CLIFFORD

CHANCE

KEEPING PACE WITH EU PAYMENTS: THE PSD3 AND OPEN FINANCE PROPOSALS

KEEPING PACE WITH EU PAYMENTS: THE PSD3 AND OPEN FINANCE PROPOSALS

Since the adoption of the Payment Services Directive 2 (PSD2) in 2015, there has been a rapid evolution of the payments sector, with the emergence of new payment solutions and more sophisticated types of fraud.

To keep pace with these developments, the European Commission has proposed making targeted amendments and updates to the existing regulatory regime for payment services and electronic money (e-money) via a new (i) Payment Services Directive (PSD3) and (ii) Payment Services Regulation (PSR). This is accompanied by a new open finance proposal in the shape of a regulation on a framework for Financial Data Access (FIDA).

These proposals will now need to be considered by the European Parliament and Council. The majority of these amendments are unlikely to take effect before 2025 at the earliest (except potentially the amendments to the Settlement Finality Directive which have a shorter transition period). However, some of the changes proposed may have a significant impact on businesses, including the requirement for existing payment institutions and e-money institutions to reapply for licences.

We consider some of the key changes being proposed in more detail and what impacted firms can do now to prepare.

Key elements of the PSD3 / PSR and open finance package

Structure of the package

The PSD3 and PSR proposals combine the existing payment services and electronic money regimes into a single legal framework. PSD3 itself covers the authorisation and supervision of payment institutions and e-money issuers, whilst conduct of business requirements for payment services (including the rights and obligations of the parties involved) are set out in the new PSR. PSD3 will need to be transposed into the local laws of each EU Member State which may lead to nuances in the approach to implementation, whereas the PSR will become directly applicable in each EU Member State.

A key benefit of moving the requirements on transparency and practical operation of payment services into a regulation is to increase harmonisation across Member States as compared with the position under PSD2, where gold plating and exercise of national options and discretions has made it more complex for firms to comply with different local implementation. Provisions on strong customer authentication (SCA) and access to payment accounts by third party payment service providers (TPPs) have also been moved from regulatory technical standards into the PSR itself.

The PSR aims to further improve and expand the provision of open banking type services (i.e. payment services involving TPPs having access to the payment account data of a payment service user (PSU)). The FIDA builds upon and expands the scope of the existing TPP access provisions in the PSR, extending the open banking principle to other types of accounts and financial products under a broader "open finance" initiative. It introduces financial sector-specific rules as envisaged by Chapter III of the proposed EU Data Act (which we discuss in our separate briefing).

Recitals to the FIDA indicate that in the longer term, the Commission aims to transfer regulation of account information service providers (AISPs) from the PSR to the FIDA, to address the risk of having inconsistent rules governing AISPs under the PSR and financial information service providers under the FIDA. However, this will not be automatic and will depend on whether a financial data sharing scheme has developed under the FIDA. The Commission is required to review this issue by 4 years after entry into force of the FIDA.

Key objectives of the payments and open finance proposals

The PSD3, PSR and FIDA proposals seek to address four key issues identified from the Commission's review of PSD2.

- Tackling fraud risk and improving customer choice and confidence in payments

  The Commission identifies that PSUs continue to be exposed to fraud risk and lack confidence in payments. Various elements of the proposal therefore aim to strengthen user protection and confidence in payments, including improvements in the application of strong customer authentication (SCA).

- Improving the functioning of the open banking and open finance sector

  The PSR seeks to improve the competitiveness and address remaining obstacles to provision of open banking services, including introducing a requirement for payment account providers to provide a dedicated data access interface and permissions dashboard to allow PSUs to manage data access permissions granted to TPPs. The FIDA introduces a similar regime for open finance more broadly.

- Increasing harmonisation of implementation and enforcement of payments and e-money regulation

  The Commission notes in the proposal that the single market for payments remains fragmented, leading to "forum shopping" by payments firms. The proposals therefore aim to increase harmonisation by moving conduct of business requirements into the new PSR. They also introduce stronger provisions on penalties and enforcement of the rules. The rules applicable to e-money institutions (except for the rules on authorisation and supervision) will also be merged into the PSR.

- Improving access to payment systems and bank accounts for non-bank PSPs

  The Commission identifies that there remains an unlevel playing field between banks and non-bank payment service providers (PSPs) ensuing from the lack of direct access by the latter to certain key payment systems and issues relating to data access interfaces for TPPs. Accordingly, the proposals strengthen existing rights on access to payment systems and accounts.

Reapplication process for existing payment institutions and e-money institutions

The PSD3 and PSR do not materially change the current list of regulated payment services. However existing payment institutions and e-money institutions are required to reapply for a licence under the new regime within 24 months of PSD3 coming into force in order to rely on the grandfathering provisions, which allow firms' existing licenses to be valid for 30 months after PSD3 enters into force.

If existing payment institutions and e-money institutions can demonstrate compliance with the new requirements (including requirements in relation to initial capital and own funds and a new requirement to have a winding-up plan in the event of a failure, which includes continuity of any critical activities by outsourced service providers, agents or distributors), then they will be granted automatic authorisation under the new PSD3 regime.

Scope and exclusions

The Commission's consultations on the PSD2 review asked wide-ranging questions about the scope of payment services subject to regulation. However, the PSD3 and PSR proposals do not make major changes to the scope of the rules. Instead, the PSR makes some targeted updates to the exclusions from scope, including:

- A new exclusion for cashback provided without an accompanying purchase. Whilst ATM operators are not subject to authorisation requirements, they are subject to a lighter registration regime and new requirements on fee transparency.
- Clarification of the "commercial agent" exclusion (often relied upon by e-commerce platforms) by harmonising the definition of commercial agent, making clear that the exclusion applies irrespective of whether or not the commercial agent is in possession of the client's funds where the agreement under which the commercial agent is appointed gives the payer or payee "*a real margin to negotiate with the commercial agent or conclude the sale or purchase of goods and services*". The European Banking Authority (EBA) will provide guidelines in respect of the commercial agent exclusion.
- Clarification on the limited network exclusion.
- The removal of two exclusions contained in PSD2 in respect of the professional physical transport of banknotes and coins, and cash-to-cash currency exchange operations where the funds are not held on a payment account. There is no commentary around these changes and therefore the implications for providers of such services that currently rely on these exclusions, and whether they will become subject to licensing if these proposals are adopted, are unclear.

The PSR also introduces new obligations on technical service providers even if they are not themselves providing regulated payment services, as discussed below.

Access to payment systems and competition considerations

The PSR enhances and extends existing PSD2 rules on proportionate, objective, transparent and non-discriminatory (POND) access to payment systems and access to bank accounts. In particular:

- Payment system operators are required to have POND rules on access to payment systems designated under the Settlement Finality Directive (SFD). This is accompanied by a proposal to amend the SFD to allow payment institutions to participate directly in payment systems designated under the SFD. This is intended to level the playing field between banks and non-banks PSPs by opening up access to non-bank PSPs to some key payment systems, which will allow payment firms to provide a full range of payment services to their clients.
- PSD2 rules on banks providing access to payments accounts are being reinforced to address concerns that excessive "de-risking" by banks is creating significant competitive challenges for payment institutions and e-money issuers. The grounds on which banks may refuse to provide access to payment accounts are being tightened, so that a refusal or withdrawal of access may only be based on "serious grounds" such as reasonable suspicion of illegal activity or risk to the bank. These protections will also be extended to cover firms applying for a licence as payment institution, as well as the agents and distributors of payment institutions.

Authorisation of payments and strong customer authentication

Various provisions from the SCA regulatory technical standard have been moved into the PSR. There are also updates to the substantive requirements, including:

- A new confirmation of payee requirement

  This will apply to all (i) credit transfers in currencies of the EU which are not instant credit transfers and (ii) instant credit transfers in currencies which are not in euro. A similar requirement will apply to instant credit transfers denominated in euro which will fall within the scope of the Commission's proposal on Instant Payments amending the SEPA Regulation.

- Enhanced transaction monitoring requirements

  PSPs will need to have transaction monitoring mechanisms in place in connection with the application of SCA and to improve the prevention and detection of fraudulent transactions. Transaction monitoring should be improved on a continuing basis, making full use of new technologies such as artificial intelligence. The EBA will, through regulatory technical standards, provide further technical requirements for transaction monitoring mechanisms.

- Arrangements for voluntary sharing of payment fraud data

  The PSR expressly allows PSPs to enter into data sharing agreements and share payment fraud data to assist with transaction monitoring and fraud detection, on a voluntary basis, subject to compliance with applicable data protection requirements such as completing a data protection impact assessment and prior consultation with the relevant data protection authority. Shared payment fraud data may only be used to enhance transaction monitoring, and the sharing of personal data for this purpose must not lead to the termination of a customer relationship with the PSP or affect their future on-boarding by another PSP.

- Clarification of security standards for non-digitally initiated payments

New rules clarify the security standards expected for non-digitally initiated payment transactions, such as mail or telephone orders. New definitions are introduced to distinguish these types of payments and delineate between "initiation of a payment transaction" and "*remote* initiation of a payment transaction".

- Improving accessibility of SCA

  New provisions seek to improve accessibility of SCA measures, including for elderly or disabled PSUs and those without a smartphone.

- Application of dynamic linking to contactless payments

  The PSR provides that dynamic linking will need to be applied where there is remote placement of a payment order. Recitals to the PSR clarify that this would include contactless payments using near-field communication (NFC) such as via a smartphone wallet or similar technology (unless an exemption from SCA applies), noting that NFC should be considered as a functionality of a payment instrument and not a payment instrument as such.

Role of technical service providers

The PSR retains the existing exclusion from the scope of regulated payment service providers for technical service providers (TSPs). However, it introduces new requirements governing the role of TSPs and their relationship with PSPs.

TSPs and operators of payment schemes are subject to liability for financial damage caused to the payee, or the PSP of the payee or payer, for failing to support the application of SCA. There is also a new requirement for PSPs and TSPs to enter into an outsourcing agreement in cases where the TSP provides and verifies elements of SCA.

In addition, the PSR introduces new rules in relation to prohibiting fees for terminating contracts where payment services are offered jointly with technical services. There is an exception where the contract has been in place for less than 6 months, in which case, charges must be appropriate and in line with costs.

Liability

The PSR builds on the existing provisions contained in PSD2 in relation to a PSP's liability for an authorised payment transaction by clarifying that only reasonable grounds for suspecting fraud *by the payer* can lead to a refusal to refund by the PSP.

To support the new confirmation of payee requirement (outlined above), the payer's PSP will be liable if it fails to notify the payer of a discrepancy between the payee's unique identifier and name given by the payee.

Further, PSPs will (in some cases) be required to compensate consumers where they are tricked into making a payment by someone pretending to be an employee of the PSP.

Other changes under PSD3 and PSR proposals

The PSD3 and PSR proposals make various other targeted updates and amendments, including:

- minor changes to information requirements for payment contracts;
- the extension of alternative dispute resolution (ADR) requirements to single payment contracts;
- a new prohibition on PSPs unilaterally increasing spending limits for customers;
- introduction of product intervention powers for the European Banking Authority (EBA);
- extension of the surcharge ban to all credit transfers and direct debits (and not just those covered under the Regulation on technical and business requirements for credit transfers and direct debits in euro, as was the case under PSD2); and
- a change to the definition of an AISP confirming that a "licence as a service" business model is allowed, whereby information is aggregated by an AISP but transmitted to a third party that will use the aggregated data to provide a service to the AISP's customer.

Open finance and data-driven financial services

The FIDA proposal aims to enable customers and firms to better control access to customers' financial data and promote digital transformation for financial services. It sets out a new regulatory regime for the sharing of customer data on a wide range of financial services and products, including:

- mortgages, loans and accounts (other than payment accounts in scope of the PSR regime);
- savings products, financial instrument investments, cryptoassets, real-estate and related investments;
- occupational and personal pension products;
- non-life insurance products (excluding sickness and health insurance); and
- data which forms part of a creditworthiness assessment.

The regime will apply to financial information service providers (FISPs) authorised under FIDA and regulated firms (or "financial institutions") providing in-scope financial services and products, where they act as "data holders" or "data users". Broadly speaking, data holders are financial institutions that collect, store or process relevant customer data and data users are financial institutions and FISPs that access and use that data in accordance with permissions granted by the customer for them to do so.

Data access requirements

Under the proposed new regime, where a customer submits an electronic request to a data holder, data holders would be required to make relevant customer data available, either:

- to customers without undue delay, free of charge, continuously and in real time; or
- to a data user for the purposes for which the customer has granted permission to the data user, without undue delay, continuously and in real time.

Data provided to data users must be in a format based on generally recognised standards. Data holders must communicate securely with the data user and request data users to demonstrate they have the customer's permission to access the relevant customer data. Data holders must also provide customers with a permission dashboard to monitor and manage the permissions they have granted to data users.

Data users would also be required to put in place security and related measures and ensure they do not process customer data for purposes other than for performing the service expressly requested by the customer. Both data holders and data users must respect confidentiality of trade secrets and intellectual property rights when customer data is accessed.

Financial data sharing schemes

The FIDA proposal envisages the establishment of financial data sharing schemes setting out common standards for the data and technical interfaces to allow customers to request data sharing under the regime. Data holders and data users are required to become members of a financial data sharing scheme within 18 months of the FIDA regulation entering into force.

Financial data sharing schemes are also required to establish a model to determine the maximum amount that data holders are able to charge data users for making data available through a technical interface, set out the contractual liability of scheme members and provide for an effective dispute resolution system. If no financial data sharing scheme is developed for a category of customer data covered by the FIDA, the Commission would be empowered to adopt a delegated act to set common standards for data sharing and technical interfaces, a model to determine maximum charges for data sharing and the liability of entities making customer data available.

The ability of data holders to charge data users for access to data remains in contrast to the TPP access provisions proposed under the PSR, which would continue to provide for TPPs to access payment accounts with no charge and without establishment of a contractual relationship between the payment account provider and TPP. However, the PSR proposal does also envisage that TPPs may establish contractual relationships with payment account providers, including under a scheme for paid access to additional open banking services other than those mandated under PSR, for example for variable recurring payments under a so-called "premium" API.

Authorisation of FISPs

The FIDA sets out authorisation requirements for FISPs, including information required to be provided as part of the authorisation application, similar to what is proposed for AISPs under PSD3. FISPs would either need to be established in the EU or appoint a legal representative in the EU that will be held liable for any non-compliance of the FISP with obligations under the FIDA. A passporting regime has been proposed to allow FISPs to provide services across the EU.

FISPs would also be subject to various ongoing organisational requirements under the FIDA proposal, again broadly similar to those applicable to AISPs under PSD3. They will also be subject to operational resilience, risk management and incident reporting requirements under the EU digital operational resilience act (DORA).

Next steps

Now that these proposals have been published, they will be considered by the European Parliament and Council. However, it is unclear whether the European Parliament will be able to agree its position before the upcoming elections in June 2024 which may delay finalisation of these proposals and their publication in the Official Journal.

The PSD3 proposal requires Member States to transpose and apply implementing legislation from 18 months after entry into force (with the exception of amendments to the SFD which are to apply from 6 months after entry into force). The PSR proposal states that it will apply from 18 months after entry into force. Rules on financial data sharing schemes and authorisation of financial information service providers under FIDA are also due to apply from 18 months after entry into force, with other provisions applying from 24 months after entry into force.

What should payments firms be doing to prepare?

Existing payment institutions and e-money issuers will need to prepare to re-apply for authorisation under PSD3 once it has been published in the Official Journal and enters into force. All PSPs will need to carry out a gap analysis against PSD2 to assess where they will need to make changes or upgrades to comply with PSD3 and PSR requirements. Firms may also wish to monitor the legislative process for these new rules and make appropriate representations through industry associations or otherwise on key issues.

In addition to analysing the requirements of the PSD3 (as transposed into national law) and PSR, PSPs will also need to look out for the accompanying technical standards and guidelines that will be developed. These include technical standards on:

- authorisation under PSD3, including the information to be provided as part of the authorisation application, a common assessment methodology for granting authorisation, and on requirements for professional indemnity insurance or a comparable guarantee;
- calculation of own funds requirements for payment institutions executing a small number of high value payment transactions;
- safeguarding requirements, including risk management frameworks;
- the limited network and related exclusions from scope;
- the format and information to be contained in a notification by banks that refuse to open or close a payment account for a payment institution, its distributor or agent, or an applicant for a payment institution licence;
- criteria for being exempt from the obligation to have in place a dedicated interface for TPP access;
- fraud reporting requirements;
- standard forms and templates for the submission of the payment fraud data by competent authorities; and
- authentication, communication and transaction monitoring mechanisms.

The EBA is also expected to issue guidelines on the commercial agent exclusion, fraud risks and payments trends and complaints procedures.

AUTHORS

Laura Douglas
Senior Associate
London
T: +44 207006 1113
E: laura.douglas@cliffordchance.com

Wouter van den Bosch
Senior Associate
Amsterdam
T: +31 20 711 9407
E: wouter.vandenbosch@cliffordchance.com

Meera Ragha
Senior Associate
London
T: +44 207006 5421
E: meera.ragha@cliffordchance.com

Marian Scheele
Senior Counsel
Amsterdam
T: +31 20 711 9524
E: marian.scheele@cliffordchance.com

CONTACTS

Kikun Alo
Senior Associate
London
T: +44 207006 4067
E: kikun.alo@cliffordchance.com

María Luisa Alonso
Counsel
Madrid
T: +34 91 590 7541
E: marialuisa.alonso@cliffordchance.com

Diego Ballon Ossio
Partner
London
T: +44 207006 3425
E: diego.ballonossio@cliffordchance.com

Marc Benzler
Partner
Frankfurt
T: +49 69 7199 3304
E: marc.benzler@cliffordchance.com

Anna Biała
Counsel
Warsaw
T: +48 22429 9692
E: anna.biala@cliffordchance.com

Lucio Bonavitacola
Partner
Milan
T: +39 02 8063 4238
E: lucio.bonavitacola@cliffordchance.com

Riccardo Coassin
Counsel
Milan
T: +39 02 8063 4263
E: riccardo.coassin@cliffordchance.com

Simon Crown
Partner
London
T: +44 207006 2944
E: simon.crown@cliffordchance.com

Lounia Czupper
Partner
Brussels
T: +32 2 533 5987
E: lounia.czupper@cliffordchance.com

Pierre d'Ormesson
Avocat
Paris
T: +33 1 4405 5135
E: pierre.dormesson@cliffordchance.com

Boika Deleva
Senior Associate
Luxembourg
T: +352 48 50 50 260
E: boika.deleva@cliffordchance.com

Jaime Denis
Abogado
Madrid
T: +34 91 590 7521
E: jaime.denis@cliffordchance.com

Miloš Felgr
Partner
Prague
T: +420 222 55 5209
E: milos.felgr@cliffordchance.com

Steve Jacoby
Regional Managing Partner CE
Luxembourg
T: +352 48 50 50 219
E: steve.jacoby@cliffordchance.com

Hélène Kouyaté
Counsel
Paris
T: +33 1 4405 5226
E: helene.kouyate@cliffordchance.com

Frédérick Lacroix
Partner
Paris
T: +33 1 4405 5241
E: frederick.lacroix@cliffordchance.com

Caroline Meinertz
Partner
London
T: +44 207006 4253
E: caroline.meinertz@cliffordchance.com

Monica Sah
Partner
London
T: +44 207006 1103
E: monica.sah@cliffordchance.com

Helene Uffelmann
Senior Associate
Frankfurt
T: +49 69 7199 3186
E: helene.uffelmann@cliffordchance.com

Richard Whiteaway
Senior Associate
London
T: +44 207006 4171
E: richard.whiteaway@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

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

2307-006943