POSITION PAPER

ESBG Response to the European Banking Authority public consultation on the revision of the Guidelines on major incident reporting under PSD2

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

EU Transparency Register ID 8765978796-80

December 2020

ESBG

ESBG Response to the European Banking Authority public consultation on the revision of the Guidelines on major incident reporting under PSD2

The European Savings and Retail Banking Group (ESBG) welcomes the opportunity to respond to this public consultation from the European Banking Authority on the revision of the Guidelines on major incident reporting under PSD2.

ESBG and its Members are highly supportive of the proposed revision. We especially welcome the fact that the amended Guidelines optimise the reporting templates and allow PSPs more time to report major incidents to National Competent Authorities. We also appreciate that the new reporting framework will avoid the reporting of minor incidents, thus shifting banks' time and resources on the really major ones. At the same time, ESBG and its Members would appreciate further clarity on the interpretation of some criteria and definitions and recommend the various reporting frameworks be further aligned. ESBG and its Members stand ready to further engage with the EBA in the weeks and months to come.

Instructions

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2. Comments are most helpful if they:

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

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 14.12.2020. Please note that comments submitted after this deadline, or submitted via other means may not be processed. The EBA is consulting for a shortened period of two-months because the EBA's review of the Guidelines resulted in most of the substantive parts of the requirements to be retained and because the majority of the amendments aim at optimising and simplifying the reporting process for reporting entities and national competent authorities.

Publication of responses

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

Data protection

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

Deadline for responses

14 December 2020.

Background and rationale

Background

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

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

To achieve this aim, Article 96(3) of PSD2 conferred a mandate on the EBA to develop, in close coordination with the ECB and after consulting all relevant stakeholders, including those in the payment services market, 'Guidelines in accordance with Article 16 of the EBA Regulation (EU) addressed to each of the following:
a) PSPs, on the classification of major operational or security incidents and on the content, the format, including standard notification templates, and the procedures for notifying such incidents;
b) competent authorities, on the criteria for how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities.'

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

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

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

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

Rationale

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

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

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

Type of incidents and criteria triggering a major incident report

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

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

- A large number of reported operational incidents appear to have a very low impact on the institution, with most of them related to failure of less significant tasks and single processes (e.g. further processing of batch-payments in net settlement systems, temporary glitches) without a significant impact on the PSP or its PSUs;
- Some of the security incidents appear not to be captured by the current criteria and thresholds; and
- The quantitative threshold for the absolute amount of the criterion 'Transactions affected' appears to have led to very uneven numbers between the operational and security incident reports, and in particular the threshold set for the higher impact level is too low for operational incidents.

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

Q1. Do you agree with the change proposed in Guideline 1.4 to the absolute amount threshold of the criteria 'Transactions affected' in the higher impact level?

Yes, we agree.

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

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

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

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

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

Q2. Do you agree with the changes proposed in Guideline 1.4 to the assessment of the criteria 'Transactions affected' and 'Payment service users affected' in the lower impact level, including the introduction of the condition that the operational incidents must have a duration longer than one hour?

Yes, we agree with the increase of the threshold and the duration longer than 2 hours for the operational incidents. At the same time, we would welcome further clarification and examples of the cases where "issues affecting the initiation and/or processing of transactions may be rectified within a period shorter than one hour but the overall unavailability of the PSPs' services to the payment service user is longer than two hours".

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

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

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

Yes, we agree. At the same time, we would also welcome some clarification on how and when PSPs should consider that the criterion "Breach of security measures" is triggered. Would this be at the same level as in ECB's cyber incident reporting?

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

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

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

The EBA also observed that the criteria 'High level of internal escalation' and 'Reputational impact' are often being met and subsequently reported together. The EBA considered that this may be due to the fact that these criteria are usually consequential to other criteria being triggered, they can be triggered by institutions that are erring on the safe side and they are very subjective. In order to provide greater clarity on when these criteria should be used, the EBA proposes minor amendments to the description of these criteria in Guideline 1.3 and the examples provided in the Annex to the Guidelines.

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

Deficiencies in the reporting process

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

a) The use of different variations of the templates specified in the Annex to the Guidelines, which does not allow the EBA, the ECB and some CAs to assess efficiently the reported incidents;
b) PSPs submitting the three different reports (initial, intermediate and final) related to the same incident separately, although the Guidelines are explicit that the reports should be submitted in an incremental manner and with the template provided in the Annex to the guidelines;
c) PSPs not respecting the deadlines for submission of the different incident reports;
d) PSPs not populating the template for incident reporting exhaustively;
e) PSPs not providing sufficient details related to the incident;
f) PSPs not updating information provided with previous reports;
g) PSPs not informing CAs about the reclassification of the incident from major to non-major (around 16% of the reported incidents have been downgraded but were not subsequently re-classified from 'major' to 'non-major');
h) Lack of reporting of incidents affecting services that have been outsourced to third parties; and
i) Insufficient information provided when the reporting to CAs has been delegated.

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

- In relation to 23(a) - the introduction of a standardised file containing the templates in the Annex to the Guidelines and this template to be made publicly available by the EBA on its website. The change was reflected in Guideline 2.1.
- In relation to 23(b) - clarifications on the requirement to submit the reports in an incremental manner, namely that it requires submitting the reports related to the same incident sequentially and that each report should contain the previous reports related to the same incident (e.g. when submitting the intermediate report, the PSP should also include a [updated] initial report). In other words, the template for incident reporting should contain the incident report and all previously submitted reports related to the same incident. These changes were reflected in Guidelines 2.2.
- In relation to 23(c) - simplification of the incident reporting process, by removing the obligation for PSPs to provide updates to the intermediate reports every 3 working days, extended the deadline for the submission of the final report from 2 weeks to 20 working days, and optimised the reporting template to ease the burden to PSPs. The EBA also clarified that the 4-hour deadline for submission of the initial report as required under Guideline 2.7 applies from the moment of classification of the incident (and not the detection of the incident).
- In relation to 23(d) - a clarification in Guideline 2.1 that all fields of the templates should be populated.
- In relation to 23(e) - a clarification as to what type of information is expected to be provided in some of the fields of the notification template in the Annex to the Guidelines, including by extending the examples given, and the introduction of specific fields requesting information that is requested under the fields with general details (e.g. information of the impact of the incident in other Member States).

- In relation to 23(f) - a clarification that the previously reported information should be updated, if applicable, and the introduction of fields specifying the changes made to the previously submitted reports related to the same incident. The main changes were introduced in Guidelines 2.2 and 2.12, as well as by introducing additional fields in the notification template in the Annex to the Guidelines.
- In relation to 23(g) - a further explanation that any re-classification of an incident from major to non-major should be communicated to the competent authority in line with the requirement of Guideline 2.21 and without undue delay.
- In relation to 23(h) - a clarification in the scope of the Guidelines that they apply also to major incidents affecting functions outsourced by payment service providers to third parties and that these incidents should also be communicated from PSPs to CAs.
- In relation to 23(h) - a clarification that each PSP should ensure that, when an incident is caused by a disruption in the services provided by a technical service provider (or an infrastructure) that affects multiple PSPs, the delegated reporting should refer to the individual data of the PSP, except in the case of a consolidated reporting. The clarification was introduced with a new Guideline 3.6.

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

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

Yes, we agree.

Q5. Do you support the introduction of a standardised file for submission of incident reports from payment service providers to national competent authorities? If so, what type of structured file format would you support (e.g. "MS Excel", "xbrl", "xml") and why?

Since major incident reporting is a manual process, we are satisfied with the current solution. As of the current process, other formats than MS Excel are therefore not relevant. However, if further standardisation of files for submission would lead to possible automation possibilities, we would be open for discussing the introduction of more efficient tools and approaches as well.

Simplification of the notification process and changes to the reporting templates

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

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

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

In addition, to ensure transparency of the process and better link between the different reports related to the same incident, the CP proposes to introduce a requirement for CAs in Guideline 2.7 to acknowledge the receipt of the initial report and assign a unique reference code unequivocally identifying the incident. Competent authorities will have discretion at national level to decide on the format of said reference code and will be required to include as prefix the 2-digit ISO code3 of their respective Member State when sharing the incident with the EBA and the ECB, to ensure uniqueness of the code at EU level.

Q6. Do you agree with the proposed changes to Guidelines 2.4, 2.7, 2.12, 2.14, and 2.18 that are aimed at simplifying the process of reporting major incidents under PSD2?

Yes, we agree. In addition, we would appreciate a further explanation on the meaning of the following expression: "the 4-hour deadline for submission of the initial report as required under Guideline 2.7 applies from the moment of classification of the incident (and not the detection of the incident). We would especially encourage a more detailed definition of "classification".

The EBA observed that PSPs do not populate some of the fields of the reporting templates. In addition, after assessing the information provided in those fields, the EBA arrived at the view that some information has little added value and is of limited use for supervisors. To that end, the EBA

proposes that the below fields should be removed from the reporting templates and, thus, the respective information no longer be requested from PSPs:

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

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

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

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

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

- 'Malicious code';
- 'Information gathering';
- 'Intrusions';
- 'Distributed/Denial of Service attack (D/DoS)';

- 'Deliberate internal actions';
- 'Deliberate external physical damage';
- 'Information context security'; and
- 'Fraud'.

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

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

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

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

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

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

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

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

Overall, we agree. We are supportive of the proposed categories and sub-categories of incidents and the terminology used. Nevertheless, we do not consider that the terms and categories are well defined. Indeed, a relevant part of the definitions provided by the EBA is based on examples (e.g. see page 45 of the Consultation Paper). We believe it is necessary that the EBA provides more precise and unambiguous definitions in order to make sure incidents are properly categorized in practice. Additionally, we think there is a need for further clarifications:

• On the exact scope of the sub-category "Information context security".
• Regarding the above-mentioned Point d.) of Deficiencies in the reporting process: We understand that the requirement is not to leave any fields blank in the report. In case the respective field does not apply or is not relevant for the article – is there a preference how to indicate that (eg: n.a/u.a.)? Otherwise, we suggest to add said option to the list.

We would also like to propose to make optional the field "Assessment of the effectiveness of the actions taken" in the template of the final report. It is very time consuming to get the requested information on time and this may entail the inability/impossibility to respect the deadline.

Finally, financial institutions are obliged to be compliant to various reporting obligations, e.g. the "ECB Reporting for significant cyber incidents" reporting scheme. Each reporting obligation is using different classification schemes of incidents, which makes it difficult to reflect in incident management processes and tools. Further harmonisation between the EBA and ECB reporting obligations would be highly appreciated.

Other general observations

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

In accordance with Guideline 2.21, all incidents that have initially been classified as major but at some point during the lifetime of the incident have stopped fulfilling the criteria of the Guidelines should be reclassified as non-major and the PSP should subsequently submit a final report to their NCA. The outcome of the assessment showed that 27% of the reported major incidents have been or should have been reclassified by PSPs to non-major at some point during the lifetime of the incident. The EBA considered these 27% to be within the expected margin of reclassified incidents, especially taking into account that the GL on major incident reporting require incidents that can probably reach the thresholds of the criteria also to be reported. However, EBA would like to highlight that PSPs that do not reclassify major incidents to non-major are in breach of the Guidelines.

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

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

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

About ESBG (European Savings and Retail Banking Group)

The European Savings and Retail Banking Group (ESBG) represents the locally focused European banking sector, helping savings and retail banks in 21 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 885 banks, which together employ 656,000 people driven to innovate at 48,900 outlets. ESBG members have total assets of €5.3 trillion, provide €1 trillion in corporate loans, including to SMEs, and serve 150 million Europeans seeking retail banking services. ESBG members commit to further unleash the promise of sustainable, responsible 21st century banking. Learn more at www.wsbi-esbg.org.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ■ B-1000 Brussels ■ Tel: +32 2 211 11 11 ■ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ■ www.wsbi-esbg.org

Published by ESBG. December 2020.