Bird & Bird & PayBelgium
SCA as applied to open banking

10 December 2020

Scott McInnes / Julien Sad
Bird & Bird LLP

Agenda

1. AIS – basic SCA principles
2. PIS – basic SCA principles
3. EBA opinion on obstacles – 7 topics
4. Reverse engineering – not SCA compliant?

1. AIS – basic SCA principles

AIS

Art. 97(1)(a) PSD2: "… *a* [PSP] *applies* [SCA] *where the payer … (a) accesses its payment account online*"

EBA June 2018 Opinion:

- ASPSP in charge of SCA
- unless otherwise agreed between the ASPSP and the TPP – but (1) the ASPSP remains fully responsible for compliance with SCA requirements + (2) ASPSP may need to comply with EBA guidelines on outsourcing

AIS

<u>Optional</u> exemption for ASPSP:

- no SCA required when "*a* [PSU] *is limited to accessing … (a) the balance … (b) the payment transactions executed in the last 90 days …*".
- But SCA needed when "*(a) the* [PSU] *is accessing online the information … for the first time; (b) more than 90 days have elapsed since the last time the PSU accessed online the information … and* [SCA] *was applied*"

EBA June 2018 Opinion:

- "*The 90-day period is specific to* ***each AISP*** *and is also separate from the 90-day period for the PSU* ***directly*** *accessing its account information*"
- "*Making a payment directly or via payment initiation and performing SCA will* ***not*** *restart the 90-day counter …*"

AIS

Art. 36(5) RTS

"[AISPs] *shall be able to access information … (a) whenever the* **[PSU] *is actively requesting*** *such information; (b) where the* [PSU] ***does not actively request such information****, no more than four times in a 24-hour period, unless a higher frequency is agreed between the* [AISP] *and the* [ASPSP]*, with the* [PSU's] *consent*".

- Presumably no SCA required in scenario (b) since it is not "the payer" accessing its payment account? Implicit in various EBA statements
- How does the ASPSP know we're in scenario (b) (i.e. no SCA requirement)?

2. PIS – basic SCA principles

PIS

Art. 97(1)(b) PSD2: "*... a* [PSP] *applies* [SCA] *where the payer ... (b) initiates an electronic payment transaction*"

EBA June 2018 Opinion: same as AIS, i.e. ASPSP in charge (possibility to delegate to TPP but (1) ASPSP remain fully responsible + (2) possible outsourcing)

Several optional exemptions in the RTS available to ASPSP:

Remote:
- LVP (below 30 EUR + cumulative 100 EUR/no more than 5 tx)
- TRA (max. 500 EUR)
- Credit transfers between PSU's accounts held by the same ASPSP

Non-remote (i.e. proximity):
- Contactless (below 50 EUR + cumulative 150 EUR/no more than 5 tx)
- Unattended terminals, for transport or parking

Remote + proximity:
- Trusted beneficiaries
- Recurring transactions
- Secure corporate payments

3. EBA opinion on Obstacles

EBA Opinion on obstacles (4 June 2020)

- Art. 32(3) RTS: "[ASPSPs] *that have put in place a dedicated interface shall ensure that this interface does not create obstacles to the provision of* [PIS] *and* [AIS]. *Such obstacles,* ***may*** *include, among others,* ***preventing the use by*** **[TPPs]** ***of the credentials*** *issued by* [ASPSPs] *to their customers,* ***imposing redirection*** *to the* [ASPSP's] *authentication or other functions, requiring additional authorisations and registrations in addition to those provided for in* [PSD2]*, or requiring additional checks of the consent given by* [PSUs] *to* [TPPs]"

EBA Opinion on obstacles (4 June 2020)

- EBA Opinion on obstacles – general comments:

  - "*redirection can be an obstacle if implemented in a manner that creates **unnecessary friction** in the customer experience when using TPPs' services, or if the authentication procedure with the ASPSP is **more cumbersome** compared to the equivalent experience PSUs have when directly accessing their payment accounts or initiating a payment with the ASPSP*"

  - " *… in a redirection or decoupled approach, where the PSU is redirected to the ASPSP to authenticate, the interaction between the PSU and the ASPSP should be **minimised to what is necessary** in order for the PSU to authenticate. The authentication procedure with the ASPSP as part of an AIS/PIS journey should not include **unnecessary steps or require the PSU to provide unnecessary or superfluous information** compared to the way in which the PSU can authenticate when directly accessing their payment accounts or initiating a payment with the ASPSP. The EBA deems such unnecessary steps or information required as obstacles*"

[B&B comment: nothing new here; see Dec. 2018 EBA guidelines on exemption from fallback requirement – Guideline 5]

EBA Opinion on obstacles (4 June 2020)

- EBA opinion on obstacles – 7 specific areas:
  - 1 to 4 are directly related to SCA
  - 6 and 7 are indirectly related to SCA
  - 5 (account selection) is not related to SCA

Bird & Bird

Area 1: authentication procedures that ASPSPs' interfaces are required to support

- All SCA procedures made available by ASPSP to PSU should also be available to AISP/PISP. For example, if ASPSP supports biometrics in mobile banking app, it should also be available to AISP/PISP – e.g. app-to-app redirection from TPP app to ASPSP app without any additional steps (e.g. without being redirected first to ASPSP's mobile website) [B&B comment: not new – see e.g. Art. 30(2) RTS, EBA response to issues raised in EBA Working Group on APIs]

- After SCA, PSU should automatically be redirected back to TPP app without having to manually re-open the TPP app

Area 2: mandatory redirection in a shop

- Some TPPs: "redirection in a shop is an obstacle *per se*. Therefore ASPSP should implement embedded (or decoupled) SCA"

- EBA:
  - Redirection *per se* is not an obstacle. Mandatory redirection is only an obstacle if (1) it is the sole method of carrying out SCA **and** (2) does not support all the SCA methods made available by ASPSP to PSU [B&B comment: not new – see EBA June 2018 Opinion]
  - No legal requirement for ASPSP to implement embedded SCA
  - No legal requirement for ASPSP to enable PIS-initiated payments using SCA procedures that ASPSP does not (yet) offer to its PSU

Area 3: multiple SCAs

- AIS-only journey: not more than one SCA

- PIS-only journey:
  - If PISP transmits to ASPSP all information necessary to initiate the payment (e.g. payer's IBAN): not more than one SCA (unless the ASPSP has duly justified security reasons why two SCAs needed, e.g. suspicion of fraud)
  - If PISP doesn't transmit all necessary information (e.g. account selection by PSU in ASPSP domain): two SCAs is not an obstacle

- Combined AIS + PIS journey: two SCAs is not an obstacle [B&B comment: one of the two factors used to perform SCA at the time of account access can be re-used within the same session at the time that a payment is initiated, provided that (1) the other element required for SCA is carried out at the time of the payment initiation and (2) dynamic linking element is present and linked to that latter element – see Q&A2018_4141]

Bird & Bird

Area 4: 90-day re-authentication

- Some TPPs: "SCA every 90 days is an obstacle. And AISP (rather than PSU) should be allowed to perform the SCA"

- EBA:
  - the 90-days re-authentication requirement is not an obstacle
  - Obligation and responsibility to perform SCA lies with ASPSP; not TPP (unless ASPSP delegated to TPP + possible outsourcing)
  - NCAs should encourage all APSPs to make use of 90-day exemption [B&B comment: reminder: ASPSP can only show balance + transactions executed in the last 90 days]

Area 6: additional checks on consent

- A general, ex-ante consent required by the ASPSP, from the PSU, in order for PSUs to be able to use PISP/AISP is an obstacle
- For corporate accounts specifically: same principles for "authorised users" acting on behalf of the corporate

[B&B comments:
- not new; see e.g. EBA opinion of June 2018 on implementation of RTS: "ASPSPs do not have to check consent"
- link with SCA: fact that ASPSP authenticates PSU is enough confirmation of "explicit consent"
- for CISP, PSU needs to give consent to CISP **and ASPSP**]

- However, possible for PSU to request its ASPSP to deny access to its payment account(s) to one or more particular TPPs. ASPSP needs to comply with Article 68(5) PSD2 (as implemented within national laws), including "*immediately report the incident to … the competent authority*" [B&B comment: but ASPSP cannot offer the PSU the possibility to generally "opt-out" from TPP services – EBA Q&A 2018_4309]

Bird & Bird

Area 7: additional registrations

- Some registration processes are not obstacles if (1) technically necessary to ensure a secure communication with ASPSP (e.g. with ASPSP authentication app), (2) are processed in a timely manner, and (3) do not create unnecessary friction in the PSU journey

- However, additional registrations required by ASPSP to be able to access PSU payments accounts or ASPSP's production interface, that go beyond the above, are obstacles. E.g.
  - ASPSP requiring TPP to pre-register their contact details in order to access API (but if optional or agreed between parties: not an obstacle)
  - ASPSP mandatory registration steps or processes to have access to ASPSP's production API

Area 5: account selection (not SCA related)

- Requiring the PSU to manually input their IBAN into the ASPSP's domain = obstacle
- If the TPP transmits the IBAN(s) to ASPSP: ASPSP requesting the PSU to re-select the account(s) is an obstacle (but merely displaying the accounts is not an obstacle)
- If the TPP doesn't transmit the relevant account details to ASPSP:
  - If TPP is authorised to provide AIS (+ has relevant PSU consent): ASPSP to enable TPP to retrieve the list of PSU account(s), thus enabling PSU to select account(s) in TPP domain (and after that PSU selection in TPP domain, TPP to send a separate request for account access or payment initiation to ASPSP)
  - If TPP is not authorised to provide AIS (or is but hasn't received relevant PSU consent): the ASPSP "***could***" enable the PSU to select the account(s) in the APSPS domain, e.g. drop-down list or pre-populate if only one account

4. Reverse engineering – not SCA compliant?

EBA Q&A 2019_4826

- **Question from NCA (perhaps NBB?):** "*In our view,* [reverse engineering] *allows for the* ***circumvention of the application of [SCA]*** *by the ASPSP. The TPP essentially requests the PSU to enroll a second instance of the ASPSP' mobile application not on a phone under the PSU's control (possession) but on a server owned by the TPP. It is then the* ***TPP that selects the password or PIN code*** *to gain access to the mobile application and not the PSU. … Hence the [SCA] that was in place through the mobile channel (possession of phone and mobile application + knowledge of PIN/password) is now entirely replaced by what is in the* ***possession of the TPP*** *(mobile application + PIN/password). This allows for the* ***TPP to have continued access to all payment (and non-payment) accounts*** *held by the PSU and to initiate payments* ***without the PSU being involved****. Hence this technique allows for the circumvention of the requirement imposed on ASPSPs to apply* [SCA] *under Article 97 of the PSD2.*"

- **EBA answer:** "*… ASPSPs should allow TPPs, as part of the contingency mechanism in Article 33(4) of the [RTS], to use all interfaces made available by the ASPSP to its PSUs for accessing their payment accounts online directly. This includes not only the ASPSP's internet banking interface, but also the ASPSP's mobile banking application made available by the ASPSP to its PSUs, where applicable.* ***The latter does not however imply that TPPs have an automatic right to access the ASPSP's proprietary mobile banking interface that connects the ASPSP's mobile banking app to the ASPSPs' backend systems.*** *It is the ASPSP's responsibility to ensure that TPPs can be identified and can rely on the authentication procedures provided by the ASPSP to its PSUs …*

  …

  Furthermore, TPPs accessing the PSUs' payment accounts using the contingency mechanism … should also comply with their respective obligations under Article 33(5) of the Delegated Regulation, as well as with any other applicable EU legislation. ***In particular, the access by TPPs via the PSU interface(s) should not be used as a way of circumventing the application of [SCA] by the ASPSP.***"

NBB letter to Belgian PSPs (13 May 2020)

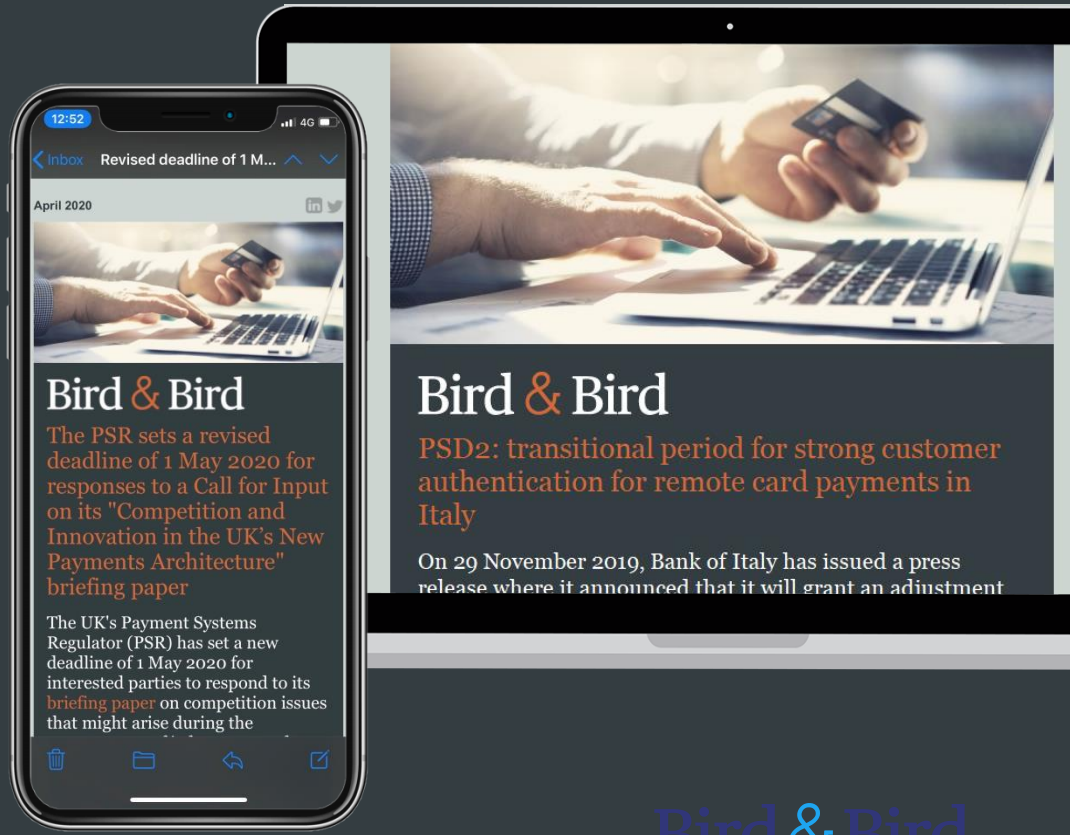
- To ASPSPs: APIs and fallback should be "in order" (i.e. compliant with PSD2, RTS, EBA guidelines on Obstacles, etc) by 31 December 2020

- To TPPs: as soon as ASPSP APIs and fallback are "in order", you should stop using RE **in order to access payment accounts** (presumably because when RE non-payment accounts, TPPs also have access to payment accounts – but, in the NBB's view, in breach of the SCA requirements related to access to payment accounts?)

[NBB also discussed RE (and screen scraping) in its "Financial Market Infrastructures and Payment Services Report 2020", published in September 2020 – see here, page 48)]

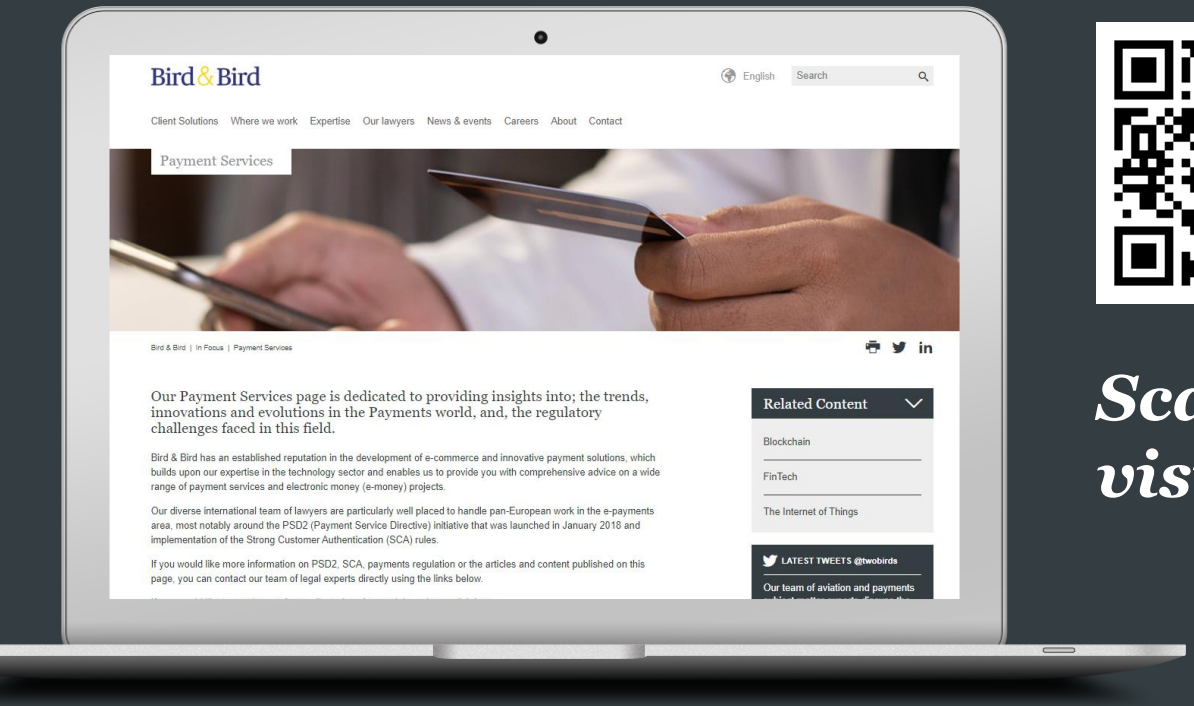
International Payments alerts

Scan the QR code or click here to sign up for our international Payments alerts



Bird & Bird

Bird & Bird In Focus page: Payment Services



Scan the QR code or visit [our website]

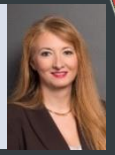
Bird & Bird

A few members of the Bird & Bird Payments team

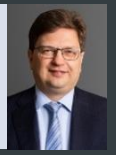
Trystan Tether
Partner
Tel: +44 20 7415 6034
trystan.tether@twobirds.com

Scott McInnes
Partner
Tel: +32 2 282 60 59
scott.mcinnes@twobirds.com

Cathie-Rosalie Joly
Partner
Tel: +33 1 42 68 67 42
cathie-rosalie.joly@twobirds.com



Dr. Michael Jünemann
Partner
Tel: +49 697 4222 6000
michael.juenemann@twobirds.com



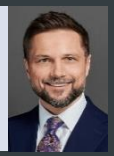
Adrian Calvo
Counsel
Tel: +34 917 90 60 83
adrian.calvo@twobirds.com

Stefano Febbi
Partner
Tel: +39 02 3035 6030
stefano.febbi@twobirds.com

Hans Svensson
Partner
Tel: +46 8 506 320 48
hans.svensson@twobirds.com

Kristiina Lehvilä
Senior Counsel
Tel: +358 9 62266756
kristiina.lehvila@twobirds.com

Slawomir Szepietowski
Partner
Tel: +48 22 583 79 13
slawomir.szepietowski@twobirds.com



Annette Printz Nielsen
Partner
Tel: +45 39 14 16 60
annette.nielsen@twobirds.com

Konrad Siegler
Partner
Tel: +36 1 301 8916
konrad.siegler@twobirds.com

Ivan Sagál
Partner
Tel: +420 226 030 509
ivan.sagal@twobirds.com

Kim Kit Ow
Partner
Tel: +65 6428 9810
kimkit.ow@twobirds.com

Michelle Chan
Partner
Tel: +852 2248 6111
michelle.chan@twobirds.com

Shane Barber
Partner
Tel: +61 2 9226 9814
shane.barber@twobirds.com

Bird & Bird

Thank you & Bird & Bird

Scott McInnes
Partner
Tel: +32 2 282 60 59
scott.mcinnes@twobirds.com

Julien Sad
Associate
Tel: +32 2 282 60 41
julien.sad@twobirds.com

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Berlin & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw