PSD2 and draft EBA RTS: a lot of issues remain unclear…

Scott McInnes, Bird & Bird LLP

3 May 2017

Brussels Partner Scott McInnes specialises in competition law, as well as the regulation of financial services and in particular payments.

The purpose of this article is to highlight some of the questions that are still open on the topic of SCA (Strong Customer Authentication) and Third Party Provider (TPP) access to the payment account after the draft Regulatory Technical Standards published by the EBA on 23 February 2017 [1].

*

* *

Introduction

PSD2 (i.e. the revision of the EEA Payment Services Directive, to be implemented within the laws of the EEA Members States by 13 January 2018 for most – but not all – of its provisions) raises a lot of questions of legal interpretation.

Some of these questions have been answered informally (i.e. in a non-legally binding way) in the five PSD2 Transposition Workshops (TWs) that have taken place to date, and in which the European Commission (EC), European Central Bank (ECB) and various national regulators have participated.

Some other questions have been answered, at least in draft form, by the European Banking Authority (EBA) which has been given a mandate in PSD2 to prepare draft Regulatory Technical Standards (**RTS**) on two of the most debated topics under PSD2, namely Strong Customer Authentication (SCA) and how so-called TPPs (Third Party Providers – categorised as AISPs/Account Information Service Providers and PISP/Payment Initiation Service Providers) are to receive access (free-of-charge) to payment accounts maintained by ASPSPs (Account Servicing Payment Service Providers – we will call them "banks" in the rest of this article because that is what most ASPSPs will be).

On 23 February 2017, the EBA delivered its draft RTS, which is generating a lot of questions in the industry[2]. At the time of writing, the rumour is that the EC intends to exercise its right to send the draft RTS back to the EBA for further work – something that the EC is allowed do within a period of three months, i.e. by 23 May 2017. The purpose of this article is to highlight some of the questions that are still unclear in the draft EBA RTS, and that the EBA and ultimately the EC (as the institution who will ultimately adopt the RTS) will probably want to address in the coming weeks and months. We also provide here our own views and tentative answers to some of the questions – although nothing in this article should be

[1] The author is grateful to Trystan Tether, Partner at Bird & Bird LLP in London, for his comments on a draft version of this article. All mistakes and omissions reside solely with the author.

[2] The draft RTS is available here: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

interpreted as constituting legal advice. We address first the topic of SCA, before turning to the second topic of TPP access to payment accounts.

Strong Customer Authentication (SCA)

PSD2 contains a principle that when a "payment service user" (PSU) (1) accesses his payment account online, or (2) initiates an electronic payment transaction, or (3) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses, that action needs to be subject to SCA, also sometimes referred to as two-factor authentication[3]. SCA means that two of the following factors should be present to authenticate the user: something only the user knows (e.g. a password or a PIN) and/or something only the user has (e.g. a card reader, secure key generator or mobile phone) and/or something only the user is (e.g. fingerprint, face or other biometric recognition).

PSD2 entrusted the EBA to come up with proposed exemptions to the principle of SCA[4]. Some of the exemptions proposed by the EBA in its draft RTS raise a number of questions, such as the exemption for low-value payments, the TRA (Transaction Risk Analysis) exemption, and the "trusted beneficiaries" exemption. We now address each of these in turn.

- **Low-value payments (LVP).** The EBA proposed an exemption for contactless low-value payments in the face-to-face world, as well as low-value remote (e.g. online) payments. Those exemptions are based on the value of each individual payment (below 50 EUR for face-to-face contactless payments, below 10 EUR for remote payments), but also a cumulative value or number of previous contactless payments without SCA (150 EUR or five contactless transactions[5]) and previous remote payments without SCA (100 EUR or five remote transactions). The problem is that the PSP (Payment Service Provider) of the merchant (the "acquirer" in relation to card payments) is unable to keep track of the cumulative value or the cumulative number of transactions without SCA (only the PSP of the payer, i.e. the "issuer" in relation to card payments, is able to keep track of that cumulative value or cumulative number of transactions). For example, in the case of remote payments, if I want to shop online at a particular web merchant, how is the PSP of that web merchant supposed to know that I already spent X Euros at other web merchants without performing SCA, or that this would be my 6th remote transaction without SCA? In practice, it is impossible for the acquirer to know – and therefore acquirers face a dilemma in relation to the LVP exemption:

    1. either implement a "no risk approach", i.e. always request for the issuer to perform SCA even for LVP transactions since there is always a risk that the cumulative value/number of transactions limit will be exceeded; and let the issuer determine whether the conditions for the LVP exemption are met, and therefore allow the transaction to take place without SCA? or

    2. adopt the "risky approach", i.e. never request SCA in relation to LVP transactions, but therefore take the risk that, once in a while, the acquirer will violate the RTS since the acquirer should legally be requesting SCA given that the limit on the cumulative value or number of previous transactions has already been reached. The acquirer would also take the risk that, if the issuer realises that the transaction does not benefit from the LVP exemption/cannot

[3] Article 97(1) of PSD2.
[4] (Article 98(1)(b) of PSD2.
[5] Is this the cumulative value/number of transactions since the last SCA was performed in relation to an attempt to pay contactless? Or since the last "dip the card and PIN" transaction? Or is it OK if the last SCA was performed in relation to a remote payment?

take place without SCA, the issuer will decline the transaction – and the acquirer will have to re-submit the transaction, but this time requesting the issuer to perform SCA.

- **Transaction Risk Analysis (TRA) – how is the "ping pong" between the acquirer and the issuer expected to work in practice?** The draft EBA RTS contains the concept of TRA (generally referred to as RBA/Risk-Based Assessment or Risk-Based Authentication), i.e. the possibility for the PSP of the payee (the "acquirer" in the case of card payments) and the PSP of the payer (the card "issuer" in the case of card payments) to determine that a transaction is "low risk" and therefore not request (for the acquirer) or perform (for the issuer) SCA – subject to certain requirements (e.g. having fraud transaction monitoring mechanisms in place, having fraud levels below certain thresholds, etc.). However, it is not obvious in practice how the TRA "ping pong" between acquirers and issuers is supposed to take place. Below is the author's simplified understanding of what the draft EBA RTS seem to provide for:

    1. If the acquirer does not meet the conditions to do TRA (e.g. transaction above 500 EUR, or transaction below 500 EUR but the acquirer does not meet the fraud thresholds), the acquirer will request the issuer to perform SCA. If the issuer doesn't meet the conditions for TRA, or if he does but considers that the transaction is high-risk, the issuer will perform SCA. If the issuer meets the conditions for TRA and concludes that the transaction is low-risk, the issuer could move to the next stage of the payment process (i.e. the authorisation stage) without performing SCA.

    2. If the acquirer meets the conditions to do TRA (e.g. transaction below 500 EUR and basis points of fraud below the required thresholds), performs its TRA and:

        - concludes that the transaction is high risk, the acquirer needs to request the issuer to perform SCA – see point 1 above.

        - concludes that the transaction is low-risk, the acquirer will not request the issuer to perform SCA – and therefore, technically, the issuer will not be able to perform SCA. If the issuer agrees that the transaction is low-risk, the issuer will authorise the transaction with no SCA taking place. However if the issuer considers that the transaction is high-risk, or if the issuer realises that the acquirer should have requested SCA (e.g. the transaction is above 500 EUR[6]), the issuer is apparently expected to decline/not authorise the transaction (presumably this is what the EBA means in their draft RTS when they refer to the fact that the issuer always has "the last say"[7]); in which case the acquirer may decide to re-submit the transaction to the issuer, but this time requesting the issuer to perform SCA (see point 1 above).

- **Trusted beneficiaries – available for card payments?** The draft RTS contain an exemption for "trusted beneficiaries" (sometimes also referred to as "white

[6] If the transaction is between 30 EUR and 500 EUR, how is the issuer supposed to know whether the acquirer fulfils the other conditions to do TRA, e.g. the fraud basis points requirements? Will acquirers be required to pass on that information to issuers – and if so how (e.g. in the authorisation message)? If so, doesn't this raise a potential competition law concern that acquirers pass onto issuers, who can also be acquirers, up-to-date information on their basis points of fraud – which arguably is or may be a factor of competition between acquirers?

[7] See question 295 in the table accompanying the draft EBA RTS.

listing"), i.e. the payer is allowed to white-list one or more payees, and payments made to those payees would benefit from an exemption to the principle of SCA. Since Article 13(1)(a) of the draft EBA refers to "payment transactions", therefore not making a distinction between different means of payments (i.e. credit transfers and card payments), this exemption is available to both methods of payments. It has been reported in the specialised press that this was indeed the intention of the EBA[8]. However, some argue that this exemption is only available to credit transfers, and therefore not to card payments, because of:

1. an unclear statement in the table that accompanies the draft RTS[9]

2. the fact that in the recitals to the draft RTS, in relation to another exemption for "recurring payments", the EBA explicitly indicates that such other exemption is available to both cards and credit transfers, whereas a similar explicit statement is not made in the recitals in relation to white-listing.

Since the wording of Article 13(1)(a) is clear (i.e. the white-listing exemption is available to all kinds of "payment transactions"), in the writer's view a statement made in the non-legally binding table is irrelevant[10]; and the absence of a specific reference in the recitals to white-listing being available for card payments is also not compelling. However, for the avoidance of doubt, perhaps the EBA or EC could clarify this point in the next version of the RTS?

- **Trusted beneficiaries – available to large online merchants?** Assuming that the white-listing exemption to the SCA principle is available for card payments (see above), is the consumer allowed to white-list large online merchants so that he will never again have to perform SCA when purchasing at those merchants? If so, this could potentially be a very large exemption to the principle of SCA, and large merchants may systematically request consumers to white-list them so that future payments at those merchants can take place via a one-click checkout. The EC seems to be concerned about this possibility and may therefore want to change the draft RTS in such a way that:

  1. either white-listing will not be available to cards, or

  2. if it is available to cards, the scope is somewhat limited in order not to make the exemption available to large online merchants. However, in that case, it is not clear where the EC will want to place the limit: white-listing of family and friends would presumably be OK. But what about white-listing of my favourite online platform to buy music and other e-content, or what about the white-listing of online marketplaces? The EC may argue that those large online websites already benefit from the TRA exemption, and therefore should not be eligible for the white-listing exemption.

- **"Card-on-file" payments - do they benefit from an exemption?** There is a statement contained in the (non-legally binding) table accompanying the draft EBA RTS that is being interpreted by some as exempting from SCA transactions initiated on the basis of card credentials that the merchant holds on file; therefore allegedly allowing all merchants doing card-on-file to continue to benefit from one-click

---

8 https://paymentscompliance.com/premium-content/insights_analysis/regulator-clarifies-psd2-%E2%80%98whitelisting%E2%80%99-after-mastercard-concerns

9 See page 87, question 80 in the table accompanying the draft EBA RTS.

10 In addition, the comment may be understood as meaning that: payees are not allowed to do white-listing; all payers are allowed to do white-listing.

checkout[11]. If the EBA had meant to grant such a potentially wide-ranging exemption, one might have expected the EBA to make reference to this alleged exemption in the body of the RTS (or at least in the recitals). Arguably what the EBA intended to stipulate by the relevant wording in the table was that the technical service providers who provide card-on-file technical solutions to merchants do not qualify as "PSPs" under PSD2, and therefore do not have to comply with the SCA requirements. We assume that this will be clarified in the next version of the draft RTS.

In addition to the above exemptions to the principle of SCA proposed by the EBA in its draft RTS, we would like to briefly touch upon two other topics: "special commercial cards" and ATM transactions.

- **"Special (commercial) cards", in particular in the travel sector – should they be exempted?** Under the current draft EBA RTS, all card-based payments are in principle covered, i.e. whether it is a consumer card or a commercial card, whether it is a physical/plastic card or virtual one/VCN (Virtual Card Number), whether it is a multiple-use card or single-use card, etc. (with the exemptions of "limited network" cards that fall outside the scope of PSD2, including the SCA provisions of PSD2 – see Article 3(k) PSD2 for the definition of "limited network"). Some argue that transactions with commercial cards should be exempt when the cards are "lodged" – for example with a(n) (online) travel agent (TA or OTA), and/or "special" cards used for B2B or wholesale payments in particular in the travel sector, such as virtual cards or VCN (Virtual Card Number), in particular due to the impossibility (or at least extreme difficulty) of performing SCA whenever those cards are used, but also the fact that those cards only attract minuscule levels of fraud today. Apparently the EC would have some sympathy for the arguments made in relation to those "special cards" and may be minded to grant them an exemption.[12]

- **ATM transactions.** It is stated in the table that accompanies the draft EBA RTS that the articles on SCA in PSD2 (i.e. Article 97 et seq.) would not only be applicable to POS (face-to-face and remote) transactions, but also to ATM withdrawals. This makes legal sense given the definition of "payment instruction" in Article 4(5) PSD2: " *'payment transaction' means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee*" (emphasis added). However, assuming that ATM withdrawal can take place in contactless mode, does the exemption for face-to-face contactless payments apply to ATM withdrawals, e.g. no SCA for contactless ATM withdrawals below 30 EUR? If so, the same issue as above arises regarding the impossibility for the ATM acquirer to know whether the cumulative value/number of transactions is complied with – and therefore the dilemma arises as to whether the ATM acquirer always requests SCA for contactless ATM withdrawals even below 30 EUR, or never requests SCA for such withdrawals but with a risk of violation of the RTS and/or the transaction being declined by the issuer.

TPP access to the payment account

The second main topic addressed in the draft EBA RTS is the topic of TPP access to the payment account, and in particular the key topic of debate of whether TPPs should be allowed to continue to access the payments through "screen scraping" (sometimes also referred to as "direct access") or not. In its draft RTS, the EBA allows the banks to choose

[11] See pages 74-75, question 52 of the draft EBA RTS.
[12] See for example this article for more details: http://www.businesstravelnews.com/Payment-Expense/Impending-EU-Regulations-Could-Pose-Hurdles-for-Corporate-Cards

whether to grant the TPP access via a so-called "dedicated interface" (in practice, an API) or via the same interface as the one made available by the bank to the payment service user (PSU). It is formally stated in the draft RTS that, as from the date of the RTS becoming applicable, screen scraping will no longer be allowed[13]. However, TPPs have certainly not spoken said their last word on this issue, and there is a rumour that the EC may decide to continue to allow a form of screen scraping as a "fallback" option (perhaps in situations where a dedicated interface does not work?).

Another issue that is being debated at the moment is what type of account qualifies as a "payment account" to which TPPs can get access. A payment account is defined in Article 4(12) of PSD2 as "*an account held in the name of one or more payment service users which is used for the execution of payment transactions*". There still seems to be uncertainty as to what constitutes a payment account, although we are gradually seeing more clarity emerge on this topic with the consultation papers published by UK Treasury (HMT)[14] and the UK Financial Conduct Authority (FCA)[15]. The current position appears to be as follows:

- current account: this is clear – it is payment account.

- credit card account: according to the UK HMT and FCA consultation papers, it does constitute a payment account. However, it appears that UK HMT may have refined its view on this topic to the effect that AISPs can access a credit card account, whereas PISPs cannot. The reason for this distinction seems to be based on the fact that, since consumers are not able to initiate payments from their credit card payment, PISPs shouldn't be able to do so either. In addition, it is not obvious why PISPs (who today push credit transfers from the bank account of the consumer to the bank account of the merchant, but not card-based payments) would start initiating card payments with interchange fees, scheme fees, processing fees, acquirer margin, etc. On the other hand, AISPs will apparently be able to access the data related to the credit card account, just like the consumer can.

- E-money account: for the same reason as the credit card account, it is likely that the national regulators will conclude that an e-money account constitutes a payment account that TPPs (at least AISPs) can access; this is at least the view expressed by UK HMT and UK FCA in their consultation papers. However, payment accounts can only be accessed to the extent they are "*held in the name of one or more payment users*". It seems to be the case that some prepaid card issuers only have one prepaid account/"pool" account, of which each of the cardholders holds a share, but which is not held in the name of the various prepaid cardholders; and therefore potentially such an account should not be legally accessible? In addition, since a TPP can only access the payment account of the user based on his "explicit consent", if the account is shared by several thousand prepaid cardholders, surely it cannot be the case that a TPP would have access to information in relation to prepaid cardholders who have not given their explicit consent to the TPP?

- According to the UK FCA consultation paper, the following accounts also constitute payment accounts: flexible savings accounts and current account mortgages. On the other hand, UK FCA is of the view that fixed term deposit accounts (where there are

[13] See pages 4 and 11 of the draft EBA RTS. The Speech from EBA chairman of 21 February 2017 is available here: https://www.eba.europa.eu/documents/10180/1760799/Andrea+Enria+speech+on+PSD2+at+Westminster+Forum+210217.pdf

[14] Available here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/589023/implementation_of_revised_EU_directive.pdf

[15] Available here: https://fca.org.uk/publication/consultation/cp17-11.pdf

restrictions on the ability to make withdrawals), child trust fund deposit accounts and certain cash Individual Savings Accounts (ISAs) are not payment accounts.

More to come on this topic, no doubt…

* *

*