediate reports about, at least, significant changes they have become aware of since the previous notification such as, e.g. whether the incident has escalated or decreased, new causes identified or actions taken to fix the problem. In any case, payment service providers should produce an intermediate report at the request of the competent authority in the home Member State.

2.13. As in the case of initial reports, payment service providers should make use of estimations when actual data are not available and indicate in each report the date for the next update, which should be as short as possible and under no circumstance should go beyond 3 business days.

2.14. Should the payment service provider not be able to comply with the estimated date for the next update, they should contact the competent authority in order to explain the reasons behind the delay, propose a new plausible submission deadline (no longer than 3 business days) and send a new intermediate report updating exclusively the information regarding the estimated date for the next update.

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

Final report

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

2.17. Payment service providers should deliver the final report to the competent authority in a maximum of 2 weeks 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 yet) should contact the competent authority before it has lapsed and provide an adequate justification for the delay, as well as a new estimated date for the final report.

2.18. Payment service providers should aim at including in their final reports full information, which comprises actual figures on the impact instead of estimations, and, 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.

2.19. Payment service providers should also send a final report when they identify that an already reported incident has been misclassified and does not, in fact, rank as a major incident. In this case, payment service providers should send the final report as soon as this circumstance is detected and, in any case, by the estimated date for the next reporting. In this particular situation, payment service providers should facilitate an explanation of the reasons justifying this downgrading.

Guideline 3: Delegated and consolidated reporting

3.1. Payment service providers wishing to delegate their reporting obligations under the PSD2 on a third party should inform the competent authority in the home Member State and ensure the fulfilment of the following conditions:

a. The designated third party is established in the Union.

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

c. The delegation complies with the requirements for the outsourcing of important operational functions as set forth by Article 19 of the PSD2 for payment institutions and the general rules on outsourcing laid down by the CRD and the CEBS Guidelines on outsourcing for credit institutions.

d. 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.

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

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

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

d. Ensure that when there are fields of the template where a common answer is not possible (e.g. sections 3, 5 and 8), the third party fills them out individually for each affected payment service provider, further specifying the identity of each PSP the information relates to.

e. Ensure that 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 contents thereof, but only to the extent possible so as to avoid any breach of confidentiality as regards the information that relates to other payment service providers.

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

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

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

Guideline 4: Operational and security policy

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

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

Guideline 5: Assessment of the relevance of the incident

5.1. Competent authorities in the home Member State should assess the relevance of an 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 a given incident:

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

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

Guideline 6: Information to be shared

6.1. Competent authorities should provide information about major operational or security incidents to other domestic authorities, as a minimum, at the time of receiving the initial report (or, alternatively, the report that prompted the sharing of information) and when they are notified that business is back to normal (i.e. last intermediate report).

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

- "Date of beginning and/or detection of the incident".
- "Estimated or actual date of recovery".

- "Short description of the incident (including non-sensitive parts of the detailed description)".
- "Short description of measures taken or planned to be taken to recover from the incident".
- "Description of how the incident could affect other PSPs and/or infrastructures".
- "Description (if any) of the media coverage".
- "Other impact (if relevant)".
- "Cause of incident (including root cause, if already known)".

6.3. Competent authorities should conduct proper anonymisation, as needed, and leave out any information that could be subject to confidentiality or intellectual property restrictions before sharing any incident-related information with other domestic authorities.

6.4. Competent authorities should at all times preserve the confidentiality and integrity of the information exchanged and their proper authentication towards other domestic authorities.

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

Guideline 7: Information to be shared

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

7.2. Competent authorities should forward the report to EBA/ECB following the deadlines and procedures established by the latter.

Guideline 8: Communication

8.1. Competent authorities should at all times preserve the confidentiality and integrity of the information exchanged and their proper authentication towards EBA/ECB.

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

Annex 1 – Reporting template for payment service providers

Major Incident Report					
1 - GENERAL DETAILS					
Type of report					
Type of report (*)	○ Individual		○ Consolidated		
Affected PSP					
PSP Name (*)					
PSP unique identification number, if applicable (*)					
PSP authorisation number, if applicable (*)					
Head of Group, if applicable (*)					
Home country (*)					
Country(ies) affected by the incident (*)					
Contact person (*)					
Contact email (*)					
Contact telephone (*)					
Reporting entity (if different from the affected PSP)					
Name (*)					
Unique identification number, if applicable (*)					
Authorisation number, if applicable (*)					
Contact person (*)					
Contact email (*)					
Contact telephone (*)					
Report details					
Date and time of the report (*)	DD/MM/YYYY, HH:MM				
Is this an update of a previous incident report ? (*)	YES ○	NO ○	If so: reference of such report		
Is this the final report (*)	YES ○	NO ○			
In case it is the final report, and the incident has been downgraded, please provide a short explanation					
What is the ETA for next update? (*)	DD/MM/YYYY, HH:MM				
2 - INCIDENT DISCOVERY					
Date and time of beginning of the incident, if known (*)	DD/MM/YYYY, HH:MM				
Date and time of detection of the incident (*)	DD/MM/YYYY, HH:MM				
If still ongoing, when is it expected to be over? (*)	DD/MM/YYYY, HH:MM				
Actual date and time of recovery of the incident, if applicable (*)	DD/MM/YYYY, HH:MM				
Who discovered the incident? (*) (1)		*If other, please explain:*			
Please, provide a short description of the incident (*)					
Incident status (*)	Detection ☐	Repair ☐	Restoration ☐		
	Diagnostics ☐	Recovery ☐	Closure ☐		
3 - INCIDENT CLASSIFICATION					
Overall impact	Integrity ☐	Confidentiality ☐	Continuity ☐		
	Availability ☐	Authenticity ☐			
Transactions affected (2)	Number of transactions affected	% of regular level	Value (in EUR)		
	Alternative figures, if applicable				
	Comments:				
Clients affected (3)	Total number of clients	As a % of total clients			
Service downtime (4)	Total service downtime	HH:MM			
Economic impact (5)	Direct costs (in EUR)	Indirect costs (in EUR)			
High level of internal escalation (6)	Describe the level of internal escalation of the incident, indicating if it triggered a crisis mode (or equivalent)				
Other PSPs or relevant infrastructures potentially affected (7)	Describe how this incident could affect other PSPs and/or infrastructures				
Reputational impact (8)	Describe how the incident could affect the reputation of the PSP (e.g. media coverage, whether there is a legal or regulatory infringement, whether the PSP has been put in a competitive disadvantage…)				
Other impact (specify)					
PSP internal classification of the incident, if applicable					
4 - INCIDENT DESCRIPTION					
Type of Incident	Operational ☐	Security ☐			
Cause of incident	Under investigation ☐				
	External attack ☐	→ Type of attack: Distributed/Denial of Service (D/DoS) ☐; Infection of internal systems ☐; Targeted intrusion ☐; Other ☐			
	Internal attack ☐				
	External events ☐	If Other, specify			
	Human error ☐				
	Process failure ☐				
	System failure ☐				
	Other ☐	If other, specify			
Was the incident affecting you directly, or indirectly through a service provider?	Directly ○	Indirectly ○	If indirectly, please provide provider's name		
Please provide a sufficiently detailed description of the incident (e.g.): - What is the specific issue? - How it happened? - How did it evolve? - Was it related to a previous incident? - Consequences (in particular for clients)					

5 - INCIDENT IMPACT						
Building(s) affected (Address), if applicable (*)						
Commercial channels affected (*)	Branches ☐ E-banking ☐		Telephone banking ☐ Mobile banking ☐ ATMs ☐		Point of Sale ☐ Other ☐	
	If Other, 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 services ☐ Account information services ☐ Other	
	If Other, specify:					
Functional areas affected (*)	Authentication/Authorisation ☐ Communication ☐		Clearing ☐ Direct settlement ☐		Indirect settlement ☐ Other ☐	
	If Other, specify:					
Systems and components affected (*)	Application / Software ☐ Database ☐		Hardware ☐ Network/infrastructure ☐ Other ☐			
	If Other, specify:					
6 - INCIDENT MITIGATION						
Which actions/measures have been taken or are planned to recover from the incident?						
Have Business Continuity Plans or Disaster Recovery Plans been activated?	*YES* ○		*NO* ○			
If so, when?	DD/MM/YYYY, HH:MM					
If so, please describe						
Is an investigation still ongoing?	*YES* ○		*NO* ○			
If still ongoing:						
When is it planned to be concluded?						
How is the incident investigated and what are the priorities?						
Please provide additional details, if needed						
Did the PSP had to cancel or weaken some controls because of the incident?	*YES* ○		*NO* ○			
If so, please explain						
7 - ROOT CAUSE ANALYSIS AND FOLLOW UP						
What was the root cause, if already known?						
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known						
8 - ADDITIONAL INFORMATON						
Has the incident been shared with other PSPs for information purposes?	*YES* ○		*NO* ○			
If so, please provide details						
Was a civil complaint filled against the PSP?	*YES* ○		*NO* ○			
If so, please provide details						

Notes:

(*) Mandatory fields
(1) Pull-down menu: client; internal organization; external organization; none of the above
(2) Pull-down menu: > 10 % of regular level of transactions and > EUR100,000; > 25 % of regular level of transactions or > EUR1M; none of the above
(3) Pull-down menu: > 5,000 and > 10 % clients; > 50,000 or > 25 % clients; none of the above
(4) Pull-down menu: > 2 hours; < 2 hours
(5) Pull-down menu: > Max (0,1 % Tier-1 capital, EUR200,000) or > EUR5,000,000; none of the above
(6) Pull-down menu: Yes; Yes, and crisis mode (or equivalent) was called upon; No
(7) Pull-down menu: Yes; No
(8) Pull-down menu: Yes; No

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

INSTRUCTIONS TO FILL OUT THE TEMPLATE

General details

Type of report:

Individual: the report refers to a single PSP.

Consolidated: the report refers to several PSPs making use of the consolidated reporting option. The fields under "Affected PSP" should be left blank (with the exception of the field "Country(ies) affected by the incident") and a list of the PSPs included in the report should be provided filling in the corresponding table (Consolidated report – List of PSPs).

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

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

PSP unique identification number: the relevant unique identification number used in each Member State to identify the PSP.

PSP authorisation number: Home Member State authorisation number, when applicable.

Head of Group: in case of groups of entities as defined in article 4(40) of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) 1093/2010 and repealing Directive 2007/64/EC, please indicate the name of the head entity.

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

Country(ies) affected by the incident: country/ies where the incident has materialised (e.g. several branches of a PSP located in different countries). It may or may not be the same as the Home Member State.

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

Contact email: email to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate e-mail.

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

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

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

Unique identification number: the relevant unique identification number used in each Member State to identify the entity that is reporting the incident, when applicable.

Authorisation number: Home Member State authorisation number, when applicable.

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

Contact email: email to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate e-mail.

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

Report details

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

Is this an update of a previous incident report?: in case there is a previous report on the same incident, please indicate the reference number of such communication, if available, which is the unique code issued by the competent authority at the first data record.

Is this the final report?: in case the incident is under control, business is back to normal and some root cause analysis has taken place, despite not having been addressed yet. At this stage, the PSP should have actual figures to replace any initial estimates. It may also be the final report in case the incident has been downgraded and does not qualify as major any longer.

In case it is the final report, and the incident has been downgraded, please provide a short description: given that the downgrade of an incident is envisaged as a special case of final report (e.g. it is reported as major and then reassessed and downgraded to non-major), the PSP is asked to provide some explanations on the reasons behind this reclassification.

What is the ETA for next update? Please, indicate the estimated time of arrival (ETA) for the submission of the next update.

Incident discovery

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

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

If still ongoing, when is it expected to be over?: approximate date (and time) when the open incident is expected to be solved.

Actual date and time of recovery of the incident, if applicable: when the incident is under control and business is back to normal, to be completed in the final intermediate report.

Who discovered the incident?: either a client, some other party from within the PSP (e.g. internal audit function) or an external one (e.g. external service provider). If it was none of those, please provide an explanation under "comments".

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

Status:

Detection: the incident has just been discovered.

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

Repair: the attacked items are being reconfigured.

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

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

Closure: the final step in the incident lifecycle, during which a user and an incident handler check that the service is fully available have been performed.

Incident classification

Overall impact

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

Availability: the property of payment-related services being accessible and usable upon demand by authorised clients.

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

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

Continuity: the property of an organisation being capable of delivering its payment-related services at acceptable predefined levels after disruptive incidents occur.

Transactions affected: percentage of payment transactions and/or total value (€) compromised. As a general rule, the regular level of payment transactions is the daily annual average of the previous year, for all the payment services executed by the affected payment service provider(s). If not representative enough, other figures could be used as a reference along with an explanation (if this is the case, please explain it under "Alternative figures" free format box). Additionally, the PSP is requested to provide the total number of transactions affected and its value in euros.

Clients affected: aggregated number and/or percentage of active and passive clients that have been impacted. The basis figure for calculation should be the number of clients bound contractually with the PSP(s) at the time of the incident (or the most recent figure available), regardless of their size and the type of service they are benefiting from. Additionally, the PSP is requested to provide information about the total number of clients affected and the actual percentage.

Service downtime: period of time while the service is not accessible or usable. PSPs should consider both the time intervals where a payment service provider is open for business as required for the execution of a payment services as well as the closing hours and maintenance periods, where applicable.

Economic impact: including any costs that can be directly or indirectly associated to the incident (expropriated funds/assets, replacement costs of hardware/software, other forensic or remediation costs, fees due to non-compliance of contractual obligations, sanctions, external liabilities, lost revenues, etc.). The PSP is requested to separately indicate the amount of direct and indirect costs.

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

High level of internal escalation: if the incident has been escalated to the executive officers of the organization (or the third party provider, in case of consolidated reporting), outside of any periodical reporting procedure. It should also be explained to what extent the incident was escalated, specifying further whether it triggered a crisis mode (or equivalent).

Other PSPs or relevant infrastructures potentially affected: whether other PSPs or infrastructures (e.g. payment systems) may be directly or indirectly impacted as a result of their business connections. The PSP is also requested to provide details as to whether the incident has the potential to be replicated at other PSPs, or affect the smooth functioning of financial market infrastructures or to compromise the solidity of the financial system as a whole, indicating as well any potential cross-border effects. 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, whether the payment service provider stops fulfilling its obligations in the infrastructures it is a member of.

Reputational impact: if the incident could undermine user's trust in the PSP and, more generally, in the underlying payment instrument, service or the market as a whole. Payment service providers should consider the level of visibility gained by the incident in terms of, e.g. clients' account data leaked/stolen, payment instruments and/or personalised security credentials compromised or recurrence of the same type of incident. In addition, the PSP should provide details on how their reputation has or could be impacted by considering, e.g. the scale of the media coverage of a given incident (taking into account not only

traditional media, such as newspapers, but also blogs, social networks, etc.), whether the incident itself represents or is likely to lead to any breaches of legal or regulatory obligations, or lead to the PSP to be taken to court or whether it has put the PSP in a competitive disadvantage).

Other impact (specify): please, indicate any other impact not covered in the previous lines.

PSP internal classification of the incident: for those cases were the PSP has internally classified the incident, please provide some information regarding this aspect, in particular which level it was assigned (e.g. major, significant, minor...).

Incident description

Type of Incident

Operational: incident stemming from inadequate or failed processes, people and systems or from acts of God that affect the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.

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

Cause of incident:

Under investigation: the cause has not been determined yet (it is acknowledged that in some cases the cause of the incident might not be known at an initial stage of the investigation).

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

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

Type of attack:

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

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

Targeted intrusion: unauthorized act of spying, snooping, and stealing information through cyber space.

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

ticked and details added in the free text field.

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

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

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 that support the payment activity.

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

Please provide a sufficiently detailed description of the incident: please, describe the main features of the incident, covering at least the points featured in the questionnaire (what specific issue the PSP is facing, how it started and evolved, possible connection with a previous incident and consequences, especially for customers).

Incident impact

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

Commercial channels affected

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

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

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

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

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

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

Payment services affected

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 client to provide cash and debit his/her payment account by the corresponding amount.

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

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

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

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

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

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

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.

Functional areas affected

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

Communication: flow of information for the purpose of identification, authentication, notification and information between AS PSP and PISP, AISP, payers, payees and other PSP.

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 and/or securities, 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 and/or securities, when this action is carried out by another PSP on behalf of the affected PSP.

Systems and components affected:

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

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

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

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

Incident mitigation

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

Have Business Continuity Plans or Disaster Recovery Plans been activated?: please, provide the most relevant details of these plans, if activated.

Is an investigation still ongoing?: describe whether the incident and its cause are still under investigation. Provide additional details as needed.

If still ongoing…

When is it planned to be concluded?: please, provide details as to the envisaged timetable for the complete

resolution if the incident (including its root cause).

How is the incident investigated and what are the priorities?: please, provide details about the underlying strategy and rationale followed when addressing the incident.

Did the PSP had to cancel or weaken some controls because of the incident?: please, provide details as to the underlying reasons justifying the weakening or cancelling of controls.

Root cause analysis and follow up

What was the root cause, if already known?: please, explain which is the root cause of the incident or, if it was not known yet, the preliminary conclusions drawn from the root cause analysis.

Main corrective actions/measures taken 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 (to be completed only in the final report).

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 and the underlying reasons.

Was a civil complaint filed against the PSP?: indicate whether the PSP has been taken to court as a result of the incident. The fact that a civil complaint is in progress, it does not mean that the incident cannot be solved

5. Accompanying documents

5.1. Draft cost-benefit analysis / impact assessment

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

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

A. Problem identification

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

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

[2] EBA: Consumer trends report (2016); EC: Green paper on retail financial services (2015)

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

To address these issues, these draft Guidelines on incident reporting specify the criteria for the classification of major operational or security incidents by payment service providers as well as the format and procedures they should follow to communicate such incidents to the competent authorities in the home Member State. In addition, the Guidelines determine the criteria that should govern the sharing of incident-relevant information between competent authorities and other domestic authorities and harmonise the reporting process between competent authorities and the EBA and the ECB.

B. Policy objectives

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

In general, the outlined Guidelines contribute to the EBA's objective of fostering regulatory and supervisory convergence and the development of a single market for payment services in the Union. They will contribute to a consistent, efficient and effective implementation of the provisions of the PSD2 and enhance supervisory convergence across Member States.[3]

More specifically, the framework proposed by these draft Guidelines could contribute to maintaining effective incident management procedures and establishing a common and consistent approach regarding the reporting process. The notification of other national authorities as well as the EBA and the ECB contributes to improving the assessment of the collective impact on the different stakeholders in the domestic and the Union payment service market. It further fosters a prompt reaction to incidents, the containment of potential spill-over effects and the prevention of future similar events. This hampers the negative impact of major operational and security incidents, which could affect the integrity, availability, confidentiality, authenticity and/or continuity of the services provided by the payment service provider. Therefore, the draft Guidelines help to ensure that the damage to users, other payment service providers or the payment systems from operational and security incidents is minimised.

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

[3] EBA: Annual report (2015) and 2017 work programme

C. Options considered and preferred option

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

In the preferred option, the Union-wide criteria and thresholds to determine whether an operational or security incident is major are defined. As summarized in Table 1 of Guideline 1 on incident classification, a combination of seven quantitative and qualitative criteria is retained. They are chosen based on most commonly used practices in the Member States. In general, they consider the magnitude and scope of the impact, the amount at risk, the impact on other payment service providers or other payment infrastructures and the reputational risk for the service provider. For the four quantitative criteria clear numerical threshold are defined. For the criteria *transactions affected* and *clients affected*, two threshold options are retained for two different levels. For the *duration* of the incident, a major incident is reached if the incident hinders operations for more than two hours. For the three qualitative criteria no single qualitative element currently seems to clearly dominate the landscape. However, *reputational impact* due to an incident is one of the main concerns in most Member States. A benchmark is reached if the qualitative criterion is triggered.[4]

Payment service providers should classify an incident as major if it fulfils either one or more criteria at Level 2 or at least three criteria at Level 1.

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

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

E. Cost-Benefit Analysis[5]

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

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

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

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

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

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

5.2. Overview of questions for consultation

Question 1: Do you consider the definitions included in the draft Guidelines to be sufficiently clear?

Question 2: Do you consider the criteria and methodology applicable for the assessment and classification of an incident as major to be sufficiently clear? If not, what should be further clarified?

Question 3: Do you consider that the methodology will capture all of / more than / less than those incidents that are currently considered major? Please explain your reasoning.

Question 4: In particular, do you propose to add, amend and/or remove any of the thresholds referred to in Guideline 1.3? If so, please explain your reasoning.

Question 5: Do you think that the information depicted in the template in Annex 1 is sufficient to provide competent authorities in the home Member State with a suitable picture of the incident? If not, which changes would you introduce? Please explain your reasoning.

Question 6: Are the instructions provided along with the template sufficiently clear and helpful to remove any doubts that could arise when completing the required fields? If not, please explain your reasoning.

Question 7: As a general rule, do you consider the deadlines and circumstances that should trigger the submission of each type of report (i.e. initial, intermediate and final) feasible? If not, please provide a reasoning and justify any alternative proposal.

Question 8: Do you consider I that the delegated reporting procedure proposed in the draft Guidelines will provide added value to the market? Please explain your reasoning.

Question 9: Do you consider that the consolidated reporting procedure proposed in the draft Guidelines will provide added value to the market? Please explain your reasoning**.**