
Visa is committed to help boost Europe’s Digital Economy and to play its part in establishing a true Digital Single Market in Europe.

We are therefore deeply concerned about the European Banking Authority’s (EBA) Draft regulatory technical standards (RTS) on Strong Customer Authentication (SCA) and Secure Communication as the text in its current form can potentially be more harmful than helpful to achieving those overarching objectives.

We believe many of the foreseen harmful effects can easily be prevented if the EBA allows for authentication based on risk analysis. Such an approach would provide for a practical and equitable balance between payment security and user convenience. This in effect would help ensure unnecessary hurdles do not hamper future innovation, enhancing cross-border trade and in establishing a robust digital economy in Europe.

And all of this inconvenience comes with no benefits for consumers who are already protected against fraud or with any evidence that it will actually reduce fraud.

What is Strong Customer Authentication?

The revised Payment Services Directive (PSD2) mandates to perform SCA for all electronic payments. This means that payment service providers (e.g. your bank) have to verify at least two from a list of three factors – something you know such as a password, something you have such as a payment card and something you are, for example, a biometric. The European Banking Authority (EBA) is responsible for developing the RTS setting out the requirements to deliver SCA. The EBA published its Draft RTS for public consultation on 12 August 2016 and is expected to publish the final version by 12 January 2017.
What’s wrong with the Draft RTS?

Lack of risk-based approach is inconsistent with PSD2.

The EBA neglected to include exemptions to the mandate to perform SCA based "on the level of risk involved in the service provided" despite being required to do so under Article 98 of PSD2. The EBA’s inconsistency with primary EU legislation is of notable concern.

Online shopping will become more burdensome.

For the benefit of consumers, industry has successfully removed friction from electronic payments and, at the same time, has deployed a catalogue of sound and effective risk management techniques.

Today both payment service providers and merchants make intelligent decisions about the level of risk of the transaction. For example, if you go onto a website to buy a book, the issuer of a payment card and the merchant have choices on how they process the transaction.

The merchant may recognise you as a regular returning customer buying goods for delivery to the same address; the card issuer may note that you are using the same PC, laptop or mobile that you always use to make purchases. This allows them to approve transactions which are clearly undertaken by the recognised customer and only require a step up to SCA when a potentially enhanced risk occurs. This is what we call a “risk based approach”.

Many payment service providers have become very sophisticated and need to require SCA for only 5% of all transactions, and this without suffering additional fraud. A risk based approach as such provides consumers with a familiar and safe experience every time they make purchases on the internet, all while being protected.

Thresholds alone will stifle innovation.

The EBA has established hard limits for transactions with low-value thresholds, above which SCA has to be applied for every transaction.

This for example would require a consumer to enter additional details, such as an SMS code, for every purchase they make on the internet over €10, even when for instance it is known that they are a returning customer with the same delivery address. These hard limits together with the absence of an exemption based on risk is inconsistent with PSD2 considering that irrespective of whether SCA is applied, the consumer is always protected and is never held liable (unless gross negligence or fraudulent behaviour is proven). PSD2 guarantees that fraudulent transactions will be refunded to the consumer within one business day.

The EBA’s approach to e-commerce in today’s modern and technologically fast-paced society is a significant threat to future innovation and Europe’s future growth. It is therefore very worrying that the EBA has imposed a one-size-fits-all model to managing risk in its Draft RTS without taking into account whether it would actually reduce fraud or how it would impact the economy.

How can this be fixed?

Allow risk-based approach.

As envisaged in PSD2, an amendment allowing an exemption based on risk analysis for all payment instruments and a Recital in the RTS clarifying that merchants and their payment service provider can “adopt alternative methods of authentication” and take liability in case of fraud, would in effect make many of the foreseen inconveniences that would be faced by consumers disappear. This would ensure a level playing field between all the different payment instruments used today, avoiding disruption to the e-commerce value chain including consumers.

PSD2 creates the necessary framework to allow the flexibility needed to ensure that present and future authentication solutions (that do not rely exclusively on SCA as defined in the Draft RTS) can adapt to market trends, while preserving the confidence of consumer on their payment instruments.
Visa’s Proposal to amend Article 8 of the Draft RTS

“Exemptions of transaction risk analysis should be allowed. The transaction risk analysis should be based on models which are:

(a) based at minimum on comprehensive real-time risk analysis taking into account should include, where possible: (i) an adequate transaction history of that customer to evaluate the latter’s typical spending and behaviour patterns, (ii) information about the customer device used and where applicable (iii) a detailed risk profile of the payee and the payees device,
(b) proven to be efficient for fighting against fraud and assessed according to Article 7,
(c) are continuously reviewed according to fraud rates & improved in order to address new fraud scenarios & new technological threats.”

Visa’s Proposal to clarify Recitals in the Draft RTS

Visa is concerned about how the EBA in its Draft RTS has interpreted the relevant liability provision in PSD2.

The EBA states that the liability regime of Article 74(2) of PSD2, which allows the merchant and its payment service provider the option not to accept SCA and to be held liable in case of fraud, is only applicable in the transitional period between the entry into force of PSD2 and the applicability of the RTS.

We disagree with this interpretation as there is no legal foundation as to why it should only apply in the transitional period. The respective liability provision should rather be considered as the basis for the merchant and its payment service provider to be able to actively decide whether SCA is needed to secure a transaction according to the risks involved, in exchange for taking liability in case of fraud. Again, in all such cases, the consumer would always remain protected.

The recitals of the draft RTS should reflect that Article 74(2) of PSD2 grants the right to merchants to decide whether SCA (as described in PSD2) should happen or whether they could adopt alternative methods of authentication in exchange of taking liability for the transaction.

This is in line with previous regulatory ECB and EBA mandates on SCA. This is essential in order to preserve for instance the commonly used and secure one-click payment option.

Electronic payments sit at the heart of Europe’s digital economy, it is therefore imperative that the EBA incorporate an exemption based on the level of risk in its RTS so as not to impede current and future efforts in establishing a genuine Digital Single Market in Europe.
Contact
Visa
Brussels Office
Rue Luxembourg 3
1000 Brussels

Marc Temmerman | temmermm@visa.com | T +32 (0)2 274 4747
Peter Møller Jensen | jensenp@visa.com | T +32 (0)2 274 4745

About Visa Europe:
Visa Europe is a wholly owned subsidiary of Visa Inc. (NYSE:V). Visa Inc. is a global payments technology company that connects consumers, businesses, financial institutions and governments in more than 200 countries and territories to fast, secure and reliable electronic payments. We operate one of the world’s most advanced processing networks — VisaNet — that is capable of handling more than 65,000 transaction messages a second, with fraud protection for consumers and assured payment for merchants. Visa is not a bank and does not issue cards, extend credit or set rates and fees for consumers. Visa’s innovations, however, enable its financial institution customers to offer consumers more choices: pay now with debit, pay ahead of time with prepaid or pay later with credit products.