Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

# Comments

## EBA consultation paper on the draft revised Guidelines on major incident reporting under PSD2 (14 October 2020)

Contact:

Berit Schimm

Telephone: +49 30 2021-2111

Telefax: +49 30 2021-19 2100

E-mail: b.schimm@bvr.de

Berlin, 14. December 2020

Coordinator:
National Association of German
Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefon: +49 30 2021-0

Comments: EBA consultation paper on the draft revised Guidelines on major incident reporting under PSD2 (14 October 2020)

*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?:*

We support the proposed increase of the absolute threshold. Focus on relative thresholds appears to be more sensible and meaningful (analogous to the internal classification of incidents).

*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?:*

The condition "or" instead of "and" in the lower impact level leads to a significant tightening of the reporting situation. A purely percentage-based approach without an absolute lower impact level leads to an increase in the number of reports with low relevance and thus to disproportionate additional work for payment service providers and their IT service providers. Even short-term production restrictions during off-peak hours will become subject to reporting - depending on the number of customers affected. We therefore strongly advise against the proposed change in the criteria for affected customers and affected transactions. Otherwise, we would suggest the deletion of the absolute thresholds.

The inclusion of the criterion "duration of the incident >1h" does not contribute to the relief either. From the point of view of the customers it is not the operational incident time that is important but the "service downtime". The separation between "duration of the incident" and "service downtime" is therefore not defined or equal in many institutions. We therefore suggest deleting the criterion of "operational downtime" or at least replacing it with "service downtime" and providing for a uniform duration of > 2 hours.

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

We support the use/introduction of clearly quantifiable values/criteria. However, the criterion "breach of security measures" does not meet this requirement, as it is not clear for us. With regard to the impact on "availability", it leads to a redundancy with the criteria "affected transactions" and "affected customers". As a result, the violation of both criteria at the lower thresholds leads to reports whose content does not represent a material incident.

Another redundancy results from the criterion "High level of internal escalation", as the violation of security measures is regularly accompanied by a high internal escalation level. The target of receiving fewer operational reports is missed with this change. We expect an opposite effect. In addition, the relevant reports get lost in this point. Therefore the criterion should not be applied.

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

In view of the current draft regulation on cyber resilience (DORA) and the expected transfer of major incident reporting into DORA regulations, the question arises of the goal of revising the Guideline on Incident Reporting at this point of time. At least, it must be ensured that the rules defined in DORA and in the revised guidelines are coordinated with each other or that the requirements defined in the Guidelines are included in DORA.

Note: The reporting credit institutions should receive feedback if a report is incorrect.

Comments: EBA consultation paper on the draft revised Guidelines on major incident reporting under PSD2 (14 October 2020)

*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?:*

Existing national solutions for reporting must be maintained. Otherwise, there will be a high, short-term adaptation effort, which is to be expected again with DORA.

In principle, a standardised format makes sense in order to enable machine processing. Here, service provider independent (XML) formats and formats of standard applications (here: MS-Excel) are to be preferred. These formats have proven themselves in practice. They allow the necessary flexibility across all reporting institutions.

*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?:*

2.4: No comments.

2.7: We support the specification "after classification as major incident" instead of "after detection".

2.12: In our opinion, this regulation is not a simplification: In our view, an interim report should be provided when:

- the service has been restored (incident resolved, problem still exists)
- a downgrade from higher impact level to lower impact level or an escalation from lower level to higher level took place or
- the supervisor explicitly requests an interim report.

2.14: No comments.

2.18: We welcome the time relief.

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

Existing templates must be retained, as otherwise there will be an adaptation effort that is to be expected again with DORA (see answer 5). Many mandatory fields are defined in the new template, but it is not always possible to fill in all the newly proposed items (especially for the initial or interim report). Fields must also be able to be filled in as N/A or left blank.