EBA/Op/2017/09

29 June 2017

Opinion of the European Banking Authority

on the European Commission's intention to partially endorse and amend the EBA's final draft regulatory technical standards on strong customer authentication and common and secure communication under PSD2

Introduction and legal basis

On 22 February 2017, the European Banking Authority (EBA) submitted for endorsement to the European Commission the final draft regulatory technical standards (RTS) under Article 98 of Directive (EU) 2015/2366[1] (PSD2).

The RTS establish the requirements for strong customer authentication (SCA) to be complied with by payment service providers (PSPs), the exemptions from the application of SCA, the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials, and the requirements for common and secure open standards of communication (CSC) between account servicing payment service providers (ASPSPs), payment initiation service providers (PISPs), account information service providers (AISPs), payers, payees and other PSPs.

By letter dated 24 May 2017, the Commission, acting in accordance with the procedure set out in the fifth and sixth subparagraphs of Article 10(1) of Regulation (EU) No 1093/2010[2], informed the EBA that it intends to partially endorse the RTS with amendments.

The EBA's competence to deliver an opinion on the Commission's proposed amendments to the RTS is based on the sixth subparagraph of Article 10(1) of Regulation (EU) No 1093/2010.

[1] 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 (OJ L 337, 23.12.2015, p. 35).

[2] 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).

In accordance with Article 14(5) of the Rules of Procedure of the Board of Supervisors[3], the Board of Supervisors has adopted this opinion.

General comments

The Commission has communicated its intention to amend Chapters 1, 3 and 5 of the draft RTS presented by the EBA. The letter details four substantive changes and 'numerous improvements to the legal drafting, editorial changing … as well as some additional clarifications on the text in the recitals and explanatory memorandum'.

a. the Commission proposes that the audit performed in relation to the exemption based on using transaction risk analysis should be performed by statutory auditors (Article 3(2) of the draft RTS as amended by the EBA);

b. the Commission proposes adding an exemption to strong customer authentication for certain corporate payments when they use dedicated payment processes or protocols (new Article 17 of the draft RTS as proposed by the Commission);

c. the Commission proposes that, in relation to the use of exemptions to strong customer authentication, payment service providers should report the outcome of their monitoring and the methodology used to calculate the fraud rate under the exemption based on using transaction risk analysis to the EBA, in addition to reporting this information to the national competent authorities (Articles 18(3) and 20(2) of the draft RTS as amended by the EBA);

d. the Commission proposes that, in case of the unavailability or inadequate performance of a dedicated interface, AISPs and PISPs should be allowed to access information using the customer interface (Article 33 of the draft RTS as proposed by the Commission).

With regard to the 'numerous improvements to the legal drafting' to which the Commission letter refers, the EBA would like to address a small number of changes that the EBA believes affect the substance of the RTS and that are outlined in the section 'Specific comments' below.

By way of a general response, the EBA would like to reiterate that the RTS that were submitted had to balance a number of competing objectives of PSD2, including enhancing security, promoting competition, ensuring technological and business-model neutrality, contributing to the integration of payments in the EU, protecting consumers, facilitating innovation and enhancing customer convenience. Following an extensive consultation process in 2016, the EBA made a number of changes to the substance, and therefore also to the balances and trade-offs, of the RTS it had initially proposed, before submitting the final draft to the Commission in February 2017.

[3] Decision adopting the Rules of Procedure of the European Banking Authority Board of Supervisors of 27 November 2014 (EBA/DC/2011/01 Rev4).

The EBA would also like to point out that the RTS have remained controversial since the EBA submitted them; there has been continued lobbying from various market participants, in particular with regard to the Commission's proposal to change the RTS in terms of AISPs and PISPs accessing customer information.

Finally, the EBA notes that, as reflected in recital 23 to Regulation (EU) No 1093/2010 (the EBA Regulation), it was the intention of the EU legislators that technical standards would be subject to amendment by the Commission if they were incompatible with Union law, did not respect the principle of proportionality or ran counter to the fundamental principles of the internal market for financial services as reflected in the *acquis* of Union financial services legislation. The EBA is of the view that some of the suggested amendments as currently drafted are not prompted by one of those circumstances.

Specific proposals

a. The Commission proposes that the audit performed in relation to the exemption based on using transaction risk analysis should be performed by statutory auditors (Article 3(2) of the draft RTS as amended by the EBA)

The EBA notes that the Commission does not propose to change the essence of the principle laid down in Article 3(2) of the EBA draft but proposes to specify that a 'statutory' audit, rather than any audit, must be performed. The EBA also notes that the Commission has added a reference to 'statutory' auditors to Article 3(1) of the revised draft RTS.

The EBA understands that the Commission's motivation for the change is to ensure the independent nature of the audit, and that the auditor has the qualifications and expertise required to perform the audit in the context of the transaction risk analysis exemption.

The EBA does not disagree with the motivation for the proposed change and had, in the RTS that it submitted on 22 February, highlighted that auditors should be qualified and independent, whether they were internal or external auditors.

However, the EBA is of the view that requiring a 'statutory' audit might be confusing and misleading for the following reasons:

- The existing practices with regard to auditors vary greatly within the EU. As highlighted in the many responses received on this topic during the EBA's consultation exercise, the use of statutory auditors may differ between Member States.

- The purpose of statutory audits in EU regulation is to certify financial statements. However, the purpose of the audit in the context of Article 3 of the draft RTS is of a very different nature, focusing on security. Requesting a statutory audit may therefore not ensure that auditors have the qualifications and expertise required to carry out the audit sought under Article 3.

In addition, not all PSPs are currently required to perform a statutory audit. For instance, a number of Member States exempt small payment institutions and credit unions from doing so, or do not require them to do so. The amendment proposed by the Commission would therefore impose a new statutory requirement for these providers and would appear to be incompatible with PSD2, which refers in Article 5(1)(o) to statutory audits 'where applicable'.

This flexibility allowed for in Level 1 was reflected in the wording of Article 3(2) of the RTS that the EBA submitted on 22 February, which stated that 'the period between the audit reviews … shall be determined taking into account the relevant accounting and statutory audit framework applicable to the payment service provider'. The same Article also imposed a yearly review for PSPs making use of the transaction risk analysis exemption.

The Commission's proposal to impose an additional requirement on PSPs that are currently either exempt or not required to carry out statutory audits may also be disproportionate and very costly for a number of small institutions.

Finally, the EBA is of the view that, while the independence of any auditor cannot be guaranteed, imposing an external audit on the assumption that internal auditors would not be independent does not reflect existing regulations and industry standards for internal auditors, which aim to ensure their independence.

In conclusion, the EBA is of the view that the use of 'statutory', and the limitation to external auditors in the case of the review of the transaction risk analysis exemption, is unlikely to ensure and guarantee the quality and independence of the audit that the Commission aims to achieve and may also impose disproportionate new requirements on a number of PSPs.

However, the EBA agrees with the Commission on the importance of the audit being independent and conducted by auditors with the appropriate expertise. The EBA therefore suggests a number of changes and clarifications to the Commission's proposal, by replacing in Article 3(2) 'statutory audit' with 'an audit performed by an auditor with expertise in IT security and payments and operationally independent within or from the payment service provider'. The EBA also suggests introducing a requirement for an external audit to be carried out during the first year of the PSP 's use of the exemption and at least every three years thereafter, and whenever requested by the competent authority. The EBA is of the view that these changes address the issue identified by the Commission and do so without introducing a new and potentially disproportionate requirement in the RTS.

The EBA similarly suggests replacing the reference to 'statutory auditors' in Article 3(1) with 'auditors with expertise in IT security and payments and operationally independent within or from the payment service provider'.

b. The Commission proposes adding an exemption to strong customer authentication for certain corporate payments when they use dedicated payment processes or protocols (new Article 17 of the draft RTS as proposed by the Commission)

The Commission proposes adding a new exemption for certain corporate payments when they use dedicated payment processes or protocols on the basis of the specificity of such solutions. The proposed exemption reads as follows: 'Payment service providers shall be allowed not to apply strong customer authentication in respect of legal persons initiating electronic payment transactions through the use of dedicated corporate payment processes or protocols, where the competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security to those aimed for by Directive 2015/2366'.

The EBA understands the exemption as focusing on specific existing practices involving business-to-business and machine-to-machine payment transactions using specific protocols, rather than as an exemption for all corporate transactions.

The EBA also understands that the motivation for the Commission's proposal was the assumption that the specific types of corporate payments referred to in the suggested amendment were of a less risky nature.

With regard to corporate payment transactions generally, and following the consultation with market stakeholders in 2016, the EBA assessed if corporate payment transactions should be exempted from the obligation of carrying out SCA but rejected the proposal on the grounds that there was no reliable evidence to suggest that all corporate transactions were low risk and that there were already a number of exemptions under the RTS and exclusions under PSD2 (in particular the limited network exemption) that would cover many corporate transactions.

At the time, the EBA did not consider exempting only specific types of corporate transactions.

The EBA understands from a number of responses by market players to the consultation conducted in 2016 that many protocols may not be able to comply with SCA given the way in which they are configured. A number of responses also suggested that transactions using such protocols may be less risky for two reasons: the very limited range of such payments and the controlled corporate environment. The EBA does not, however, have any evidence to suggest that the payment transactions conducted through the protocols specified in the new suggested amendment would be less risky.

The EBA also notes that the proposed amendment contains no legal definition of 'corporate' and that the overall scope of, and thresholds for, the exemption are not clear. The EBA is of the view that any such exemption would need to include clear criteria and thresholds, otherwise it would not be practical and would not be consistently implemented.

Relatedly, the EBA is of the view that defining an exemption on the basis of the use of a specific technology, such as machine-to-machine payments, would contravene the objective of the RTS, as

specified in recitals 4 and 19, to be technologically neutral, and might also risk becoming outdated or allowing the exemption to be used for different and potentially riskier purposes in the future.

The EBA also notes that, in practical terms, the suggested exemption would require national competent authorities (NCAs) to pre-exempt specific machine-to-machine protocols from the SCA requirements set out in the RTS. Such pre-approval might go beyond the regulatory power of a number of NCAs under PSD2, either on the basis that competent authorities do not have general competence to pre-approve, or owing to the NCAs' regulatory and supervisory remit not extending to processing protocols. In some Member States, for instance, another national authority may be competent for doing so. For those NCAs that do have competence, there is a risk that their decisions may diverge, leading to a lack of harmonisation and cases where a given protocol is pre-approved in one Member State but not in another.

Taking all the arguments outlined above into account, rather than adding a new exemption, the EBA suggests adding a new category under the transaction risk analysis exemption for specific payment transactions for payers that are not consumers (rather than a reference to corporate payments, given the lack of a definition of 'corporate payments'), without a monetary threshold, providing that the fraud rate is equivalent to or below a specific reference fraud rate. The EBA suggests that all the conditions set out in relation to the transaction risk analysis exemption should apply to this new category.

The new Article 17(2)(b) would then read as follows: 'where the fraud rate for remote electronic payment transactions, where dedicated payment processes and protocols that are only made available to payers who are not consumers are used, is equivalent to or below the reference fraud rate of 0.005% as specified in the table set out in the Annex for this type of transaction'.

c. The Commission proposes that in relation to the use of exemptions to strong customer authentication, payment service providers should report the outcome of their monitoring and the methodology and calculation of the fraud rate under the exemption based on using transaction risk analysis to the EBA, in addition to reporting this information to the national competent authorities (Articles 18(3) and 20(2) of the draft RTS as amended by the EBA)

The Commission is of the view that, in order to enable the EBA to assess the functioning of the exemptions, and in particular the exemption based on using transaction risk analysis for the purpose of conducting a review in accordance with Article 32 of the EBA draft, the EBA should have direct access to data from PSPs.

The EBA agrees with the intention of the Commission and agrees that being able to access disaggregated data would be helpful for the limited purpose of reviewing the way in which the transaction risk analysis exemption has been working in accordance with Article 32 of the EBA draft.

The EBA, however, has the following concerns when it comes to the inclusion as currently drafted:

- The current drafting suggests a new reporting requirement for PSPs, namely to the EBA as well as to NCAs. However, given the EBA's capacities in relation to the data and also considering that the EBA does not have direct supervisory powers over the concerned institutions, the EBA finds that collecting data only as necessary to fulfil its requirements under Article 36 of the RTS is the more efficient and effective approach.

- There is a risk that the additions from the Commission as currently drafted may overlap with another requirement for PSPs under PSD2, given that PSPs have an obligation under Article 96(6) PSD2 to collect and report statistical data on fraud to the NCAs. The NCAs are then required to share aggregate data with the European Central Bank and the EBA. It would be confusing to require, in parallel, a similar reporting requirement directly from PSPs to the EBA.

The EBA is of the view that by reinstating the words 'upon request' and adding the words 'with prior notification to the relevant competent authority(ies)' to the draft RTS, the Commission's objective can be met without giving rise to the EBA's concerns highlighted above. This insertion would enable the EBA to obtain any data directly, if it felt the need to do so, for the purpose of assessing the manner in which the transaction risk analysis exemption is working in practice. This would be in line with the requirement under Article 36 and complement the data that PSPs will be reporting as required under Article 96(6) PSD2.

d. The Commission proposes that, in case of the unavailability or inadequate performance of a dedicated interface, AISPs and PISPs should be allowed to access information using the customer interface (Article 33 of the draft RTS as proposed by the Commission)

In its fourth amendment, the Commission proposes providing a fallback option that AISPs and PISPs can exercise in the event that the dedicated interface is unavailable for more than 30 seconds, or in the event that the ASPSP does not comply with the obligations applicable to interfaces under Articles 29 and 31 of the RTS. The Commission's proposed fallback option consists of AISPs and PISPs having a right to access account information through the ASPSP's customer-facing interface.

The EBA understands that, with this proposal, the Commission aims to ensure that ASPSPs comply with their obligation under PSD2 to share customer information with third party providers (TPPs) without any discrimination and in compliance with the security requirements of Articles 65-67 PSD2. The amendment is aimed at ensuring that AISPs and PISPs can access the data they need to provide services and effectively compete against banks and other PSPs.

The EBA shares those objectives and agrees that it is important to ensure discrimination-free access. The EBA also understands from a number of respondents to its Consultation Paper in August 2016, as well as from discussions with the European Parliament, that there are genuine concerns among some TPPs that ASPSPs will not deliver what is needed, especially in the case of a dedicated interface, where the ASPSPs may not have an incentive to provide the best possible interface to competitors.

However, the EBA is of the view that imposing such a fallback requirement would go beyond the legal mandate given to the EBA under Article 97 PSD2. The EBA is also sceptical about the extent to which the proposed amendment would achieve the desired objectives and efficiently address market concerns. Indeed, the EBA has identified a number of risks that would arise were PSPs to implement the Commission's proposal.

By way of background, the EBA notes that PSD2 imposes new security requirements that will change the way the market currently operates, and will do so for all existing providers. In this context, ASPSPs will be required by law to ensure that TPPs can access only the data necessary to provide a given service to their customers, that TPPs can identify themselves in the process and that TPPs can communicate securely with each other. This means that if ASPSPs were to choose to provide such access based on their existing customer interface, this interface would need to be modified to comply with PSD2. Current access approaches, often referred to as 'screen scraping', in which the TPP impersonates the consumer and has access to all the consumer's data, rather than only the data necessary to provide payment services, would not be compliant.

The EBA is of the view that a fallback option would have a number of negative consequences, which are summarised below.

Negative consequences of a fallback option

This section details the following: cost increases, increased fragmentation compromising the development of application programming interfaces (APIs), competitive disadvantage for new entrants, a lack of improved technical reliability, incompatibility with PSD2's security requirements, supervisory constraints, and unclear consumer understanding and consent. The EBA addresses each in turn.

- **Cost increases**

In the new PSD2 era, an additional fallback option requiring ASPSPs to maintain an additional, PSD2-compliant customer-facing interface in case the dedicated interface fails, as proposed by the Commission, would have the following implications:

- the compliance costs for ASPSPs would increase because, in addition to developing a dedicated interface and maintaining their customer interface, ASPSPs would have to develop, and continuously maintain, a PSD2-compliant customer interface to ensure that the fallback option also complied with the rules under PSD2; and

- the compliance costs for AISPs and PISPs would increase, as they would have to pay to be able to access the dedicated interface and the customer-facing interface of any given ASPSP.

- **Increased fragmentation compromising the development of standardised application programming interfaces**

The EBA is of the view that requiring ASPSPs to have a fallback option in place may lead to ASPSPs abandoning the route of dedicated interfaces altogether, opting instead for customer-facing interfaces that are PSD2-compliant. However, without ASPSPs developing dedicated interfaces, the achievement of an EU-wide communication standard is extremely unlikely, which in turn has a negative impact on one of PSD2's objectives: to standardise access across the EU Member States and create a single EU payments market.

Eventually, this would compromise the development of standardised APIs across the EU, and would increase their fragmentation, along geographical or other boundaries.

- **Competitive disadvantages for AISPs and PISPs wishing to enter the market**

As explained above, the requirement for a fallback option would weaken the ability to develop an EU-wide communication standard, for instance using APIs, and increase fragmentation.

It would instead create:

- a competitive disadvantage and market entry barrier for AISPs and PISPs that are not yet in the market, because they would need to develop a plethora of approaches to accessing payment accounts through different customer-facing interfaces; and

- a competitive advantage for those AISPs and PISPs that have been in the market for many years, because they will already have developed those interfaces.

- **No improvement to technical reliability**

The fallback option is unlikely to guarantee a faultless and errorless interface, given that the modified customer interface would probably be based on the same technological infrastructure and would therefore have similar availability and performance risks to those of the dedicated interface. In short, a fallback interface would not be technically more reliable than the standardised interface itself.

- **Incompatibility with PSD2's security requirements**

The new fallback option would probably negatively affect security and might in fact be incompatible with the security requirements set out in PSD2. Indeed, given the extremely short interval of 30 seconds proposed by the Commission, the ASPSP would not have enough time to assess the situation and safely activate any fallback solution without compromising security (for example in the case of a coordinated cyber-attack). The ASPSP would not be able to act and would not even be aware of any potential defect in its dedicated interface. This might result in ASPSPs treating any access to the customer interface as a security risk, thus blocking such access in compliance with PSD2.

- **Supervisory constraints**

The proposed fallback requirement would also be extremely difficult to supervise, as competent authorities would not be able to conduct any checks or intervene *in the ante*, given the limited 30-second duration. Intervention ex post might be equally difficult.

- **Unclear consumer understanding and consent**

It is likely that it would be very difficult for consumers to understand the multiplicity of ways in which they could access their account information, depending on the providers and/or the interfaces used by those providers, and therefore to understand the implications of giving consent.

The EBA acknowledges the importance of ensuring reliable and continuous access for AISPs and PISPs, as well as TPPs, to be able to access the data required to execute a transaction when they need it. The EBA also agrees with the Commission's intentions, although it disagrees with the proposed fallback option for the reasons highlighted in the previous sections, and proposes an alternative approach in the paragraph below.

The EBA's proposed alternative approach

The EBA proposes the following four-fold alternative approach, which it believes will achieve the objectives sought by the Commission:

- to ensure that ASPSPs deliver reliable and continuous access to the data that TPPs need, the requirements set out in the RTS need to be reinforced;
- to build trust between competing actors, transparency needs to be increased;
- to facilitate a smooth transition from PSD1 to PSD2, cooperation needs to be facilitated by requiring ASPSPs to allow early testing of their interfaces; and
- to enable the EBA to review the practical implementation of the RTS, the EBA should monitor the performance of the interfaces.

To those ends, the EBA suggests including the following requirements in the RTS:

- a requirement for ASPSPs to define transparent key performance indicators and abide by at least the same service level targets as for the customer interface, regarding both the availability and the performance of the interface, as well as qualitative measures to assess whether or not they are doing so (Article 31(2));

- a requirement for PSPs to monitor and publish their availability and performance data on a quarterly basis (Article 31(3));

- a requirement for ASPSPs to make the interfaces available for testing at least three months before the application date of the RTS (Articles 29(3) and 29(5)); and

- a review of the functioning of the interfaces as part of the review planned for 18 months after the application of the RTS under Article 36, to ensure information access and sharing is working as intended.

The EBA is of the view that the suggested measures will ensure that ASPSPs deliver the information needed by TPPs to provide their services, do so in a reliable and continuous manner, and do so without jeopardising further standardisation across the EU or compromising security. The EBA is also of the view that by requiring ASPSPs to allow AISPs and PISPs to test interfaces before the RTS apply, the RTS will provide surety that all ASPSPs would have a working, efficient and reliable interface from the day the RTS apply.

The EBA also notes that PSD2 allows TPPs to use and access only the data they need to execute a payment or consolidate customer information. The EBA is of the view that, if the Commission were to clarify the definition or specification of the data to be provided by ASPSPs to TPPs, and in particular in the case of PISPs, this would contribute towards ensuring there was no misunderstanding and no diverging interpretations among market participants. It is the EBA's view that, whatever data the Commission suggests should be necessary, and acknowledging that the necessary data may not be the same for AISPs and PISPs, the same data, and only this data, should be made available regardless of whether the ASPSP grants access through a dedicated interface or an adapted PSD2-compliant customer interface. Customers using their ASPSP's customer-facing interface are likely to be able to see much more than the data that is necessary for AISPs and PISPs to service their customer.

Finally, the EBA has suggested clarifying in the recitals the purpose for which any interfaces are to be developed, namely to ensure access to information/data to TPPs, the requirements and information provided being the same regardless of the interface selected.

e. Drafting legal changes on the exemptions

In addition to the proposed substantive changes highlighted above, the Commission has also made some drafting changes, a number of which have, in the view of the EBA, led to an undesirable substantive change to the RTS.

First, the Commission has proposed drafting changes to the exemptions on contactless payments, trusted beneficiaries, recurring transactions and low-value transactions (Articles 11, 13, 14 and 16 of the EBA draft). Specifically, in Articles 11 and 16, the Commission proposes a change requiring PSPs to comply with three conditions instead of two, namely the monetary limit of a single transaction, a cumulative monetary limit and a limit based on the number of consecutive transactions.

However, the EBA introduced the last condition as an alternative to the second on the basis of the feedback received during the consultation process, as a number of market participants explained that in a many situations the provider will not be able to identify a cumulative amount, in particular for transactions that are conducted offline. The EBA therefore suggests reintroducing a choice enabling providers to either count in cumulative monetary terms or count the number of

transactions by introducing 'or' between the last two in each of the three different exemptions, to clarify that this is an option rather than two cumulative conditions. With regard to Article 13 on trusted beneficiaries, the EBA suggests reintroducing 'or confirmed' to reflect the current practice whereby the PSP sets up the list, providing the customer has confirmed it wishes this to be done. The EBA also suggests replacing the reference to 'account servicing payment service providers' with 'payment service providers', as this is the accurate terminology in the context of an exemption to SCA.

Second, the Commission has suggested a number of drafting changes in the area of the transaction risk analysis exemption, such as moving some requirements from one article to another. In a number of cases, the EBA requests that the Commission revert to the EBA's drafting, on the basis that the changes would have unintended consequences and cause confusion. Further detail can be found in the revised draft RTS that the EBA submits with this opinion.

Third, the EBA notes that the Commission has deleted the reference to and requirement to define communication messages that are compliant with ISO 20022. On balance, the EBA agrees that to ensure technological neutrality, and despite the risk of jeopardising greater harmonisation at the EU level, it may be preferable to delete this reference.

Fourth, the EBA notes the reference to anonymous payments in recital 8 and would suggest that the Commission also include it in one of the articles of the RTS.

Finally, the EBA is of the view that, for the purpose of consistency and in line with PSD2, Article 18(1) and Article 20(1)(a), in line with Article 2(1), should make reference to 'fraudulent' as well as 'unauthorised' transactions.

Conclusions

This opinion will be published on the EBA's website.

Done at London, 29 June 2017

[signed]

Andrea Enria

Chairperson
For the Board of Supervisors