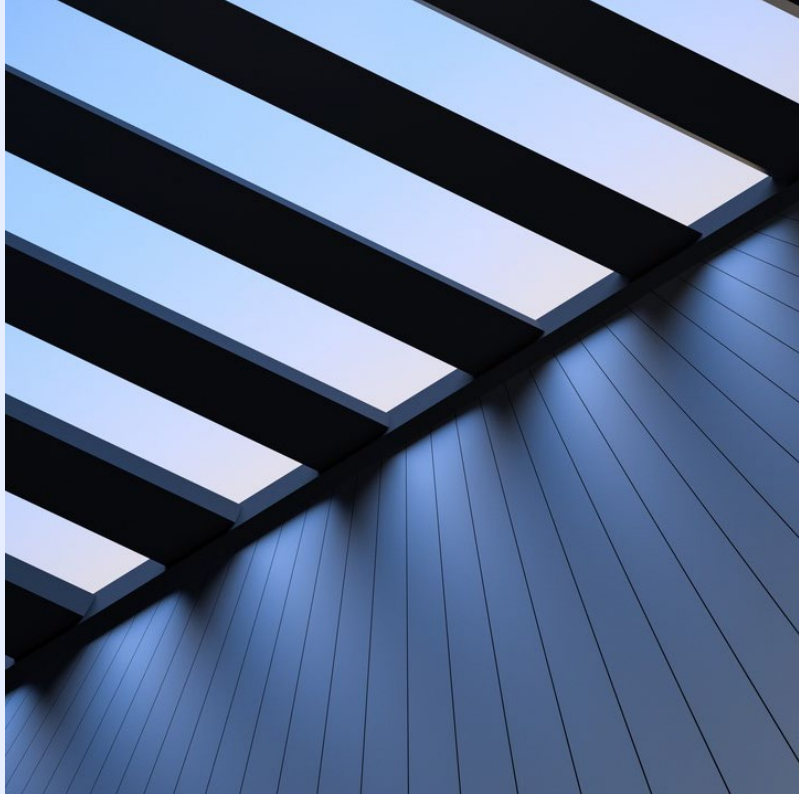
Clifford Chance

BRIEFING

Impact of PSD3 – are you ready?

April 28, 2026

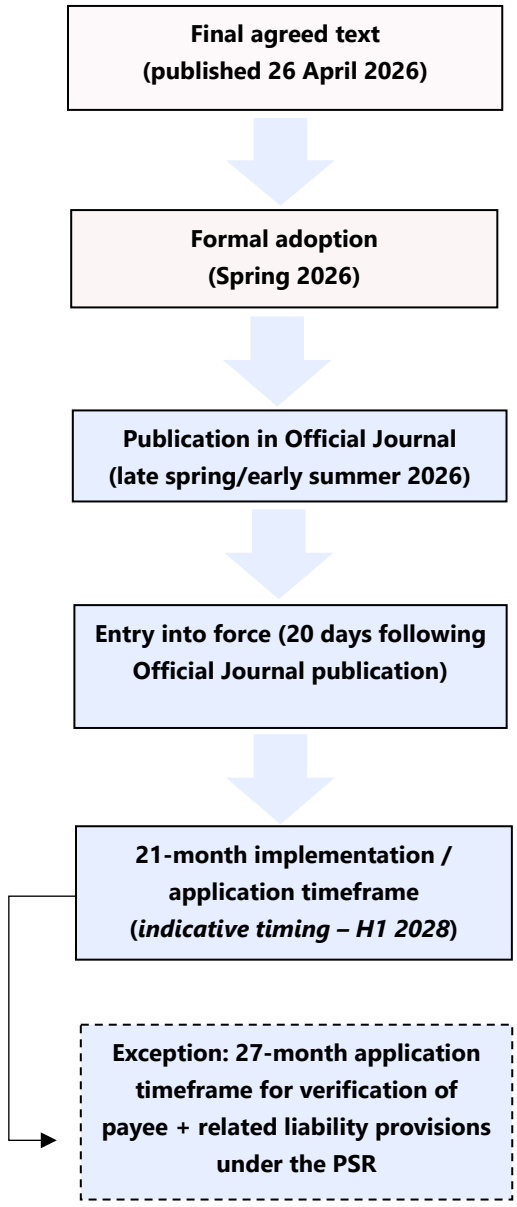


On 23 April 2026, the EU council published the final compromise texts for a new payment services package comprising: (i) Payment Services Directive (PSD3) and (ii) Payment Services Regulation (PSR).

We outline below ten key impacts for firms.

10 KEY IMPACTS FOR FIRMS:

1. Reapplication process for existing payment institutions and EMIs
2. Additional safeguarding requirements
3. Enhanced SCA rules
4. Scope and exclusions
5. Role of TSPs
6. Enhanced transaction monitoring requirements and fraud information sharing
7. Tightening rules in relation to access to payment accounts and payment systems
8. Free verification of payee service extended to all credit transfers
9. Card scheme fees
10. E-money tokens – PSD2/MiCA interplay



THE COUNTDOWN TO IMPLEMENTATION

The final agreed texts of the PSD3 and PSR proposals were published on 23 April 2026 (following lengthy trilogue negotiations). The package is expected to be formally adopted and published in the Official Journal by late spring/early summer 2026.

Following entry into force, Member States must transpose PSD3 into national implementing legislation 21 months after its entry into force. The PSR will also mostly apply 21 months after entry into force (although certain provisions have a longer lead time). On this timing, the package is expected to apply during H1 2028.

WHAT CAN FIRMS DO TO PREPARE?

Firms will need to carry out a gap analysis against PSD2 to assess where they will need to make changes to comply with PSD3 and PSR requirements, including:

I. reviewing and updating client documentation and policies and procedures;

II. reviewing the firm's business model to confirm whether any services which are currently unregulated would trigger licensing requirements under the new regime;

III. implementing technological upgrades, particularly around allowing third-party providers (TPPs) access and the enhanced strong customer authentication (SCA) rules; and

IV. preparing for other impacts (including the re-authorisation process for existing payment institutions and e-money institutions (EMIs)).

Firms should also monitor the legislative process for any accompanying technical standards and guidelines and make appropriate representations through industry associations or otherwise on key issues.

10 KEY IMPACTS FOR FIRMS:

1. Reapplication process for existing payment institutions and EMIs

PSD3 and the PSR do not materially change the current list of regulated payment services other than to add electronic money services to the list. However, existing payment institutions and EMIs are required to apply for a licence under the new regime within 21 months of PSD3 coming into force, in order to take advantage of grandfathering provisions that would permit them to continue providing the services for which they were previously authorised for a further 6 months (i.e. 27 months after PSD3's entry into force, or 30 months only in exceptional circumstances). To continue operating beyond that date, they must have submitted to the competent authority the necessary information that will allow the competent authority to assess whether they are PSD3 compliant (and deemed PSD3-authorised, as noted below) or whether their authorisation should be suspended. This reapplication requirement applies notwithstanding that PSD3 and the PSR do not materially change the current list of regulated payment services.

If existing payment institutions and EMIs can demonstrate that they already comply 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), PSD3 provides that Member States can grant them automatic authorisation.

2. Additional safeguarding requirements

PSD3 aligns the safeguarding regime for e-money institutions with that for payment institutions, and it introduces new requirements. The final text additionally clarifies that funds received in exchange for electronic money tokens should be safeguarded in accordance with Article 54 of the Markets in Cryptoassets Regulation (MiCA).

EMIs will be particularly impacted. EMIs are currently permitted to safeguard customer funds within five business days following receipt of funds received in exchange for the e-money issued (T+5) under the Second Electronic Money Directive. PSD3 requires EMIs to safeguard by no later than the end of the business day following the day when the funds have been received (i.e., T+1).

There is a new requirement to mitigate concentration risk of safeguarded funds. Firms must endeavour not to safeguard all consumer funds with one credit institution. The European Banking Authority (EBA) is required to issue regulatory technical standards (RTS) on risk management of safeguarded funds.

This was intended to be supported by allowing safeguarded accounts to be opened at central banks. The Settlement Finality Directive (SFD) permits non-bank payment service providers (PSPs) to deposit their clients' funds for safeguarding in a separate account in a bank or central bank, at the central bank's discretion. However, the ECB has prohibited Eurosystem central banks from offering or providing safeguarding accounts to non-bank PSPs or crypto-asset services providers (CASPs). We expect that other central banks may

follow suit, and so non-bank PSPs may face significant hurdles if they wish to open safeguarded accounts with central banks. If PSD3 requires non-bank PSPs to hold multiple safeguarded bank accounts, this could present practical challenges including increased costs (such as maintenance fees which are typically charged by safeguarding account providers).

Lastly, there is a requirement on payment institutions to notify regulators in advance of any material changes in relation to the safeguarding measures in relation to funds received for payment services or e-money issuance.

3. Enhanced SCA rules

The PSR introduces new requirements in relation to SCA, which will require significant technological build. We have summarised the key impacts below:

- **Banks must have a dedicated interface for TPP access**

  Currently, PSD2 allows account servicing payment service providers (ASPSPs) to communicate with TPPs through either a dedicated access interface or a modified version of the customer interface. The latter has been popular with ASPSPs that have predominantly corporate clients.

  The PSR requires all ASPSPs to rely on a dedicated interface for TPP access that provides availability and performance of at least the level of their customer interface. This is not subject to a corporate opt out. ASPSPs which do not currently have a dedicated interface will need to build one within three months of the ASPSP obtaining its licence, unless the ASPSP's competent authority provides an exemption (following a request from the ASPSP). The EBA will set out in an RTS the criteria which a competent authority may use to grant an ASPSP an exemption from having a dedicated access interface. As the legislation is not yet formally adopted, the EBA has not published a draft RTS yet, but it is expected to publish a Roadmap on the implementation of the EU Payment package, covering work under all its mandates under PSD3 and PSR.

  Even if a bank has an existing dedicated interface, it will need to conduct a gap analysis between the existing PSD2 rules and the forthcoming PSR requirements, as the existing dedicated access interface will need to be upgraded to meet the amended or new requirements.

- **Banks which currently rely on the exemption from the requirement to maintain a fallback interface should prepare to make an alternative interface available to TPPs if the dedicated interface is unavailable**

  The PSR removes the requirement for ASPSPs to maintain a contingency permanent "fallback" interface or apply for an exemption in the event that the dedicated interface is unavailable (except in authorised, exceptional circumstances), although it requires ASPSPs to "*always permit access to interfaces which allow business continuity*" for TPPs. Instead, TPPs must be offered an effective, alternative solution. These requirements are not subject to the corporate opt out.

  Banks which currently rely on the exemption from the requirement to maintain a contingency, fallback interface must now prepare to make an alternative interface available to TPPs.

- **Banks will need to provide a "dashboard"**

  ASPSPs will be required to provide a "dashboard" which is integrated within the customer interface, to allow customers to monitor and manage the consents they have given to TPPs.

  It must meet certain information and functionality requirements, such as stating which TPPs have been given data access consent, for which accounts, the purpose of the consent, the validity period of the consent, the categories of data being shared, and the dates on which the data was accessed. Customers will be allowed to withdraw consent for data access from TPPs through the dashboard. ASPSPs must keep a record for two years of data access consents which have been withdrawn or expired.

  There is a positive obligation for ASPSPs and TPPs to co-operate to provide certain information in real time.

  This is not subject to the corporate opt out.

- **Improving accessibility of SCA**

  New provisions seek to improve accessibility of SCA measures, including for elderly or disabled payment service users (PSUs) and those without a smartphone. Such accessibility support, including help or assistance on request will need to be provided free of charge.

- **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.

- **PSPs will be required to accept European Digital Identity Wallets for SCA**

  Member States are required to offer at least one EU Digital Identity (EUDI) Wallet to all their citizens by the end of 2026 under the Regulation on Electronic Identification and Trust Services for Electronic Transactions (eIDAS 2.0). PSPs will be required to accept the use of EUDI wallets for SCA.

  The EBA is required to review and update RTS taking into account innovation and technological developments, including the EUDI wallets implemented under eIDAS 2.0.

4. Scope and exclusions

Firms that currently rely on an exclusion under PSD2 should assess whether this will continue to apply under the new regime. The PSR makes targeted updates to the exclusions from scope, including:

- A new exclusion for cashback provided in retail stores without an accompanying purchase, subject to a cap in order to "*prevent unfair*

competition between ATM deployers not servicing payment accounts and retailers offering cash withdrawals without a purchase, and to ensure that shops do not rapidly run out of cash".

- Whilst ATM operators (re-defined as 'ATM deployers') 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 commercial agent "a real scope to negotiate with the payer or payee or conclude the sale or purchase of goods and services". The EBA will provide guidelines in respect of the commercial agent exclusion.
- Clarification on the limited network exclusion and the exclusion relating to certain payment transactions by means of telecom or information technology devices.
- An exclusion for payment transactions made exclusively in electronic money tokens directly from the payer to the payee, without any intermediary involved (a recital clarifies this should include transfers of electronic money tokens between two self-hosted addresses where there is no intermediary involved and should not include payment transactions between a custodial wallet and a self-hosted wallet).
- An exclusion for payments transactions carried out by a CASP intermediating between a buyer and a seller where electronic money tokens are exchanged for electronic money tokens or crypto-assets, as well as the exchange of electronic money tokens for funds, including electronic money tokens, or crypto-assets carried out by a crypto-asset service provider acting in its own name as buyer or seller of those electronic money tokens.
- An exclusion for payment transactions carried out between CASPs or their branches for their own account.

Some provisions of the PSRs now apply to technical service providers (TSPs), operators of payment systems and payment schemes, and providers of electronic communications services.

5. Role of TSPs

The PSR also introduces new obligations on TSPs, even if they are not themselves providing regulated payment services (as the existing exclusion from the scope of regulated payment service providers for TSPs is being retained). The PSR introduces new requirements governing the role of TSPs and their relationship with PSPs.

TSPs and operators of payment schemes are liable for financial damage caused to the payee, or the PSP of the payee or payer, for failing to support the application of SCA. Such liability shall be for "*direct*" financial damage which is "*proportionate to their failure*" and "*not exceeding the amount of the transaction in question*".

The PSR includes 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 three months, in which case, charges must be appropriate and in line with costs.

The PSR imposes new requirements on electronic communications service providers (e.g., mobile network operators) and very large online platforms or engines in relation to fighting impersonation fraud. This includes requiring firms to establish dedicated communication channels with PSPs or participate in a system for effective communication or in an information sharing mechanism with the aim of preventing and detecting fraudulent payment transactions.

6. Enhanced transaction monitoring requirements and fraud information sharing

PSPs will need to have enhanced 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 the RTS, provide further technical requirements for transaction monitoring mechanisms.

Whilst PSD2 contains transaction monitoring and fraud reporting requirements, the PSR significantly builds on these, including by imposing liability on PSPs in certain circumstances for financial damage suffered as a result of transaction monitoring failures. Once published, the RTS on statistical data to support these requirements is also likely to enlarge the scope of statistical data that needs to be collected. Firms will need to undertake a gap analysis to understand how the transaction monitoring and fraud reporting requirements will change. This will inform what additional data a firm needs to collect, and how the existing policies and procedures will need to be enhanced.

To assist with transaction monitoring and fraud detection, PSPs are required to enter into information-sharing arrangements and share payment fraud information.

Sharing data is 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 future on-boarding by another PSP.

7. Tightening rules in relation to access to payment accounts and payment systems

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:

- **Banks are subject to stricter rules governing when they may refuse to provide access to payment accounts**, so that a refusal or withdrawal of access may only be based on "*serious grounds*". The grounds are strictly limited and include that a bank should be able to refuse to open or be able to close a payment account for a payment institution, its agents, or an applicant for an authorisation as a payment institution, where opening or maintaining the account would be a breach of the new Anti-Money Laundering Regulation.
- The existing 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 PSR expands the types of firms that can benefit from these rules to include firms applying for a licence as a payment institution, as well as the agents of payment institutions.

  Banks will need to review and revise their policies and procedures to ensure they only refuse to open or close payment accounts for one of the limited reasons permitted under the new regime, where their clients are existing or applicant-authorised payment institutions, or their agents or distributors. This will limit when banks can refuse to open or close a payment account for such entities.
- **Payment system operators are required to have POND rules on access to payment systems designated under the SFD**. Such operators should review their access requirements to ensure compliance with these new rules.

  This aligns with changes made to the SFD to allow payment institutions and EMIs to be added to the list of eligible direct participants in settlement systems designated under the SFD. This aims to level the playing field between bank and non-bank PSPs by opening up access to non-bank PSPs to key payment systems. Non-bank PSPs may wish to consider applying directly for access to such systems.

  These requirements also apply to operators of payment schemes. However, the requirements do not apply to operators of payment systems and payment schemes composed exclusively of payment service providers belonging to the same group**.**

8. Free verification of payee service extended to all credit transfers

Currently, the SEPA Regulation (as amended by the Instant Payments Regulation) requires that PSPs provide a free verification of payee service for certain types of credit transfers. Article 50 of the PSR extends these requirements to all credit transfers, including those that fall outside the scope of the SEPA Regulation. This means that credit transfers that currently fall outside the scope of the SEPA Regulation, such as credit transfers (including

instant credit transfers) denominated in a currency other than the euro, will be subject to the verification of payee requirements.

PSPs will need to check payment account IBAN numbers (or other unique identifiers) against a corresponding bank account name before any transfer can take place, although the payer will retain the right to proceed with the payment in the event of a mismatch.

The SEPA Regulation currently allows that customers that are not consumers can opt out from receiving the verification of payee service. The PSR amends the SEPA Regulation to require that PSPs provide PSUs that are not consumers with:

- the means to opt out from receiving the service ensuring verification when submitting payment orders via payment initiation channels that are based on automated dedicated processes or protocols and that are only made available to PSUs that are not consumers.
- the right to opt in to the verification service at any time; and
- the possibility of agreeing certain parameters of the verification service within their framework contract.

Related to this, where a PSP fails to comply with Article 50 (in relation to the verification of payee requirements) and this results in a defectively executed payment transaction, the payer's PSP is required to refund the payer the amount transferred and, where applicable, restore the debited payment account to the state in which it would have been had the transaction not taken place.

Further, the payer's PSP or payment initiation service provider (PISP) is liable to compensate the payer's PSP for the financial damage caused to the payer's PSP, if the failure to comply with its obligations in Article 50 occurred because the payee's PSP or PISP failed to comply with its obligations under Article 50.

9. Card scheme fees

The PSR will require operators of payment card schemes and processing entities to ensure that the fees imposed on acquirers are categorised and disclosed in a clear and consistent manner to enable acquirers to compare billing categories between schemes and processing entities.

Such fee information should be as specific as possible and, where possible, distinguish the fees applied according to the card category, the sales channel, the transaction volume and value of the merchant and the geographical location. Any new fees or proposed fee changes should be communicated at least 6 months before the changes are to take effect. The information to be disclosed will be further specified in a delegated act.

10. E-money tokens – PSD2/MiCA interplay

E-money tokens are, at the same time, crypto-assets regulated under MiCA, and electronic money/funds within the meaning of PSD2. This interplay means that, without more, CASPs that transact e-money tokens would need to be authorised under both MiCA and PSD for the exact same service.

The EBA addressed this interplay in an Opinion in June 2025, which it followed in February 2026 with further guidance for national competent authorities on how to approach this interplay pending entry into application of PSD3/PSR.

The PSR partially resolves this issue by amending MiCA. In respect of certain crypto-asset services related to e-money tokens, a PSP authorised under PSD3 does not require separate authorisation under MiCA. Specifically, a firm authorised under PSD3 to:

- enable cash to be placed on or withdrawn from a payment account may provide custody and administration of crypto-assets on behalf of clients;
- execute payment transactions may provide: (i) the exchange of crypto-assets for funds and other crypto-assets: (ii) transfer services for crypto-assets on behalf of clients; and (iii) execution of orders for crypto-assets on behalf of clients; and
- payment initiation services may provide reception and transmission of orders for crypto-assets on behalf of clients.

To benefit from this deemed equivalence, the payment institution must provide its competent authority with the information required by Article 60(7) of MiCA at least 40 days before providing the crypto-asset service for the first time.

For completeness, CASPs authorised under MiCA would still require a separate PSD3 authorisation when they are carrying on payment services and an exclusion is not available (see section 4 above on the scope and exclusions).

WHERE ARE WE WITH FIDA – THE 'OPEN FINANCE' RULES?

The initial PSD3 and PSR proposals were accompanied by a new open finance proposal in the shape of a regulation on a framework for Financial Data Access (FIDA), which sought to build upon the TPP access provisions in the PSR, applying the open banking principle to other types of accounts and financial products under a broader "open finance" initiative.

Whilst the European Parliament adopted its negotiating position on FIDA in April 2024, the Council did not adopt its own negotiating position until 4 December 2024. Since that time, the FIDA text has been subject to protracted trilogue negotiations between the European Parliament, the Council and the Commission, as noted further below.

The proposals in FIDA represent a significant change in how financial data is shared. Under the original Commission proposals, FIDA would require financial institutions to share financial data, subject to customer consent, including requirements to share data in real time. There are also requirements to provide customers with a permission dashboard to monitor and manage the permissions it has granted to 'data users'. This is accompanied by mandatory financial data sharing schemes.

FIDA would have a far-reaching impact, as the proposal applies to a wide range of services and products, including impacting firms in the investment, insurance and asset management sector. Whilst the European Commission's original text did not exclude data from wholesale and corporate customers,

the subsequent European Parliament proposal narrowed the scope to natural persons, and micro, small and medium-sized enterprises.

FIDA has been subject to intense industry lobbying and political disagreement. Trilogue negotiations began in April 2025. As at late April 2026, after progress on the FIDA had stalled since Summer 2025, the Cypriot presidency of the Council is making renewed efforts to reach a compromise, and further developments are expected in May. It is possible that the final rules may change significantly from the latest European Council adopted text.

We recommend firms continue to monitor the legislation process for FIDA, and consider making appropriate representations through industry associations.

Author

Meera Ragha
Senior Associate, London

meera.ragha@cliffordchance.com
+44 207006 5421

Contacts

Simon Crown
Partner, London

simon.crown@cliffordchance.com
+44 207006 2944

Diego Ballon Ossio
Partner, London

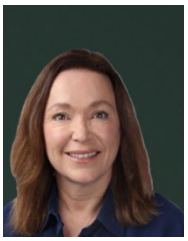
diego.ballonossio@cliffordchance.com
+44 207006 3425

Marc Benzler
Partner, Frankfurt

marc.benzler@cliffordchance.com
+49 69 7199 3304

Jaime Denis
Lawyer, Madrid

Jaime.Denis@CliffordChance.com
+34 91 590 7521



Sara Evans
Knowledge Director, London

sara.evans@cliffordchance.com
+44 207006 2557

Frédérick Lacroix
Partner, Paris

frederick.lacroix@cliffordchance.com
+33 1 4405 5241

Caroline Meinertz
Partner, London

caroline.meinertz@cliffordchance.com
+44 207006 4253

Monica Sah
Partner, London

monica.sah@cliffordchance.com
+44 207006 1103

Marian Scheele
Senior Counsel, Amsterdam

marian.scheele@cliffordchance.com
+31 20 711 9524

Jurgen van der Meer
Partner, Amsterdam

jurgen.vandermeer@cliffordchance.com
+31 20 711 9340

cliffordchance.com

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