PAYSYS REPORT

Issue 06 October 2016

In this issue:

The EBA's Regulatory Technical Standards: Regulation gone astray

We are grateful for a number of valuable suggestions by Christoph Strauch (Concardis GmbH).

(mk) The PSD2 has been passed and is about to be implemented. One of its elements is strong customer authentication (SCA) (Article 97). In Article 98, the European Banking Authority (EBA) is endowed with the task of specifying the requirements for SCA and the exemptions from SCA.[1] With respect to exemptions, Article 98(3) lists the following criteria:

(a) the level of risk involved in the service provided;

(b) the amount, the recurrence of the transaction, or both;

(c) the payment channel used for the execution of the transaction.

How it is to be applied and to what extent there can be exemptions has to be regulated by the European Banking Authority (EBA).

On 12 August 2016, the EBA published a draft of its Regulatory Technical Standards (Draft RTS).[2] The Draft RTS cover inter alia SCA. According to the EBA, SCA applies to *"electronic payments initiated by the payer, such as credit transfers or card payments, but does not apply to electronic payments initiated by the payee only, such as direct debits."* (Draft RTS, p. 9). Thus, remote payments and POS payments are covered; direct debit based POS payments such as ELV are not covered. However, providing a remote electronic mandate for a direct debit is covered as well.

In the Draft RTS, the EBA does not restate the PSD2's definition of SCA.[3] Rather, it defines the requirements for the authentication process and for the elements of SCA as defined in the PSD2.

The main elements are:

- One-time authentication code (Article 1)
- Payer information (amount of the transaction and payee) (Article 2)

- Dynamic linking (with amount of the payment and payee) (Article 2)

Articles 3, 4 and 5 cover requirements with respect to the three elements of SCA (knowledge, possession, inherence) two of which have to be used. These requirements are fairly general.

Given that the PSD2 mandates SCA and dynamic linking, there is not much that can be done with respect to these points. The EBA simply had to comply with the wording of the PSD2. But when it comes to exemptions, the PSD2 is more open to interpretation. So, this is the crucial part of the RTS.

The exemptions are fairly slim:[4]

- Cases, in which customers assess non-critical information (Article 8(1))
- Contactless e-payments of up to 50 EUR (cumulative amount of up to 150 EUR) (Article 8(1))
- Cases in which payees are included in a white list "created by the payer" (Article 8(2))
- Standing orders (Article 8(2))
- Internal transfers of one customer between accounts at the same PSP (Article 8(2))
- Remote payments of up to 10 EUR (cumulative amount of up to 100 EUR) (Article 8(2))

It is notable that the exemptions are more limited than in the EBA's "Guidelines on the Security of Internet Payments" (Guidelines).[5] The Guidelines included the possibility of alternative authentication measures for online card payments: *"The use of alternative authentication measures could be considered for pre-identified categories of low-risk transactions, e.g. based on a transaction risk analysis, or involving low-value payments, as referred to in the PSD"* (Article 7.5). Such a provision is missing in the Draft RTS.

Market participants are invited to comment on the draft RTS by 12 October 2016. The final RTS will be published after consultation and is expected to come into force in October 2018. As far as internet payments are concerned, there are already EBA Guidelines in place that had to be transposed by national regulators. Once the RTS come into force, they will replace these Guidelines.

Our Comment:

The PSD has been passed and now it is "crunch time", crucial details need to be defined. The EBA has made a first proposal. To put it in a nutshell, the industry is not happy and the main issue of contention is SCA. Given this current draft by the EBA, the SCA will be implemented in a rather restrictive way. Therefore, it is all the more important to look at the underlying rationale for regulation.

When assessing the EBA´s Draft RTS, first one has to come back to the main argument for regulation, which is security. As a competent regulatory body, the EBA (and the ECB which, according to the PSD2, is supposed to co-operate with the EBA) should take a look at the current situation. Is there, indeed, a grave security problem? First, in most countries e-commerce is growing strongly. Thus, whatever payment risks there are, they do not seem to be a strong impediment to growth. But, of course, fraud could be rising, making action necessary. Looking at card-fraud figures, it can be concluded that fraud is indeed rising. However, it is not rising as fast as e-commerce. Thus, fraud rates are going down. In fact, given the limited available data, it can be concluded that they have already been going down for a longer period of time.[6] Thus, the problem is not as grave as policy makers seem to believe. This finding should also be taken on board by the EBA. There is no upward spiralling fraud that requires drastic action by regulators. As a consequence, a strong case can be made for letting market participants proceed as they seem fit. In the present context of PSD implementation that would imply fairly wide scope for exemptions from SCA.

Another issue a regulator should address is the question of whether there is some kind of market failure with respect to the security of e-payments. In our view, this is not the case.

Fraud rates are going down

There is no upward spiralling fraud that requires drastic action by regulators

Since high fraud rates would either rebound on them or would provide an incentive for customers to switch to other PSPs and other payment instruments (or refrain from e-commerce altogether), payment schemes and PSPs have a strong incentive to keep fraud in check. Interestingly, this position is also supported by "Which?", the UK consumer organisation. In its "super-complaint", Which? argues that for most payment transactions liability is allocated in a way that provides banks and PSPs with strong incentives to contain fraud.[7] This is particularly the case for "pull payments" such as direct debits or card payments and unauthorised payments. Which? sees authorised push payments (such as credit transfers) as the biggest problem. For such transactions, if, for instance, a consumer becomes victim of a scammer, full liability lies with the consumer and none with the banks. Ironically, SCA will not improve the situation of consumers in such cases, in fact it may make them worse off.[8]

The argument of Which? strongly focusses on liability and incentives. This approach can also be found in the PSD2. As Art. 74 (2) states:
"Where the payer's payment service provider does not require strong customer authentication, the payer shall not bear any financial losses unless the payer has acted fraudulently. Where the payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer's payment service provider."

This Article strongly suggests that SCA is not meant to be the standard case with only a few exceptions. Rather, requiring or not requiring SCA is decisive for the allocation of liability. Thus, a PSP willing to shoulder liability and able to manage risk should be allowed to carry out transactions without requiring SCA.

The EBA favours a different approach. It seems to believe that more detailed regulation automatically implies more security. On page 6 of the Draft RTS, the EBA states that there are a number of trade-offs, inter alia between security and innovation:
"*the objective of ensuring a high degree of security would suggest that the EBA should develop the Technical Standards at a very detailed and technological level."*
We consider this position as a fundamental misunderstanding of security. As Bruce Schneier, a well-known expert in the field of IT security, once said: *"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."*[9]

SCA does not eliminate all risks. As the super-complaint of Which? demonstrates, plenty of risks remain even if SCA functions properly. Moreover, like any technology, SCA is not 100% proof against attacks.[10] In fact, the EBA seems to be aware of this. When considering the trade off between innovation and regulation, the EBA states:
"By contrast, the objective to facilitate innovative means of payment would suggest that the EBA should do the opposite and pitch the Technical Standards at a less detailed and higher level, so as to allow room for the industry to develop industry solutions that are compliant with the EBA's Technical Standards but that also allow for innovation over time, so as to exploit technological advancements and to respond to future security threats." (page 6 of the Draft RTS).

The way the EBA has expressed this trade-off almost makes clear already that it does not really exist. If a less detailed regulation makes it possible *"to exploit technological advancements and to respond to future security threats"*, then it seems pretty obvious that this is the high road to security.

So at least with respect to "future security threats" even the EBA does not see a trade-off. In a nutshell, the statement implies that less regulation and more innovation provide more security. But "very detailed" technical standards, mandated after years of public consultation, are not a blue print for secure payments. Rather, they are inflexible targets for fraudsters.

Thus, security should be approached in the spirit of Article 74(2). Liability rules should provide the right incentives for PSPs to manage risk properly. The PSD2 mandates that SCA is one element and that the requirement or non-requirement of SCA should have strong implications for the allocation between PSPs.

The Draft RTS are not only important for the security of e-payments, they are also important for the convenience of e-commerce/m-commerce. There is a trade-off between "detailed regulation" and convenience. Online merchants are worried that SCA will destroy a seamless customer experience when shopping online.[11] As a consequence, card abandonments are likely to rise and conversion rates to fall. Such an expectation is substantiated by the experience with 3DSecure. Conversion rates matter a lot to online merchants. In fact, in spite of strong incentives ("liability shift") many merchants chose not to implement 3DSecure and rather carry fraud themselves. From what is known in terms of anecdotal evidence from the market, these merchants do not suffer higher fraud rates than those using 3DSecure.

There is a trade-off between "detailed regulation" and convenience

Fortunately, there is also a way to combine security and convenience (to some extent): Targeted Authentication (TA).[12] Target authentication relies on a lot of risk management in the background that helps to assess the riskiness of a transaction. Low-risk transaction can do without SCA, high risk transactions require SCA and those that are almost sure to be fraudulent are declined. Such systems have been used successfully for online and POS payments. They have been implemented at PSP and/or merchant level. They made it possible to keep fraud in check and still provide a high level of convenience for customers.

Thus, one of the exemptions should be that a workable TA system is used. "Workable" could be defied in one way or the other. The simplest route would be a maximum permissible fraud rate[13] – an idea the EBA does not seem to consider. Another approach would be the "principles-based approach" suggested by Equens.[14] EBA, however, explicitly states that it is unable to define criteria for a proper risk-analysis.

"In that respect, the EBA recognises there is merit in implementing a transaction risk-analysis as part of the strong customer authentication procedure proposed in Chapter 1 of the draft RTS. However, the EBA was not able to identify which minimum set of information the RTS should require for such transaction risk analysis to be sufficiently reliable to allow a specific exemption from the application of SCA, while also ensuring a fair competition among all payment service providers. Against this background, the EBA has concluded for the Consultation Paper not to propose exemptions based on a transaction-risk analysis performed by the PSP." (Draft RTS EBA, p. 16)

We think that market participants can expect more effort from the EBA. After all, in Article 98 of the PSD2 it is stated that the EBA shall specify exemptions and that these exemptions should be based inter alia on "*the level of risk involved in the service provided*".

In Recital 108 of the PSD2 it is stated that EBA should *"ensure that it consults all relevant stakeholders, including those in the payment services market, reflecting all interests involved. If necessary for getting a proper balance of views, EBA should make a particular effort to obtain the views of relevant non-bank actors."*

Indeed, the EBA has "obtained the views" of stake holders. But it should also listen – even if this is not explicitly mentioned in the PSD2.

Notes

1. The EBA also has to specify security measures for protecting the payment service users' personalised security credentials and common and secure open standards of communication for the parties involved in a payment transaction (including payment initiation service providers).
2. EBA: Consultation Paper. On the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2, EBA-CP-2016-11, 12 August 2016. In December 2015, the EBA had already published a Discussion Paper on the same topic and invited interested parties to comment. (See also "The EBA's Discussion Paper on 'Regulatory Technical Standards'" in: PAYSYS Report, Issue 01, February 2016).
3. 'strong customer authentication' means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data. (Article 4(30), Directive (EU) 2015/2366)
4. In some cases, the first transaction of a particular type undertaken by a customer with a PSP is not exempted.
5. EBA: Final guidelines on the security of internet payments, EBA/GL/2014/12, 19 December 2014.
6. See "Fourth ECB report on card fraud published", PAYSYS Report, Issue 04-05, July 2015.
7. Which?: Which? super-complaint. Consumer safeguards in the market for push payments, 23 September 2016.
8. For instance, many card holders have been well aware that 3DSecure makes it more difficult for them to successfully dispute a card transaction.
9. Bruce Schneier, Preface to "Secrets and Lies", John Wiley & Sons, 2000.
10. See, for instance, Equens SA: "Response to EBA discussion Paper on RTS for PSD2", 8th February 2016.
11. See Ecommerce Europe: 'Targeted Authentication' best answer for secure and convenient online payments, Sep 26, 2016 (http://www.ecommerce-europe.eu/press-item/3870/) and "Recommendations for improving European online payment regulation", prepared by CleverAdvice led by Marco Fava, August 2016 (commissioned by Ecommerce Europe, EDiMA, EPIF, Choice in eCommerce and CCIA).
12. See "Recommendations" (cited in end note 11) and Peter Jones: EBA Strong Customer Authentication – the End of Frictionless Card Payments?, PSE Consulting, 2016.
13. See "Recommendations" (cited in end note 11).
14. See „Response" (cited in end note 10)

Should you have any questions or comments please contact:

Dr. Hugo Godschalk (hgodschalk@paysys.de)
Dr. Malte Krueger (mkrueger@paysys.de)

Please, send us your views to:
paysys-report@paysys.de

PAYSYS REPORT IMPRINT

PaySys Consultancy GmbH
Im Uhrig 7
60433 Frankfurt /Germany
Tel.: +49 (0) 69 / 95 11 77 0
Fax.: +49 (0) 69 / 52 10 90
email: info@paysys.de
www.paysys.de

PAYSYS REPORT
October 2016

Layout: cristina dresler | kommunikation+gestaltung

Subscription info:
The PAYSYS REPORT is published 10 times a year in English in electronic format (pdf) and contains about 4-6 pages.
The price is
250 EUR per year (single user license)
500 EUR per year (company license)

To order, please send an email to paysysreport@paysys.de indicating the type of license you wish to purchase and the method of payments (credit transfer or credit card).

PaySys Consultancy is German member of

epca
european | payments consulting | association