HM Treasury

FINANCIAL CONDUCT AUTHORITY

Expectations for the third party access provisions in Payment Services Directive II

July 2017

Expectations for the third party access provisions in PSDII

1.1 From 13 January 2018, the second Payment Services Directive (PSDII) mandates that Account Servicing Payment Service Providers (ASPSPs),[1] that provide payment accounts that are accessible online, must:

- make available payment account data to account information service providers (AISPs)
- allow payment initiation service providers (PISPs) to initiate transactions from customers' accounts

1.2 Businesses seeking to carry out these activities (AISPs and PISPs) and benefit from the right to access the account will need to be registered or authorised. AISPs or PISPs must always have the necessary consent of the payment user in order to carry out their services.

1.3 Alongside the regulations, this communication sets out further detail on HM Treasury and the Financial Conduct Authority's (FCA) expectations for PSDII implementation. This is intended to support firms in their PSDII implementation, given the short period left for firms to take steps to meet their obligations for 13 January 2018.

Background

1.4 The implementation of PSDII into UK law, and its application from 13 January 2018, marks the first step in bringing about access for third parties. The application of forthcoming regulatory technical standards on Strong Customer Authentication and Common and Secure Communication will mark the second step ('the RTS'). We recognise that there remains uncertainty as to the final content of the RTS.

1.5 By opening up access, PSDII will create the opportunity for the development of a whole range of new and innovative account information and payment initiation services. These services have the potential to significantly benefit consumers (as well as providers and the wider economy) by making it easier for consumers to manage their finances and by providing a range of alternative payment options to traditional card payments.

1.6 Our goal is to ensure that the implementation of PSDII supports greater competition and innovation, in a manner that is safe, secure and in the interests of customers. HM Treasury and the FCA recognise that the period until the RTS applies represents a transitional period for industry participants and customers. While the RTS might prescribe how this safety and security is to be delivered in future, we expect firms to adhere to the principles of safety and security from day one (i.e. 13 January 2018). For example, we expect that the firms concerned should:

- transmit credentials and data securely, in ways that safeguard against the risks of interception
- be transparent and open about their identities when interacting with one another, in order to limit the potential for criminal actors to operate in this space
- ensure that data are stored in ways that mitigate the risks of illegitimate access, and that credentials are only held if permitted under PSDII

[1] including banks, building societies, credit card issuers, e-money institutions, and other Payment Service Providers (PSPs)

Use of application programming interfaces (APIs)

1.7 While PSDII prevents HM Treasury or the FCA from mandating a particular method of access, we believe that the use of secure application programming interfaces (APIs) provides significant advantages. In line with the Competition and Market Authority's (CMA) order on Open Banking, which applies to nine UK banks, we believe there are benefits to customers and market participants if these APIs are developed according to common standards and using secure common infrastructure where necessary – 'the Open Banking Standard'. Such standardisation will support innovation by reducing barriers to entry – as third parties will not have to integrate with different technology on a firm-by-firm basis - and can enhance security across the industry.

1.8 While the CMA's order on Open Banking applies to a more limited number of products and providers than are affected by PSDII, the view of HM Treasury and the FCA is that the Open Banking approach will become the most suitable option for firms once the Open Banking Implementation Entity has delivered a solution that enables them to comply with all their obligations under PSDII and the RTS. We therefore encourage ASPSPs, AISPs and PISPs to work towards using the Open Banking API Standards as the basis on which secure API access to other payment accounts is provided in future. And we encourage prospective AISPs and PISPs to work with ASPSPs to transition to the use of secure APIs as soon as possible during 2018. By adopting Open Banking APIs, the UK can establish itself as a global thought leader in the safe and effective sharing of banking data.

The pre-RTS period

1.9 During the pre-RTS period, HM Treasury and the FCA expect firms to act to ensure good customer outcomes and to deliver the competition and innovation in the market that is being sought. In order to ensure this transition is orderly, a degree of cooperation between firms is to be expected, and indeed encouraged.

1.10 During this period, ASPSPs must not block the access of registered and authorised AISPs and PISPs except for reasonably justified and duly evidenced reasons related to unauthorised or fraudulent access or payments. This includes not blocking access via "screen scraping" (where the firm logs in to an account as if they are the user) unless the ASPSP provides another access route which AISPs and PISPs can use without having to comply with requirements yet to come into force. ASPSPs must also not take steps to dissuade customers from using these newly-regulated competitors' services, for instance through their communications or terms and conditions.

1.11 During the pre-RTS period, while AISPs and PISPs will not be legally required to identify themselves to ASPSPs when they are accessing customer accounts, they should be transparent and open about their identities when interacting with ASPSPs. In addition, all firms – whether an ASPSP, AISP or PISP – are required to have in place policies and procedures to monitor, identify and prevent fraud. We are aware that the approaches ASPSPs, AISPs and PISPs take to their interactions, and the steps they take to stop fraud and cybercrime, will continue to develop.

Registration and authorisation

1.12 All firms which started to operate as an AISP or PISP on or after 12 January 2016, that wish to operate as AISPs or PISPs must be registered or authorised by the FCA before 13 January 2018.

1.13 Firms operating as an AISP or PISP before 12 January 2016 will be able to continue to operate without registration or authorisation prior to the RTS, but they will not benefit from the right of access provided for in PSDII (we would discourage ASPSPs from adopting a blanket policy of blocking these firms). We would strongly encourage these AISPs and PISPs to apply to be registered or authorised as soon as possible, given the real and significant benefits to these

firms of doing so, and we would expect many of these firms to choose to become registered or authorised well ahead of the RTS.

1.14 The Payment Services Regulations 2017 allow for applications from 13 October 2017, to enable firms to apply and be registered or authorised by 13 January 2018. The FCA has up to three months to determine an application, providing it is complete. It is in firms' interests that applications are received as early as possible.

1.15 As with all applications, the FCA will take a proportionate approach to their assessment. It is the responsibility of the firm applying for registration or authorisation to ensure they can meet the requirements. Applications will be processed effectively and efficiently, taking into account the likely risks posed by the firm operating in a particular sub-sector. The information the FCA rely on and ask for, and the level of scrutiny the FCA apply, will vary according to the perceived risk and complexity inherent in the applicant firm's proposed business model.

1.16 HM Treasury and the FCA recognise that the requirement for AISPs and PISPs to have in place professional indemnity insurance is causing some uncertainty due to the perceived lack of an existing market for insurance that meets the minimum standards of cover set out in European Banking Authority (EBA) guidelines. HM Treasury and the FCA are working with market participants and the insurance industry to understand and address this issue.

1.17 With regards to the security requirements, until the RTS, the FCA will be assessing applicants against the EBA's Authorisation Guidelines. The FCA will consider applicants' security policies, governance, business continuity arrangements, and access to sensitive data processes as described in those guidelines, taking into account firms' business models.

1.18 At the entry point the FCA will look in detail at applicants' security policies, governance, business continuity arrangements, and access to sensitive data processes as described in the Authorisation Guidelines. It is the responsibility of the FCA to validate the adequacy of the firms' approach to these details. It is the responsibility of the firm to test the effectiveness of their approach. The draft RTS provides firms with some sense of what future requirements will be. Once the content of the RTS is settled the FCA will expect AISPs and PISPs to demonstrate how they intend to comply with these requirements at the authorisations gateway.

1.19 PSDII also requires that directors or persons responsible for the management of the institution possess appropriate knowledge and experience to perform payment services and the level of this should be proportionate to the nature, complexity and scale of risk inherent in the business activity.

1.20 There are also various conduct of business rules, rules around data protection and customer consent, and rules around information security that will apply to firms from 13 January 2018. It will be important for the FCA to understand from the firm's application how it intends to meet these requirements. It will also be important for the FCA to understand the firm's cyber risk remediation.