Deloitte.

Regulatory News Alert

PSD2 – The EBA dials up flexibility to achieve a more balanced approach

1 March 2017

On February 23, the European Banking Authority (EBA) **published** its updated and final Regulatory Technical Standard (RTS) on Strong Customer Authentication (SCA) and common and secure communication under the revised Payment Services Directive (PSD2).

Heeding some of the pressure following the public consultation on the earlier draft, to which the EBA received an unprecedented 224 responses raising over 300 different issues, the regulator introduced some important changes aimed at both increasing flexibility and providing clarity for firms. In this post we set out our view on some of the key changes the industry should be aware of.

Strong Customer Authentication

The EBA introduced two additional exemptions to its general requirement that Payment Service Providers (PSPs) must apply SCA every time a payer initiates an electronic payment transaction.

The first, and most significant, new exemption will free PSPs from applying SCA requirements to every transaction provided they can perform effective real-time payment Transaction Risk Analysis (TRA) to determine whether the transaction presents a low risk of fraud. This is subject to the PSPs managing overall fraud below predefined levels[1]. However, the Account Servicing Payment Service Providers (ASPSPs), i.e., the payer's bank, will have the final say on whether to apply SCA based on their own risk analysis.

The second exemption is for electronic payment transactions initiated at unattended terminals used for collection of transport or parking fares. The EBA recognizes the application of SCA in these terminals would be undesirable from both an operational and security perspective.

In our **analysis** of the earlier draft of this RTS published in August 2016, we had expressed the view that the EBA was erring on the side of security and consumer protection at the expense of innovation and user experience. In this final version, we believe the EBA has achieved a better balance between fostering improved security, usability, and future innovation to the benefit of consumers.

The first exemption in particular provides PSPs more flexibility, the ability to differentiate themselves, and incentives to strengthen their fraud prevention practices to protect consumers. PSPs with more advanced fraud management capabilities and richer customer data analysis capabilities will be able to leverage these to gain a competitive advantage by being able to offer a more seamless customer experience.

While overall we think the industry will welcome the increase in flexibility and choice, there are some drawbacks to consider. To take advantage of the transaction risk analysis exemption, firms will have to commit to continuous investments to improve fraud management capabilities and be willing to absorb new associated overheads introduced by the legislation, such as ongoing monitoring and documentation of fraud levels, reporting to the authorities, and periodic internal or external audit of security measures. In addition, if customers do not understand on what basis SCA is or is not applied, they may find the lack of consistency confusing. This risk is exacerbated by the fact that exemption privileges will be withdrawn by the regulator for at least three months if the fraud rates exceed prescribed limits for two consecutive quarters.

Not all PSPs will therefore necessarily want to take advantage of the new exemption, and their decision will be driven both by an assessment of their current fraud detection capabilities and the investment required, as well as the impact of SCA on their customer offering.

Screen scraping and technological neutrality

In relation to "Access to Account" (XS2A)[2] rights for Third Party Providers (TPPs), the EBA clarified that the existing practice of "screen scraping"[3] will no longer be allowed once the RTS becomes applicable. There has been much debate on whether screen scraping would be admissible under PSD2, and this confirmation provides much needed clarity for the industry, which can now fully focus its efforts into designing and implementing successful Application Programming Interface (API) strategies.

The EBA confirmed that ASPSPs will be required to offer at least one interface to TPPs to allow communication exchanges to take place. This can either be the same as the one interface offered to their existing Payment Service Users (PSUs), i.e., customers, or one dedicated solely to TPP access.

If banks choose to develop a dedicated interface, they will be required to provide the same level of functionality, availability, support, and contingency measures in case of unplanned unavailability as for the online platform provided to customers (e.g., online banking). Banks will also have to report any fault with the dedicated interface to the competent authorities, detailing the causes of the deficiency and the measures adopted to re-establish the required level of service. These measures are intended to ensure that banks do not create detrimental conditions for TPPs or place limitations on their right of access. However TPPs may still feel that the rules leave them at a disadvantage.

Deloitte.

In line with their intention to ensure the RTS remains technologically neutral, the EBA has limited the existing requirement to utilize the ISO 20022 standard only to elements related to the financial messages themselves, and not extending more broadly to the communication interface or APIs. This therefore confirms the position arising from the draft RTS that no fully harmonized standard of communication will be specified in the regulation, meaning that communication interfaces could, in theory as well as in practice, differ for each bank. The lack of interoperability created by the absence of a common communication standard means TPPs might need to build a slightly different connectivity solution for every bank they wish to connect to. This could be highly inefficient and may materially increase overhead costs for TPPs, and possibly undermine the objective to promote competition.

In addition, since banks will not be required to share the technical specification of their communication interface ahead of the RTS implementation deadline, and screen scraping will no longer be allowed from that date, TPPs may find themselves unable to access customers' bank details and infrastructure for a significant amount of time following the RTS' implementation deadline, with potential for consequent loss of business.

Finally to further ensure technology neutrality, the EBA also removed references to specific characteristics for the three elements constituting SCA from the RTS, to allow flexibility in implementation and allow for future innovations.

Conclusion

Although some questions remain, overall the final RTS achieves a much better balance between the EBA's competing objectives[4] under PSD2 by providing a greater degree of flexibility for firms and reducing unnecessary ambiguity.

It is worth noting that in addition to the more substantial changes highlighted above, the EBA made a large number of smaller changes to the text, to which firms should pay close attention. Our recommendation is that firms revisit their gap assessments in light of the updated requirements, and, if they have already progressed to IT implementation, they also revisit their requirements and design documentation.

Next Steps

The final draft RTS has now been submitted to the Commission and will undergo scrutiny by both the European Parliament and Council. Once adopted and published in the Official Journal of the European Union, the RTS will be applicable 18 months after its entry into force, suggesting an application date of November 2018 at the very earliest.

Deloitte.

Authors: Stephen Ley, Partner Risk Advisory at Deloitte LLP, Steven Bailey, Director Risk Advisory at Deloitte LLP, and Valeria Gallo, Manager EMEA Centre for Regulatory Strategy at Deloitte LLP.

[1] Full details of Exemption Threshold Value (ETV) can be found in Article 16 of the RTS. The EBA will review and, if appropriate, propose updates to the fraud rates 18 months after the application date.

[2] Under PSD2, TPPs will be able to connect, with customers' consent, directly to the customer's bank details and use the banks' infrastructure to facilitate payment initiation or account information services.

[3] The action of using a computer program to copy data from a website, without having to identify oneself.

[4] PSD2 objectives include: enhancing security, promoting competition, ensuring technology and business-model neutrality, contributing to the integration of payments in the EU, protecting consumers, facilitating innovation, and enhancing customer convenience.

Your contacts

Pascal Eber
Partner – Operations Excellence
Tel/Direct: +352 451452 649
peber@deloitte.lu

Laurent de la Vaissière
Director - Information & Technology Risk
Tel/Direct: +352 45145 2010
ldelavaissiere@deloitte.lu

Alexandre Havard
Senior Manager – Operations Excellence
Tel/Direct: +352 45145 3148
ahavard@deloitte.lu

Deloitte Luxembourg
560, rue de Neudorf
L-2220 Luxembourg

Tel: +352 451 451
Fax: +352 451 452 401
www.deloitte.lu

Designed and produced by MarCom at Deloitte Luxembourg