

## NAVIGATING THE TRANSITION TO PSD2: FURTHER CHALLENGES AHEAD?

13 January 2018 marked the deadline for national implementation of the revised Payment Services Directive (**PSD2**). However, this is by no means the end of the story, as some Member States have not yet transposed PSD2 into national law and several of the related guidelines and technical standards do not yet apply. This briefing considers how firms may seek to navigate this transitional period and remaining implementation challenges.

### EBA OPINION ON THE TRANSITION TO PSD2

In this context, the European Banking Authority (**EBA**) published an [opinion](#) in December 2017 to help firms navigate the transition from PSD1 to PSD2.

In the opinion, the EBA noted that only three of its 12 mandates to draft guidelines and technical standards under PSD2 (on passporting, authorisation and registration and professional indemnity insurance) would apply from 13 January. Therefore, the EBA encouraged national regulators to plan based on the most recent available version of final draft guidelines and technical standards, where relevant.

The EBA also stated that late national transposition of PSD2 should not prevent provision of cross-border services and in particular that:

- firms established in Member States that have transposed PSD2 on time should be able to exercise passporting rights under PSD2 into any other Member State; and
- firms established in Member States that have not transposed PSD2 but have already been authorised under PSD1 and have obtained a valid passport notification may continue to rely on that passport notification in order to provide cross-border services (regardless of whether they have already provided cross-border services in any given host Member State).

As discussed further below, the EBA confirmed in its opinion that third party payment service providers (**TPPs**) may continue to access payment accounts via "screen scraping" (i.e. logging in as user) until the regulatory technical standards on secure customer authentication and common and secure standards of communication (**RTS on SCA and CSC**) start to apply, likely during the second half of 2019. However, it encouraged the industry to comply with the requirements of the RTS on SCA and CSC "*as soon as possible*" (i.e.

### Summary

- EBA has confirmed that screen scraping (i.e. logging in as the user) is permitted until the RTS on SCA and CSC start to apply
- However, the industry is encouraged to comply with the requirements of the RTS on SCA and CSC as soon as possible
- UK Open Banking and various other industry projects to develop standards for open APIs are underway
- EBA intends to expand its Q&A tool to cover PSD2, including to clarify outstanding uncertainties under the RTS on SCA and CSC
- EBA is encouraging planning based on final draft guidelines and technical standards where relevant
- Late national transposition of PSD2 should not prevent provision of cross-border services

before they formally apply) and notes this will require "a degree of cooperation" between banks and FinTechs.

The EBA also stated that it is considering expanding its Q&A tool to cover PSD2 during early 2018 to address queries and provide clarity on the interpretation of EBA mandates, particularly on the RTS on SCA and CSC.

## **TPP ACCESS TO PAYMENT ACCOUNTS**

### **Status of the RTS on SCA and CSC**

The [Commission adopted](#) the final RTS on SCA and CSC on 27 November 2017, following which the European Parliament and Council have a "non-objection" period of three months (rather than the usual one month, as the Commission adopted the RTS with amendments to the EBA's draft), extendible by a further three months.

Assuming that neither the Parliament nor the Council objects to the RTS, they will then be published in the Official Journal and enter into force the following day. Most requirements will apply 18 months after entry into force, except for the interface testing requirements which will apply 12 months after entry into force.

### **TPP access under the RTS**

As expected, traditional "screen scraping", where a TPP uses the customer's own security credentials to access a customer's payment account, will be prohibited under the final RTS on SCA and CSC.

Instead, banks will need to provide TPPs and third party card issuers with a communication channel that allows access to the data they need and that enables banks and TPPs or third party card issuers to identify each other and communicate through secure messaging. Banks may either adapt their customer online banking interface or develop a dedicated TPP interface, as long as this offers the same level of availability and performance as the customer interface and does not create obstacles for access.

Where banks provide a dedicated TPP access interface, they must also develop a fallback mechanism in case the dedicated interface does not work properly, except where the national regulator has granted an exemption, on the basis that it satisfied the dedicated interface meets the quality criteria set out in the RTS.

Regulators can also revoke the exemption if the interface fails to meet those criteria for more than 2 consecutive calendar weeks and the bank must then establish a fallback mechanism within 2 months. This is unlikely to be long enough to complete the systems build needed to create a fallback TPP access mechanism. Therefore, in practice, all banks are likely to need to adapt their user interface to allow the swift establishment of a fallback TPP access mechanism.

However, banks that do benefit from an exemption are seemingly not required to "turn on" the fallback access mechanism if the dedicated interface does not work properly, at least until the national regulator formally revokes the exemption. This could cause significant disruption for fintechs in the event they find themselves unable to access payment account data, potentially for a period of up to 2 months. Therefore, the exemption from this fallback access requirement does not appear to significantly benefit banks, but may well cause problems for fintechs.

### **Development of the RTS on SCA and CSC**

- 23 February 2017: EBA final report published
- 24 May 2017: Commission letter to EBA setting out its intention to amend the RTS
- 29 June 2017: EBA opinion containing revised RTS
- 27 November 2017: Commission adopts RTS with amendments
- 26 January 2018: EBA letter to Commission highlighting remaining areas of uncertainty
- 13 February 2018: Commission response to EBA letter welcoming the EBA's intention to develop Q&A on the RTS
- 27 February 2018: Expiry of three month scrutiny period with EU Parliament and Council

In the event that a bank does not comply with the TPP access requirements set out in the RTS, national regulators will be required to "*ensure that the provision of payment initiation services and account information services is not prevented or disrupted*". However, it is not clear how national regulators would achieve this, as whilst they can impose fines and other sanctions under PSD2, they cannot actually force banks to grant access to TPPs.

### Dedicated interface testing and performance monitoring

The RTS also set out testing and performance monitoring requirements for access interfaces. The final RTS adopted by the Commission beef up requirements in previous drafts for banks to test their interfaces and to provide information about the performance and availability of dedicated interfaces, including requirements to notify TPPs and national regulators when a dedicated interface does not work properly.

The RTS require banks to provide a 6 month testing period for all TPP communication interfaces. In a statement accompanying the final RTS, the Commission indicated that this should comprise a 3-month "prototype" test and a 3-month "live test" in market conditions. However, this is not expressly reflected in the final RTS, although it could be inferred from the requirement that, in order for banks to qualify for the fallback exemption, the dedicated interface must have been "widely used" for at least 3 months.

Banks must define key performance indicators (**KPIs**) and service level targets for dedicated interfaces that are "at least as stringent" as those for user interfaces, and which will be monitored and stress-tested by national regulators. The RTS do not provide practical details about what this monitoring and stress-testing will entail for banks although again it is possible that national regulators or the EBA may provide further guidance on this.

Banks that provide a dedicated TPP interface will also be required to monitor the availability and performance of that dedicated interface on an ongoing basis. Therefore, banks that offer dedicated interfaces will need to ensure that they are able to capture and monitor performance information against KPIs and other targets. They are also required to publish this information on their website, in the form of quarterly statistics on the availability and performance of both the dedicated interface and the user interface allowing a direct comparison to be drawn. This is likely to require significant systems build for banks to be able to monitor and provide this information.

### TPP access during the transition

In its December 2017 opinion, the EBA confirmed that screen scraping, where a TPP logs into an account as if it were the payment service user (**PSU**), should be permitted until the RTS on SCA and CSC start to apply, unless national law prevented such access before PSD2 came into force on 12 January 2016.

Nevertheless, the EBA encourages all payment service providers to comply with the requirements of these RTS as soon as possible, whilst acknowledging that early adoption "*will require a degree of cooperation between all providers*" and potentially the early development of common industry standards.

Similarly in the UK, HM Treasury and the FCA have confirmed that banks must not block access via traditional "screen scraping" during the transition period, unless they provide another access route. At the same time, they are encouraging the industry to develop application programming interfaces

### TPP access to accounts

Under the final draft RTS on SCA and CSC:

- Screen scraping (where TPPs access payment accounts using customer login) will be prohibited, but only once the RTS start to apply, likely in Autumn 2019
- Banks can either adapt their customer interface or create a dedicated interface (API) to allow TPPs access to payment account data and to initiate payments
- If banks offer a dedicated interface, they also need a fallback mechanism to allow TPPs access via the customer interface in case the dedicated interface does not work properly
- National regulators can exempt banks from this fallback requirement if the dedicated interface meets quality criteria in the RTS
- However, the exemption can be withdrawn at short notice and so banks may need to adapt user interfaces to allow for TPP access in any case
- There are a number of outstanding questions and uncertainties under the RTS, in relation to which the EBA has indicated it may issue Q&A or other guidance

(APIs) as the basis for fintech access to payment accounts, and to transition to use of secure APIs "as soon as possible during 2018".

### **Interaction with Open Banking and development of industry standards**

The UK Competition and Markets Authority required the main UK retail banks to develop secure interfaces based on open API technology by 13 January 2018 under the UK Open Banking initiative (although extensions were granted to some banks shortly before this deadline). Whilst the scope of the Open Banking project is narrower than PSD2 and so will not apply to all ASPSPs and payment accounts to which TPPs may require access, HM Treasury and the FCA are encouraging ASPSPs to adopt Open Banking APIs more broadly.

The Berlin Group (a pan-European payments industry group) has also set up a dedicated task force with the goal of creating open, common and harmonised European API standards to enable TPPs to access bank accounts under PSD2 and released a first version of its framework on 8 February 2018.

In a recent speech from 20 February 2018, ECB executive board member Yves Mersch also encouraged the industry to "agree on one common technical specification so that the whole of Europe could base their systems upon one or a few technical API standards", stating that "[t]his will greatly facilitate market entry, avoid fragmentation and allow for competition at the service level, avoiding obstacles at the technical level".

Mersch noted that the Commission has invited market participants to establish an API Evaluation Group, which has just started work. In its letter dated 13 February 2018, the Commission also encouraged the EBA to participate in this evaluation group and take up issues discussed in that group in the Q&A tool that the EBA is envisaging for PSD2 and the RTS.

### **OUTSTANDING QUESTIONS FOR TPP ACCESS**

As noted in the EBA's letter to the Commission dated 26 January 2018, there are a number of outstanding questions about how the TPP access requirements under the RTS should be interpreted. In that letter, the EBA expressed concerns that these new amendments "may impose significant additional administrative and operational burden" on payment service providers (PSPs) and that some of the changes "leave significant room for interpretation, and increase the risk of unlevel playing field".

#### **Obstacles for TPP access**

Article 32 of the RTS provides that a dedicated TPP communication interface must not create obstacles for access, which may include (inter alia):

- preventing TPPs or third party card issuers from using the credentials issued by banks to their customers; or
- imposing redirection to the bank's authentication or other functions.

The RTS do not expressly state whether or not these examples would always be considered obstacles for access. However, the wording "may include..." suggests that there may be circumstances where they do not in fact present obstacles to TPP access.

This seems consistent with a common sense approach, as if banks were unable to restrict use of credentials issued to PSUs in any way, this would seem to contradict the ban on screen scraping (where a TPP accesses an account using the PSU's login details).

Similarly, there is a question as to whether all redirection models would be considered "obstacles" to TPP access, or whether some redirection models may be permitted – and if so, how permitted models can be identified.

This is an important issue, as the open API standards developed under the UK Open Banking initiative are based on a redirect model and the open API standards being developed by the Berlin Group also include standards based on a redirect model.

#### **Eligibility for an exemption from fallback access**

In addition, the criteria that a dedicated TPP access interface must meet before a bank can be granted an exemption from the fallback access requirement include requirements that the interface has been designed and tested "*to the satisfaction of*" TPPs and third party card issuers and "*widely used for at least three months*" by them. Banks must also ensure that any problem with the dedicated interface is resolved "*without undue delay*".

It is not clear from the RTS what banks will need to do in practice to satisfy these requirements. For example, do banks need written confirmation that TPPs and card issuers are satisfied with the interface? If so, how many TPPs and card issuers need to provide this confirmation and what if there is mixed feedback? Similarly, further guidance will be needed in relation to whether an interface is "widely used" and what counts as "undue delay", as these terms are open to different interpretations.

The Commission has tried to address the risk of national regulators interpreting these requirements differently by requiring regulators to consult with the EBA before granting the exemption. In a letter dated 13 February 2018, the Commission also welcomed the EBA's intention to extend its Q&A tool to provide clarity on the interpretation of these RTS. Therefore, the EBA may provide further guidance on these requirements in due course.





## CONTACTS

**Kikun Alo**  
Senior Associate

**T** +44 207006 4067  
**E** Kikun.Alo  
@cliffordchance.com

**Simon Crown**  
Partner

**T** +44 20 7006 2944  
**E** Simon.Crown  
@cliffordchance.com

**Caroline Meinertz**  
Partner

**T** +44 20 7006 4253  
**E** Caroline.Meinertz  
@cliffordchance.com

**Sarah Butler**  
Lawyer

**T** +44 20 7006 2773  
**E** Sarah.Butler  
@cliffordchance.com

**Laura Douglas**  
Professional Support  
Lawyer

**T** +44 20 7006 1113  
**E** Laura.Douglas  
@cliffordchance.com

**Meera Ragma**  
Lawyer

**T** +44 20 7006 5421  
**E** Meera.Ragma  
@cliffordchance.com

**Peter Chapman**  
Senior Associate

**T** +44 20 7006 1896  
**E** Peter.Chapman  
@cliffordchance.com

**Mardi MacGregor**  
Lawyer

**T** +44 20 7006 3354  
**E** Mardi.MacGregor  
@cliffordchance.com

**Maria Troullinou**  
Senior Associate

**T** +44 20 7006 2373  
**E** Maria.Troullinou  
@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

[www.cliffordchance.com](http://www.cliffordchance.com)

Clifford Chance, 10 Upper Bank Street,  
London, E14 5JJ

© Clifford Chance 2017

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street,  
London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to [nomorecontact@cliffordchance.com](mailto:nomorecontact@cliffordchance.com) or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Bangkok •  
Barcelona • Beijing • Brussels • Bucharest •  
Casablanca • Dubai • Düsseldorf • Frankfurt •  
Hong Kong • Istanbul • Jakarta\* • London •  
Luxembourg • Madrid • Milan • Moscow •  
Munich • New York • Paris • Perth • Prague •  
Rome • São Paulo • Seoul • Shanghai •  
Singapore • Sydney • Tokyo • Warsaw •  
Washington, D.C.

\*Linda Widyati & Partners in association with  
Clifford Chance.

Clifford Chance has a co-operation agreement  
with Abuhimed Alsheikh Alhagbani Law Firm  
in Riyadh.

Clifford Chance has a best friends relationship  
with Redcliffe Partners in Ukraine.