European FinTech Association

Consultation Input on the revision of the **Guidelines on Major Incident Reporting** under PSD2

Executive Summary/ Introduction

The European Banking Authority (EBA) launched a public consultation to propose revising the Guidelines on major incident reporting under the Payment Service Directive (PSD2). The proposal aims at optimising and simplifying the reporting process, capturing additional relevant security incidents, reducing the number of operational incidents that will be reported, and improving the meaningfulness of the incident reports received. The revision of the Guidelines also intends to decrease the reporting burden on payment service providers (PSPs).

EFA members being active as PSPs under PSD2 and especially members of the Payments Working Group of EFA have shared the following input with the EBA by means of the online formular on **December 14, 2020.** The document on hand was attached and will be published on our EFA website.

Response details (questions refer to EBA Consultation Paper)

QUESTION 1: 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, the European FinTech Association (EFA) welcomes the increase of the quantitative threshold used for the higher impact level with respect to the criterion "transactions affected" from 5 million to 15 million.

QUESTION 2: DO YOU AGREE WITH THE CHANGES PROPOSED IN GUIDELINE 1.4 TO THE ASSESSMENT OF THE CRITERIA 'TRANSACTIONS AFFECTED' AND 'PAYMENT SERVICE USERS AFFECTED' IN THE LOWER IMPACT LEVEL, INCLUDING THE INTRODUCTION OF THE CONDITION THAT THE OPERATIONAL INCIDENTS MUST HAVE A DURATION LONGER THAN ONE HOUR?

We agree that the introduction of the condition that the operational incidents must have a duration of longer than one hour may help ensure that only operational incidents with a significant impact are being captured by the reporting requirement.

At the same time, however, the proposed amendment to use the percentage and the absolute amount thresholds as alternatives (instead of being cumulative conditions) may have the opposite effect, bringing into scope again certain operational incidents without a significant impact (even if they have a duration of more than hour). This is especially true for the thresholds used with respect to the criterion "payment service users affected", which have not been increased in the proposed revised guidelines: while an incident may or may not reach the threshold of 10% of PSUs being affected, for payment institutions of a certain size it almost always reaches the threshold of 5,000 PSUs affected. As a result, those payment institutions may need to report incidents that – given the relative size of the payment institution and its user base, and despite a duration of more than one hour – may not have a significant impact. We would therefore suggest to keep the percentage and the absolute amount thresholds as cumulative conditions.

QUESTION 3: DO YOU AGREE WITH THE INCLUSION OF THE NEW CRITERION 'BREACH OF SECURITY MEASURES' IN GUIDELINES 1.2, 1.3 AND 1.4?

We agree with the inclusion of the new criterion "breach of security measures" provided that the final revised guidelines keep the clarification 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. That clarification is required to allow for a timely internal assessment of the incident against the guidelines.

QUESTION 4: DO YOU AGREE WITH THE PROPOSED CHANGES TO THE GUIDELINES AIMED AT ADDRESSING THE DEFICIENCIES IN THE REPORTING PROCESS?

Yes, we agree with those proposed changes.

QUESTION 5: DO YOU SUPPORT THE INTRODUCTION OF A STANDARDISED FILE FOR SUBMISSION OF INCIDENT REPORTS FROM PAYMENT SERVICE PROVIDERS TO NATIONAL COMPETENT AUTHORITIES? IF SO, WHAT TYPE OF STRUCTURED FILE FORMAT WOULD YOU SUPPORT (E.G. "MS EXCEL", "XBRL", "XML") AND WHY?

Yes, we support the introduction of a standardised file for submission of incident reports. In terms of type of structured file format, there is a preference among our members for MS Excel.

QUESTION 6: DO YOU AGREE WITH THE PROPOSED CHANGES TO GUIDELINES 2.4, 2.7, 2.12, 2.14, AND 2.18 THAT ARE AIMED AT SIMPLIFYING THE PROCESS OF REPORTING MAJOR INCIDENTS UNDER PSD2?

Yes, we agree with those proposed changes.

QUESTION 7: DO YOU AGREE WITH THE PROPOSED CHANGES TO THE TEMPLATES IN THE ANNEX TO THE GUIDELINES?

We generally agree with the proposed changes. However, with respect to the categorisation of the causes of incidents and in particular the category "malicious action" , we are of the view that the sub-category "fraud", as it is currently defined, may overlap with other sub-categories of malicious action. For instance, phishing (currently included in the definition of fraud) could also be said to fall within the sub-category "information gathering". We would therefore suggest to refine the definition of fraud so as to make it clear that the sub-category refers to fraud in a strict sense, i.e. an unauthorised use (e.g. unauthorised use of resources, copyright infringements) rather than to an activity that could be said to also fall within another sub-category (e.g. phishing).

European FinTech Association a.s.b.l., Brussels, December 14th, 2020
Contact: Payment Working Group Lead: Brigit Carroll (brigit.carroll@transferwise.com, +32 483 07 11 93)