Payment Services Directive 2: Open Up!

Nandini Sur | 26 September 2017

1. Introduction

What do the dentist and the Payment Services Directive 2 (PSD2) have in common? They both want you to open up!

On 18 July 2017, the UK published the final form of the Payment Services Regulation 2017 (PSRs 2017), the UK implementation of the PSD2 which comes into force on 13 January 2018. The PSRs 2017 introduce a host of new provisions that require providers of payment accounts (including for example banks) to allow third parties (such as payment initiation service providers like PayPal and account information service providers like OnTrees) access to clients' payment accounts.

These new requirements are particularly challenging for established payment service providers like banks to implement not in the least due to legacy IT systems that were designed to prevent access by third parties for data security reasons. To add further toothache, firms providing payment accounts will have to make changes to their risk and IT security to adapt to the new requirements.

The new provisions in the PSRs 2017 requiring account servicing payment service providers (ASPSPs) to provide third parties with access to clients' payment accounts can be found in regulation 68 which deals with the availability of funds for card-based payment transactions; regulation 69, which deals with the access to payment initiation services and regulation 70, which concerns access to account information services.

2. Availability of Funds for Card-Based Payment Transactions

A payment service provider (PSP) that issues card-based payment instruments (e.g. debit or credit cards) may request that an ASPSP (which includes businesses that provide payment accounts such as banks and credit card providers) confirm whether an amount necessary for the execution of a card-based payment transaction is available on the payment account of the payer. An ASPSP must provide the requested confirmation immediately in a yes or no answer where: (1) the account is a payment account *accessible online* when the ASPSP receives the request and (2) before the first occasion on which a request is received, the customer has given their explicit consent to the ASPSP that they can provide confirmation in respect to such requests from the PSP who has issued the card-based payment instrument.

As noted above, the ASPSP is required to provide a yes or no answer on the availability of the amount of funds immediately. According to the Financial Conduct Authority's final Approach Document on payment services and electronic money published in September 2017 (FCA Approach Document), immediately is considered to mean sufficiently fast so as not to cause any material delay on the payment

transaction and therefore, is likely to mean that the answer must be provided as soon as the request is received.

The FCA Approach Document clarifies that consent from the client must be specific and relate to the specific card-based payment instrument issuer (CPBII) making the request. It would not be sufficient to include blanket wording in a framework contract where the customer consents to the ASPSP confirming availability of funds for all CBPIIs. According to the FCA Approach Document, as explicit consent is required before the first occasion on which a request is made, consent is not required in respect of each transaction from the CBPII. However, the explicit consent obtained from the ASPSP must relate to the specific CBPII making requests.

The FCA Approach Document confirms that ASPSPs are not obliged to respond to requests from CBPIIs before the strong customer authentication regulatory technical standards apply, which is expected to be in mid-2019.

3. Access to Payment Initiation Services

Many merchants offer customers the ability to log into payment providers (such as PayPal) to enable the customer to pay for goods or services directly through their bank account without the need to provide any banking or credit card information. These providers, known as payment initiation service providers (PISPs), were previously unregulated but have now been brought into regulation by the PSRs 2017.

Where a payer gives explicit consent for a payment to be initiated through a PISP such as PayPal, Regulation 69 of the PSRs 2017 requires the payer's ASPSP to provide or make available to the PISP information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of payment transactions. The FCA Approach Document confirms that this requirement would include, as a minimum, the information that would be provided or made available to the customer directly if the customer initiated a payment and would include information regarding a failure or refusal to execute a transaction.

In order to protect consumer data including payment details, Regulation 69 also requires banks to communicate with the PISP using strong customer authentication measures to ensure security of consumer data, treat the payment order in the same way as a payment order received directly from the payer and not require the PISP to enter into a contract for the provision of such services. The FCA expects ASPSPs to provide customers using PISPs with the same level of functionality as the customer would have if the payment were initiated directly with their ASPSP.

Regulation 69 is only applicable to "payment accounts" which are accessible online. While "accessible online" is not defined in the PSRs 2017, the FCA Approach Document states that an account is accessible online in this context if the ASPSP offers online banking services in relation to that account. Thus, if an ASPSP offers customers the ability to make payment transactions online, Regulation 69 will apply. On the other hand, if the ASPSP does not provide its customers with any payment functionality, such an account would not be accessible online for the purposes of payment initiation services.

4. Access to Account Information Services

Account information service providers, a relatively new entrant to the market, include applications such as You Need a Budget and OnTrees which provide users with a

holistic picture of their finances. By logging into a single website or application provided by such an account information service provider (AISP), users can see everything from their mortgage payments due to Bank A to investment portfolios the user holds with Bank B to the user's current account balance with Bank C. As with PISPs, this previously unregulated service will be regulated under the PSRs 2017.

Where a payment service user uses an account information service, Regulation 70 requires that the ASPSP must treat a data request from the AISP in the same way as a data request received directly from the payer, unless the ASPSP has objective reasons for treating the request differently, such as for example anti-money laundering concerns. As with Regulation 69, Regulation 70 also requires ASPSPs to communicate with the AISP using strong customer authentication and also does not require the AISP to enter into a contract with the ASPSP for the provision of such services. Further, unlike with PISPs, consent for the provision of account information services is provided to the AISP rather than the ASPSP.

Regulation 70 also only applies in this context to payment accounts "accessible online". The FCA Approach Document states that an account that is available online on a view only basis would be considered accessible online for the purposes of account information services. Given the majority of payment accounts can be viewed online, the requirement for ASPSPs to provide AISPs access will be far-reaching. Furthermore, the FCA expects ASPSPs to make the same information available to a customer via an AISP as would be available to the customer if they accessed their account online directly through the ASPSP.

One can see how requiring a bank to provide access to AISPs is in line with the PSD2's purpose of increasing transparency and competition in the payments industry as AISPs will likely suggest cheaper alternatives to the user's banking products (e.g. better rates for mortgages or higher yielding interest accounts).

5. Payment Accounts

The common thread in regulations 68, 69 and 70 discussed above is that the regulations are only applicable to a "payment account" which is defined in the PSRs 2017 as "an account held in the name of one or more payment service users which is used for the execution of payment transactions".

FCA's guidance regarding payment accounts states that in determining whether an account is a payment account, it is appropriate to focus on the underlying purpose of the account. Payment accounts can include, for example, current accounts, e-money accounts, flexible savings accounts, credit card accounts and current account mortgages. What the account is called is not decisive in determining whether it is a payment account. On the other hand, in the FCA's view fixed term deposit accounts (where there are restrictions on the ability to make withdrawals), child trust fund deposit accounts and certain cash Individual Savings Accounts are not payment accounts.

Most high-street and private banks will be caught by the requirements discussed above given they provide accounts that allow users to make payment transactions. However, in other cases whether an account is a payment account needs to be considered on a case-by-case basis taking account of relevant exceptions under the PSRs 2017 and the FCA guidance referred to above.

If you require further information on anything covered in this briefing please contact Nandini Sur (nandini.sur@farrer.co.uk; +44(0)203 375 7990), Grania Baird (grania.baird@farrer.co.uk; +44(0)203 375 7443) or your usual contact at the firm on 020 3375 7000. Further information can also be found on the Compliance & Regulatory page on our website.

6. Conclusion

In the coming months and after the implementation of the PSRs 2017, we are likely to see increased competition in both the PISP and AISP arenas with the growing influence of various FinTech players. These entities should be in a better position to comply with the PSRs 2017 particularly in relation to the strong customer authentication requirements due to be implemented in 2019 since their systems can be built with the PSRs 2017 in mind. Already established banks with legacy IT systems are in a more difficult position. Banks that have not already done so will need to determine how they can comply with the requirements to provide access to clients' accounts while maintaining the security of customer data.