Skadden


If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

**Azad Ali**
Of Counsel / London
44.20.7519.7034
azad.ali@skadden.com

**Olivia Moul**
Trainee Solicitor / London
44.20.7519.7636
olivia.moul@skadden.com

**David Y. Wang**
Associate / London
44.20.7519.7149
david.y.wang@skadden.com



One Manhattan West
New York, NY 10001
212.735.3000

22 Bishopsgate
London EC2N 4BQ
44.20.7519.7000

## EU's Proposed Revisions to the Payment Services Directive, and How They Compare to the UK's Approach

On 28 June 2023, the European Commission (EC) published its proposals for both a revised Payment Services Directive (PSD3) and a new accompanying Payment Services Regulation (EU PSR). This package of reforms addresses certain key issues arising from the operation of the Second Payment Services Directive (PSD2) and sets out specific enhancements to PSD2.

As a directive, PSD3 will require transposition into member states' national legislation. The EU PSR, in contrast, will be directly applicable, with no implementation required. The intention of the directly applicable regulation is to mitigate member states' divergent interpretational approaches to certain aspects of PSD2.

Among other things, the proposed updates to PSD2 include:

- A merger of the regimes applicable to e-money institutions (EMIs) and payment institutions (PIs). This simplifies and harmonises these two very similar regimes, with PIs being authorised to offer e-money services as part of their wider payment services business.
- An extension of fraud protection measures, including:
  - IBAN/name-matching verification for euro-denominated instant payments.
  - Refunds for customers who fall victim due to lack of such verification and, subject to some exceptions, to impersonation fraud.
- Clarifications to Strong Customer Authentication (SCA) requirements, including that SCA be conducted by underlying account providers such as banks only once at the outset, when access is sought by open banking account information service providers.
- Various transparency reforms relating to costs and charges for remittances to non-EU countries and ATM withdrawal charges.
- Reforms to Open Banking: Banks will no longer need to maintain two data access interfaces (a dedicated and a "fallback interface) for customer data, and contingent data access could possibly include the use of the interface banks for their customers. The EC is also presenting proposals in a separate regulation on wider financial data access, expanding beyond account information to other financial products, thereby broadening the scope of Open Banking to wider Open Finance.
- Improvement to access by PIs to bank account services, by requiring banks to justify refusal of such services on specific grounds.

### The UK Regime

In the UK, PSD2 was implemented by way of the Payment Services Regulations 2017 (UK PSRs). The UK has been more advanced that its continental counterparts in respect of certain aspects of the payment services landscape. Notably, it has embraced Open Banking through the work of the Open Banking Implementation Entity (OBIE) and by encouraging a strong ecosystem of fintech firms in the UK.

The future of Open Banking in the UK will be overseen by the Joint Regulatory Oversight Committee (JROC), comprised of representatives from the Financial Conduct Authority (FCA), the Payment Systems Regulator, HM Treasury and the Competition and Markets Authority (CMA). In January 2023, HM Treasury issued a consultation on the UK PSRs, in which it recognised certain areas for review. Some of these areas are also addressed in the proposed PSD3 and EU PSR, but overall, the UK can be said to be pursuing its own path to reforming and evolving the UK payment services regulatory framework.

### Comparison of EU and the UK Reforms of PSD2

#### Strong Customer Authentication

It is well documented that a rise in the use of digital payments and online banking has seen a concomitant increase in fraud. As payment transactions have become increasingly frictionless, the requirements of SCA (a form of regulatory, two-factor authentication) prescribed by PSD2 have sought to ensure greater protection against fraud for payment transactions in both online and contactless offline payments. These rules have had a significant impact in reducing fraud.

The EC proposals now seek to clarify certain features of SCA rules. For example, payment service providers (PSPs) must have transaction monitoring mechanisms in place that could, in certain cases, trigger the application of SCA, helping to prevent and detect potentially fraudulent payment transactions.

The proposals require:

- Exempting certain types of transactions from SCA, including those initiated by a merchant.
- Clarifying that the specific amount and payee must be linked to the transaction.
- Requiring banks to apply SCA only once at the outset, when an open banking provider first seeks account information.
- Requiring PIs to ensure that SCA can be performed in circumstances where a user does not have access to a device such as a smartphone.

By comparison, the UK consultation recognised the prescriptiveness of SCA. In particular, there are industry concerns regarding market practice in implementing the standard and the impact on access to payment services to those in certain groups (*e.g.*, to those without a mobile phone or reliable network coverage). In response, the UK government is proposing to introduce a degree of flexibility by considering an outcomes-based approach to authenticating payments. Precise details as to what such an approach might entail are under review.

#### Enhanced User Protection

Push payment fraud is increasingly prevalent. PSD2 provides some protection for customers, as it imposes liability on the part of PIs for unauthorised payment transactions. The UK consultation recognised a lacuna: There is no equivalent legislation for victim reimbursement or PI liability in relation to authorized push payments (APP) fraud, where the payment transaction is authorised by the user but has been entered into through the deception by another — typically, where a fraudster impersonates a bank. Voluntary reimbursement is encouraged (for example the Contingent Reimbursement Model sets out standards for PSPs), but there is a lack of a comprehensive and consistent framework to address such types of fraud. Mandatory reimbursement and potential liability of PIs may be consulted on in due course.

The EU proposes liability to attach to the PI for APP fraud, subject to the user promptly notifying the PI and filing a police report, and not having been grossly negligent in falling victim to the fraud.

#### Open Banking and APIs

Accessibility of third parties to customer data in Open Banking is the subject of much discussion, notably around alternative modes of data access such as screen-scraping and around the quality of dedicated APIs mandated under PSD2.

Screen-scraping is a data collection method that gathers information using a payment service user's log-in details, where the third-party provider (TPP) acts as if it were the user. This is prohibited under PSD2. Instead, PSD2 required banks and other payment account providers to grant TPPs access to payment account data, as well as the ability to initiate payments, via dedicated application programming interfaces (APIs) developed by banks for this purpose.

The UK has seen more progress in respect of the use of such APIs and has therefore provided a more conducive environment for account information service (AIS) and payment initiation service (PIS) providers to develop. This was assisted by the work of the OBIE, which was tasked with implementing certain competition remedies and oversaw the completion of open and common banking

standards (including for APIs) being made available with respect to the nine largest current account providers, impacting 6 million users of services powered by Open Banking technology.

Further developments are expected in the UK, specifically in relation to the requirement for the use of dedicated APIs and prohibiting the use of modified customer APIs, which have been used as fallback solutions should the dedicated APIs fail. This prohibition will not apply to small PIs and small EMIs, but otherwise, an alternative fallback solution will be required within six months of product launch unless an exemption is applied for.

Issues remain, however, in the availability and quality of such APIs. JROC sought to address these issues with the publication of its joint paper in June 2023, which set out high-level principles for banks and registered third parties to follow when agreeing on an API. These include requirements that fees and charges for premium APIs should:

- Broadly reflect relevant long-run costs of providing premium APIs to TPPs.
- Incentivise investment and innovation in premium APIs.
- Incentivise the adoption of Open Banking by both consumers and business.
- Treat TPP service providers fairly.
- Be transparent.

The JROC has already published a final report on recommendations for the next phase of Open Banking in the UK. The report, published in April 2023, sets out the UK's timeline for designing a data collection framework for APIs, which will be submitted to the FCA and Payment Systems Regulator for approval in Q2 2023.

The EU is following suit with its intention to impose more detailed specifications for minimum requirements for Open Banking data interfaces. The EU also will require account providers to put in place more substantial and dedicated APIs (replacing the "dedicated" and "fallback" solutions model currently in place), and encourage a "permissions dashboard" to allow users to manage their granted Open Banking access permissions.

### Widening Access to Payment Systems for Nonbank PSPs

In the UK, both banks and nonbank PSPs (such as electronic money institutions) have access to payment systems (such as CHAPS, BACS and Faster Payments in the UK), either as direct or indirect participants. Currently, the UK PSRs explicitly prohibit direct participants in these payment systems from discriminating against admitting PIs as indirect participants, such that payment fintech companies seeking access to payments systems should be afforded equal opportunity to do so, regardless of their size and business structure, as long as they meet certain eligibility criteria as set out in the UK PSRs.

In this regard, the EU's proposals go further than the UK, as they contemplate the possibility of direct participation of payment and e-money institutions to all payment systems themselves. Such direct participation is accompanied by additional clarifications on admissions and risk assessment procedures.

### Next Steps

In the EU, both the European Council and the European Parliament will review the EC's proposals in order to agree on final texts, which will become legislation once adopted. A prescribed time frame for member states' implementation of PSD3, as well as the transition period for application of the EU PSR, is yet to be announced.

In the UK, the government continues to monitor the need for policy changes, particularly in relation to enhanced fraud prevention, and safeguarding and providing fair protection of customers when terminating payment services. More broadly, the UK payments services regulatory landscape may be the subject of a significant shift, as the government will expand the Payment Systems Regulator's powers under the new Financial Services and Markets Act 2023. It will also review the UK PSRs following consultation throughout 2023.