

EUROPEAN COMMISSION

Directorate-General for Financial Stability, Financial Services and Capital Markets Union

Director General

Brussels,
FISMA-D3/

Mr. Andrea Enria
Chairperson
European Banking Authority
One Canada Square (Floor 46)
Canary Wharf
London E14 5AA
United Kingdom

Subject: Commission intention to amend the draft regulatory technical standards on strong customer authentication and common and secure open standards of communication submitted by the EBA in accordance with Article 98(4) PSD2

Dear Mr. Enria,

Thank you for submitting to the Commission the draft regulatory technical standards (“the RTS”) on strong customer authentication and common and secure open standards of communication in accordance with Article 98(4) of Directive (EU) 2015/2366 (Payment Services Directive – PSD2).

I wish to inform you that acting in accordance with the procedure set out in Article 10(1) of Regulation (EU) No. 1093/2010 establishing a European Supervisory Authority (European Banking Authority), the Commission intends to amend Chapters 1, 3 and 5 of the draft RTS presented by the EBA.

The substantive changes envisaged by the Commission relate to the following issues:

1. Independent auditing of the security measures in case when transaction risk analysis exemption is applied (Ref. Chapter 1, Art. 3(2) of the EBA draft)

The proposed change is based on the following reasoning. The transaction risk analysis exemption from strong customer authentication under Article 16 of the draft you presented relies heavily on the sophisticated risk analysis methodology. Therefore an audit of this methodology, of the risk model and of the reported fraud rates should be performed by statutory auditors to ensure objectivity in the application of this exemption between different providers, independent verification of the conditions imposed by the RTS and a good quality of the reported data.

2. New exemption to strong customer authentication for certain corporate payment processes (Ref. Chapter III, NEW Article 17)

The proposed change is based on the following reasoning. While we concur with your views in relation to the application of the security measures of the RTS to all corporate payments, we have included a new exemption to the application of strong customer authentication concerning certain corporate payments when they use dedicated payment processes or protocols in the cases where, due to the specificity of such solutions and the level of security achieved by them, the competent authorities can establish that those processes or protocols achieve the high levels of security of payments aimed for by PSD2.

3. Fraud reporting by payment service providers directly to EBA (Ref. Chapter III, Articles 16(2) and 17(2) of the EBA draft)

The proposed change is based on the following reasoning. In accordance with Article 32 of the draft RTS you provided, the EBA should be able to conduct a review of the fraud rates defined under Article 16 and reported in accordance with Article 17. In order to do so effectively, the EBA should not only rely on the high-level, aggregated data reported by competent authorities in accordance with Article 96(6) of PSD2, but should also have access to the individual fraud data and reports from the payment service providers.

4. Contingency measures in case of unavailability or inadequate performance of the dedicated communication interface (Ref. Chapter 5, Article 28 of the EBA draft)

The proposed change is based on the following reasoning. The RTS shall ensure that an unavailability or inadequate performance of the dedicated interface does not prevent payment initiation services and account information services providers from offering their services to the users, where at the same time the user-facing interfaces operate without any difficulties and allow the bank to offer its own payment services.

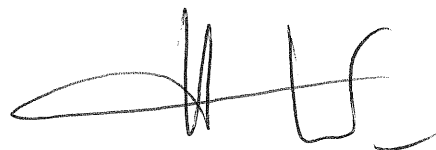
In case of unavailability or inadequate performance of the dedicated communication interface, banks should offer secure communication through the user-facing interfaces as a contingency measure. Relevant provisions of PSD2 (Articles 65-67) should apply, including identification and authentication procedures. Payment initiation services and account information services providers should in particular comply with their obligations under Articles 66(3) and 67(2) of PSD2.

The use of the contingency measures should be fully documented and reported to the authorities by the relevant providers, upon request, including justification for the use of these measures. Once the dedicated interface is restored to full service, payment initiation services and account information services providers should be obliged to use it.

The text of the draft RTS with the amendments intended by the Commission is attached to this letter. As the Legal Service of the Commission did not get the opportunity to perform an early legal review of the EBA draft prior to the official submission of the text, this version contains not only the substantive changes described above, but also numerous improvements to the legal drafting, editorial changes, such as changes in the order of some paragraphs and articles (including changed numbering), as well as some additional clarifications on the text in the recitals and explanatory memorandum.

I look forward to your reply to this letter, in accordance with the procedure foreseen in the EBA Regulation.

Yours sincerely,

A handwritten signature in black ink, consisting of a large, sweeping initial 'O' followed by a series of vertical and horizontal strokes that form the letters 'G' and 'U'.

Olivier Guersent