Tim Wright Partner
tim.wright@pillsburylaw.com
Pillsbury Winthrop Shaw Pittman LLP, London

Implementing the EBA's technical standards

The second Payment Services Directive (Directive (EU) 2015/2366) ('PSD2') is a game changer. It not only focuses on tightening the payments sector's operating model, but also requires banks and other payments providers to open their infrastructure and customer data assets to third-party payment service providers ('PSPs') to enable them to develop new products, bringing PSPs into the scope of regulation for the first time. To this end, the PSD2 mandates certain standards and requirements intended to enable consumers to benefit from safer and more innovative electronic payments. The regulatory technical standards ('RTS') of the European Banking Authority ('EBA') on strong customer authentication ('SCA') and common and secure communication ('CSC') and the underlying Regulation (EU) 2018/389 underpin the new security requirements under the PSD2, regulating access by account information service providers ('AISPs') and payment initiation service providers ('PISPs') to customer payment account data held by account servicing payment service providers ('ASPSPs'). The EBA published the RTS on SCA and CSC in the Official Journal on 13 March 2018. It will have legal application from 14 September 2019. Tim Wright, Partner at Pillsbury Winthrop Shaw Pittman LLP, discusses the EBA's RTS.

Smooth and transparent implementation

Market participants must develop and/or enhance their hardware, software, operating procedures and documentation and, in the case of ASPSPs, establish and maintain interfaces and infrastructure to enable access by PSPs. The EBA and the national competent authorities ('NCAs') received "numerous queries" from market participants about the implementation of certain aspects of the RTS, which needed answering to enable interfaces and infrastructures to be built in a manner compliant with the RTS. So, on 13 June 2018, the EBA published two papers intended to clarify these issues: one an opinion (EBA-Op-2018-04) and the other a consultation paper (EBA/CP/2018/09).

Given the PSD2's objectives of contributing to a single EU payments market, the EBA and the NCAs have a common interest in ensuring that these measures are implemented in a consistent way across the EU. With these and other measures, such as the extension of the EBA's Interactive Single Rulebook, the EBA aims to provide assistance to market participants to ensure a smooth and transparent implementation of the RTS on SCA and CSC. With this in mind, the EBA has focused 'in particular on those queries for which clarity is required sooner, to enable industry players to continue in their preparations and to facilitate early readiness to comply with the RTS.'

The opinion

The opinion focuses on the implementation of the RTS. Although addressed to the NCAs, it should prove useful to PSPs and others. It identifies certain 'pressing' areas, including: exemptions to SCA; consent; the scope of data; and methods of carrying out SCA.

Exemptions from the SCA requirement

The opinion also contains a helpful table, which specifies the exemptions available to PSPs under Articles 10-18 of the RTS on SCA and CSC, depending on which payment instrument is to execute a transaction (See Figure 1 overleaf). Only one exemption needs to be applied for any given transaction, even if it qualifies for more than one. The opinion also clarifies that payees can never decide whether to use an exemption.

Consent

The opinion explains that ASPSPs should not check the consent of the payment service user who has contracted with an AISP, PISP or card-based payment instrument issuer ('CBPII') and that it is the ASPSP that must employ SCA and determine whether an exemption should be applied. Further, when determining which method(s) to use to carry out the authentication procedure, the ASPSP must ensure that all SCA methods can be supported when using the application programming interface ('API').

The scope of data

When the RTS apply, the data that payment account holders will be able to see will comprise a core set of data that is common across most providers, but there may be variations among them. According to the EBA, this means that the data that AISPs can access may vary, depending on the ASPSP with which the payment account is held. The extent and scope of the data may also vary, depending on the channel used by the customer (and in particular between web interfaces and mobile (or tablet) apps). AISPs can access the maximum amount

Figure 1: Exemptions available to PSPs under Articles 10-18 of the RTS on SCA and CSC

RTS article	Exemption	Payer's PSP	Payee's PSP	
			Credit transfers	Cards
Access to information	Access to payment account information	Yes	N/A	N/A
Article 11	Contactless payments at point of sale ('POS')	Yes	No	Yes*
Article 12	Unattended terminal for transport and parking	Yes	No	Yes*
Article 13	Trusted beneficiaries	Yes	No	No
Article 14	Recurring transactions	Yes	No	Yes*
Article 15	Credit transfers to self	Yes	No	N/A
Article 16	Low-value transactions	Yes	No	Yes*
Article 17	Secure corporate payments processes and protocols	Yes	No	N/A
Article 18	Transaction risk analysis	Yes	No	Yes*

*The payer's PSP always makes the ultimate decision on whether to accept or apply an exemption; the payer's PSP may wish to revert to applying SCA to execute the transaction, if technically feasible, or to decline the initiation of the transaction.

continued

of data available to payment service users with regard to their payment account(s) held with a specific ASPSP, regardless of the electronic channel (e.g. mobile application or web) used to access it. In other words, if more data is available through a computer connection online than through a mobile app, the AISP is able to access data available online via the interface, regardless of the channel used by the payment service user to access the AISP.

Methods of carrying out SCA

The EBA identifies three main methods of carrying out the authentication procedure of the payment service user through a dedicated interface, and APIs in particular: redirection, embedded approaches and decoupled approaches (or a combination thereof). In the cases of redirection and decoupled approaches, the payment service user's authentication data is exchanged directly between payment service users and ASPSPs. Embedded approaches are different: the payment service user's authentication data is exchanged between third-party providers and ASPSPs through the interface. A number of national markets have seen ASPSPs traditionally using redirection, while in other markets they have used a more embedded approach.

When determining which method(s) to use for the purpose of carrying out the authentication procedure, in line with Article 97(5) of the PSD2 and Article 30(2) of the RTS, all methods of SCA provided to the payment service user need to be supported when an AISP or PISP is used (if they were not, this would constitute an obstacle to the provision of AISP and PISP). Which method, or combination of methods, any particular ASPSP needs to use will, therefore, depend on the authentication procedures that it offers to its own payment service users.

Further clarification

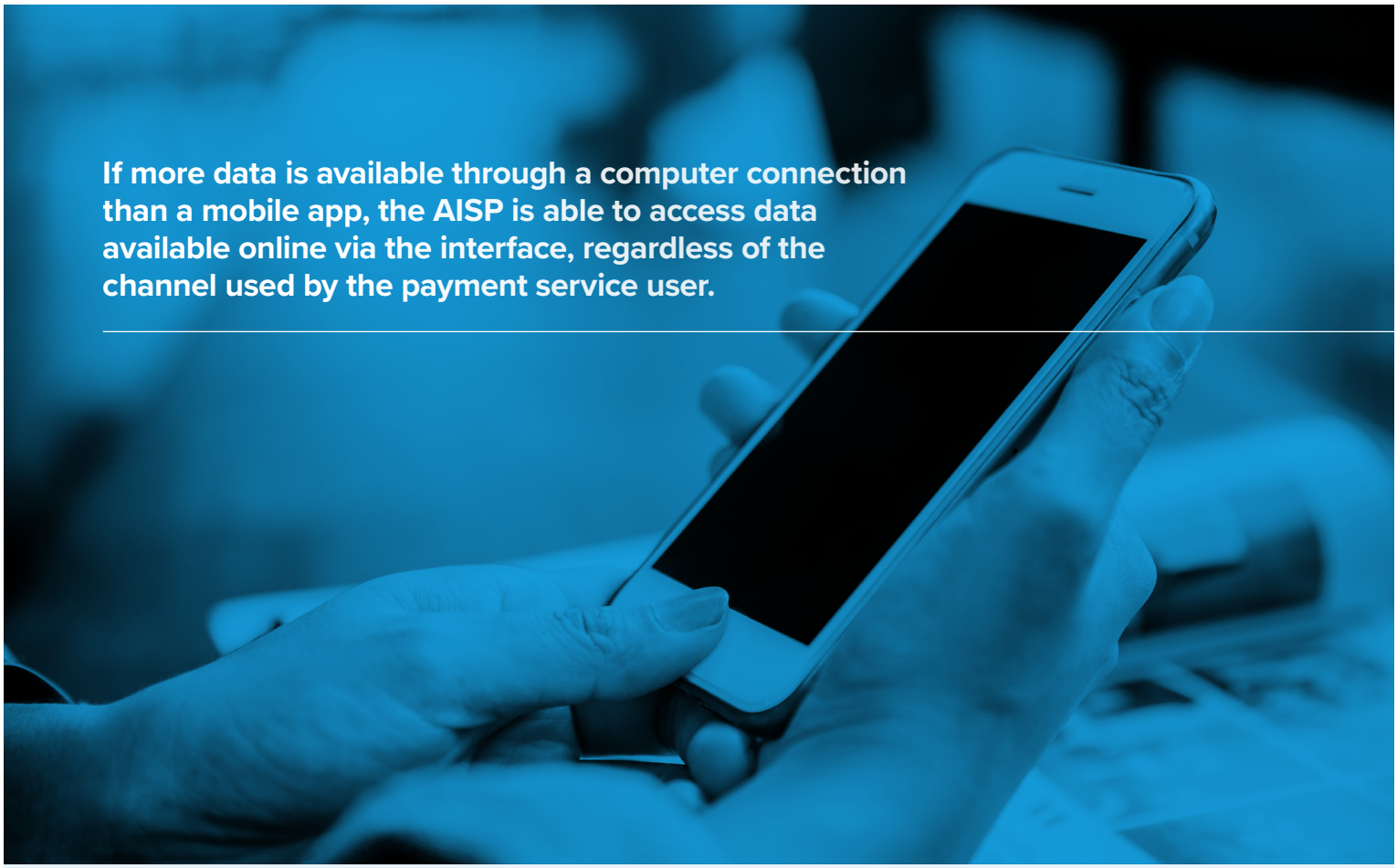
The EBA provides further clarification on interpretation of the RTS on SCA and CSC through its Interactive Single Rulebook. The Rulebook is an online tool that provides a comprehensive compendium of the level 1 text for the Capital Requirements Regulation (Regulation (EU) 2013/575) and the Capital Requirements Directive (Directive (EU) 2013/36); the Bank Recovery and Resolution Directive (Directive (EU) 2014/59); and the Deposit Guarantee Schemes Directive (Directive (EU) 1994/19), as well as the PSD2, and the corresponding technical standards developed by the EBA and adopted by the European Commission, the EBA Guidelines and related Q&As. The Q&A tool has been extended to PSD2-related queries, and those related to the EBA's level 2 legislation.

The consultation

ASPSPs can choose between, on the one hand, offering a dedicated interface for communicating with AISPs, PISPs and CBPIIs, and on the other, offering the interface for identification and communication with the ASPSP's payment service users. Where the dedicated interface is chosen, the ASPSP must establish contingency measures (a fallback interface) in the event of unavailability of, or performance issues affecting, the dedicated interface.

However, Article 33(6) of Regulation (EU) 2018/389, the regulation that sets outs the RTS, provides an exemption to the requirement that ASPSPs implement the fallback interface where they can demonstrate that the dedicated interface meets the following four specific conditions, which are described in more detail in the RTS, but summarised here as: (1) obligations for the dedicated interface; (2) designed and tested for the satisfaction of PSPs; (3) dedicated interface has been widely used; and (4) resolution of problems.

The operation of the exemption was one of the key issues raised by market participants with the EBA and the NCAs, with much uncertainty surfacing as to the information to be considered for each of the four conditions. The problem stems from the Article 33(6) conditions being high level and formulated on the assumption that the dedicated interface has been operative for some time so that the conditions can be assessed by the



If more data is available through a computer connection than a mobile app, the AISP is able to access data available online via the interface, regardless of the channel used by the payment service user.

NCAs. The timeline creates difficulties for ASPSPs seeking exemption prior to the September 2019 'go live,' given that these ASPSPs are seeking an exemption ahead of the RTS applying and before the dedicated interface - for most ASPSPs - has been used operationally.

The EBA's consultation paper seeks to clarify these requirements, and the information that the NCAs should consider when reviewing applications for exemption from ASPSPs, with the aim of delivering consistent application of the rules across the EU - not least because Article 33(6) also requires competent authorities to consult with the EBA prior to granting any exemption in favour of an ASPSP. The draft guidelines are intended to enable competent authorities to carry out a quick assessment of exemption requests. This should enable the NCAs to apply a pragmatic and consistent approach to the four conditions when assessing exemption requests, which should be very helpful - especially during the period in which the bulk of exemption requests is expected to be received (i.e. from now until 14 September 2019).

The requirements proposed in the draft guidelines also provide clarity on service level, availability and performance of the interface that ASPSPs must have in place; the publication of performance indicators; the stress testing to be carried out; obstacles to accessing payment accounts; the design and testing of the interfaces (to meet the requirements of the PSPs); the wide usage of the interface; problem resolution; and the NCAs' consultation with the EBA. Comments on the consultation, which will close on 13 August 2018, can be submitted via the EBA's website. A public hearing to discuss the draft guidelines was held on 25 July at the EBA's London premises. The finalised guidelines will apply from 1 January 2019.

Data in the payments industry

The EBA's papers coincided with a discussion paper (DP18/1) published by the UK Payment Systems Regulator ('PSR'), which it launched on 12 June 2018. Called 'Data in the payments industry,' the paper reflects that as non-cash payment methods have increased, so has the amount of payments data that has been generated. The UK payments sector is evolving fast, and the PSR expects that data will have a key role to play, with changes in the sector being driven by a variety of market, technical, end-use and regulatory factors, all of which have data at their core. This raises questions about who has access to the data - whether for the development of innovative products or for the security of the data from a cyber attack.

Following on from research completed during its scoping exercise, and evidence presented by the Payments Strategy Forum, the PSR now wants to better inform its own thinking about the potential impact of data on issues relevant to its objectives, so that it can understand, within the context of its statutory remit, the opportunities and potential risks presented by the changing treatment of data in the payments industry and see whether there are areas in which the PSR should consider developing policies or taking action. In particular, data protection provisions under PSD2, as well as the General Data Protection Regulation (Regulation (EU) 2016/679) and Open Banking, are changing the existing landscape and giving consumers far greater control over how their data is used and who it is shared with. The PSR seeks comments by close of business on 3 September 2018.

Change as the new normal

The PSR and the EBA clearly recognise the pace of change in the sector. The EBA, for example, foresees, given the pace of change in the payments market, wider acceptance of the new services, and dedicated interfaces becoming a more familiar feature of the payments landscape, meaning that it will probably have to review the guidelines sooner than is usual. Similarly, the PSR is focusing on the pace of technological change "which is leading to payments data being collected, processed, shared and used in digital form at lower cost and on a larger scale than ever before."