CLIFFORD
CHANCE

CRYPTO-ASSET SERVICE PROVIDERS: NAVIGATING YOUR EU REGULATED STATUS

— THOUGHT LEADERSHIP

NOVEMBER 2024

CRYPTO-ASSET SERVICE PROVIDERS: NAVIGATING YOUR EU REGULATED STATUS

The Markets in Crypto-Assets Regulation (MiCA) delivers a new EU-wide regulatory framework for issuing, intermediating and dealing in crypto-assets. Under MiCA, Crypto-asset service providers (CASPs) must be authorised, comply with conduct, disclosure, governance and organisational requirements and have prudential safeguards in place. In this briefing we take a closer look at some of the wider EU regulatory requirements that will attach to some CASPs for the first time, and to existing service providers more broadly, as EU-regulated entities.

CASP obligations under MiCA

We gave an overview of these obligations in our July 2024 briefing EU Crypto Regulation: MiCAR Overview for Issuers and Crypto-Asset Service Providers. MiCA's provisions relating to the offering and admission to trading of stablecoins took effect on 30 June 2024. Other parts of MiCA, including the authorisation requirements for CASPs, apply from 30 December 2024.

MiCA will impact individual CASPs differently.

- First, firms already offering crypto-asset services in the EU will have some familiarity with financial services regulation in the individual EU member state(s) in which they operate. These firms will benefit from the transitional regime that will enable them to continue providing certain services until their application is decided. We expect that, in practice, during the transitional period these CASPs will adjust and improve their systems and controls and other processes to achieve levels required by MiCA.[1]
- Secondly, we can expect to see some new entrants seeking EU authorisation in order to rely on the rights under MiCA to passport their services across the EU.
- Finally, we can also expect some firms that are authorised in the EU under other financial services frameworks to take advantage of MiCA to expand their service offering to include those relating to crypto-assets. These firms will be well versed in EU regulatory requirements and therefore able to leverage or adjust their existing internal processes for MiCA compliance.

Some EU frameworks will be familiar

Pre-MiCA, firms that have been providing crypto-asset services in the EU have been subject to certain obligations as a result of qualifying as 'Virtual Asset Service Providers' (VASPs), under the EU anti-money laundering (AML) and counter-terrorist financing (CTF) frameworks as these regimes were implemented in individual member states.

There is a patchwork of local regulatory regimes across the EU which implement the registration requirement that applies to VASPs, and often 'gold-plate' that requirement with additional obligations relating to, for example, systems and controls, or fitness and propriety. This means that compliance with local registration requirements has placed different obligations on existing firms depending on their location. But the EU's AML/CTF framework is changing (including, as explained further below, extension of the so-called 'travel rule' to crypto-asset transfers), which will affect all CASPs wherever located in the EU.

1 MiCA contains transitional provisions permitting CASPs providing crypto-asset services in accordance with applicable law in individual EU member states prior to 30 December 2024 to continue to do so until 1 July 2026 or until they are granted or refused an authorisation under MiCA (whichever is sooner). The European Securities and Markets Authority (ESMA) has recently provided helpful clarification (in ESMA_QA_2295) that firms operating under the transitional provisions do not need to comply with MiCA's CASP provisions until their application for authorisation is approved.

All CASPs will be 'obliged entities' under the forthcoming Anti-Money Laundering Regulation (AML Regulation), which will repeal and replace the Anti-Money Laundering Directive with effect from 10 July 2027. The AML Regulation forms part of the EU's new AML/CTF framework and will be supplemented by technical standards and guidance to be developed by the new Anti-Money Laundering Authority (AMLA). Depending on their size, CASPs may also be subject to direct supervision by AMLA.

VASPs are also likely, in aligning their operations in particular member states, to have been ensuring compliance with data protection and privacy laws, in particular the General Data Protection Regulation (GDPR), when controlling or processing personal data. As noted below, new data-sharing obligations will apply from 2026/2027.

Similarly, VASPs may have considered how their existing services sit alongside the payment services and electronic money perimeter under the revised Payment Services Directive (PSD2) and the second Electronic Money Directive (2EMD); for example, to what extent their services involve the transfer of funds such that this may constitute a payment service or the issuance of electronic money. With MiCA some of these points will need to be reconsidered, and PSD2 is being replaced, as noted further below.

Entities already authorised under existing EU frameworks (for example, crypto-asset firms authorised under PSD2 or 2EMD, or other financial entities authorised under MiFID2, AIFMD, CSDR) will already be fully familiar with EU regulation and supervision, and be aware of forthcoming developments in the EU's legislative pipeline. To the extent that these firms wish to carry on MiCA activities, they will need to notify their intention to conduct CASP activities to the competent authority of their home member state and comply with MiCA's CASP requirements, rather than seek a separate CASP authorisation. However, in practice, this may require a substantive review of existing arrangements in order to meet the cyber and resilience expectations set for CASPs.

Wider obligations – existing and incoming EU frameworks impacting CASPs

EU legislative frameworks do not operate in isolation and authorised CASPs will need to be aware of other key existing requirements or forthcoming changes to EU frameworks with which they will need to comply as a result of being authorised under MiCA. While these frameworks will be familiar to existing financial institutions intending to perform crypto-asset services, compliance may require significant system builds and additional work for some newly authorised CASPs and those transitioning into a MiCA authorisation.

DORA – Digital operational resilience and cybersecurity

CASPs will be financial entities for the purposes of the EU's Digital Operational Resilience Act (DORA) a directly applicable EU Regulation which applies from 17 January 2025. DORA aims to ensure that all EU financial entities have robust digital operational resilience regimes in place to be able to withstand and recover from ICT-related incidents, including cyber-attacks.

While MiCA provides an 18-month transitional period for existing crypto-asset providers to ensure they are fully compliant with MiCA, many jurisdictions have shortened this period to 12 months. Existing crypto-asset providers will not be treated as CASPs during this time (see footnote 1, above) but, in practice, prospective CASPs will need to ensure they can demonstrate compliance with DORA from its application date. This is because the expectation is that EU competent authorities will assess their ability to comply with DORA obligations as part of the application for CASP authorisation.

DORA defines digital operational resilience as:

> "*The ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities*

needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including through disruptions."

To ensure resilience, financial entities must comply with a range of detailed obligations imposed by DORA. Financial entities are required to implement DORA on a proportionate basis, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.

DORA obligations include:

- Governance and organisation requirements;
- ICT risk management requirements;
- ICT-related incidents management, classification and reporting;
- Digital operational resilience testing;
- Management of ICT third-party risk; and
- A new oversight framework of critical ICT third-party providers.

A key issue for CASPs will be compliance with Article 30 of DORA, which will require identification of ICT third-party services providers and will also potentially require negotiation with such providers to put in place very stringent requirements and termination rights in respect of the services provided by ICT third-party services providers and their subcontractors (including, potentially, the chain of subcontractors). Difficulties in practice start with the identification of ICT third-party services providers and whether technology relied on in order to deliver crypto-asset related services would fall within this definition. For example, to what extent a layer 1 or layer 2 blockchain would qualify as an ICT third-party services provider or whether certain aspects do. This is exacerbated by the fact that some providers may be based outside of the EU and would not normally see themselves in scope of EU legislation such as DORA.

Depending on their activities, CASPs may also fall within scope of the revised Network and Information Security Directive (NIS2), which has applied since 18 October 2024. NIS2 aims to further harmonise the EU cybersecurity framework. However, DORA is considered a *lex specialis* for financial entities, meaning that certain of its provisions, which are tailored for the financial sector, override those of the broader cybersecurity framework in NIS2 in the event there is conflict between the two frameworks. In September 2023, ESMA published guidelines clarifying which provisions in DORA will apply to financial entities within scope of both pieces of legislation rather than those provided for in NIS 2.

Payment services and electronic money

Interplay between PSD2 and MiCA

Where CASPs themselves offer services that qualify as payment services, they must comply with the requirements of PSD2, which include strong customer authentication, transparency requirements and security measures.

While CASPs will not automatically be deemed to be conducting payment services under PSD2, there is an interplay between PSD2 and MiCA, especially in relation to the issuance of e-money tokens, which is currently linked to the concept of electronic money. 'Electronic Money Tokens' (EMTs) are defined in MiCA by reference to the definition of e-money in 2EMD. The effect of this is that, under PSD, EMTs may qualify as "funds" for the purposes of PSD2, such that a transfer of EMTs may be defined as a payment service being provided. CASPs will therefore need to carefully consider their activities in respect of stablecoins and EMTs in order to identify whether any of their activities inadvertently stray into the provision of payment services that would require PSD2 authorisation.

The European Banking Authority (EBA) issued an Opinion in 2022 which is helpful in the context of CASPs providing payment services. The EBA stressed the need for the potential future revised PSD2 to pay close attention to the treatment of EMTs, the issuers of which are proposed to be required to conform to requirements under the EMD2, and which

are proposed to fall in scope of the definition of "funds" for the purposes of PSD2.

Where CASPs provide payment services, Article 70(4) of MiCA provides:

> "Crypto-asset service providers may themselves, or through a third party, provide payment services related to the crypto-asset service they offer provided that the crypto-asset service provider itself, or the third party, is authorised to provide those services under Directive (EU) 2015/2366.
>
> Where payment services are provided, crypto-asset service providers shall inform their clients of all of the following:
>
> (a) the nature and terms and conditions of those services, including references to the applicable national law and to the rights of clients;
>
> (b) whether those services are provided by them directly or by a third party."

Revised EU Framework for payment services and electronic money

PSD2 is to be replaced by the new EU legislative package, comprising a new Payment Services Regulation (PSR) and a new Payment Services Directive (PSD3). You can read an overview of these proposals in our previous briefing Keeping pace with EU payments: The PSD3 and Open Finance proposals. As at the time of writing, the new package is still proceeding through the EU legislative process, with trilogue negotiations yet to begin. The PSR/PSD3 package is expected to apply from 2026/2027.

Data protection and access to customer data

GDPR – Processing of personal data

Depending on its activities, a CASP is likely to be processing many types of personal data of customers – for example, identification data, contact information, authentication data (that is, biometric data, usernames, passwords), transactional data, etc. The EU General Data Protection Regulation (GDPR) applies to:

- Controllers and processors that process personal data in the context of the activities of an EU establishment, regardless of whether the data processing takes place in the EU or not.
- Non-EU controllers and processors with no EU establishment that offer goods or services to individuals in the EU or monitor their behaviour that takes place in the EU.

GDPR defines personal data as any information relating to an identified or identifiable person (called a 'data subject'). An authorised CASP could be either a controller or a processor in relation to personal data (the European Data Protection Board has published Guidelines on these concepts).

GDPR sets out high-level data processing principles and grounds for the lawful processing of personal data related to a data subject, as well as providing for a range of rights for data subjects, including the right of access and right to data portability. Sanctions for non-compliance with GDPR can be significant.

FIDA – Access to customer data

GDPR gives consumers a right to share their personal data held by any financial services provider directly with third-party providers. However, that right does not cover non-personal data related to business customers and is only applicable "where technically feasible."

The forthcoming Regulation on framework for financial data access (FIDA) promotes 'open finance' (an extension to the current open banking framework) and will enable data sharing and third-party access, in line with EU data protection and consumer protection rules. It will impose a legal obligation on 'data holders' to share customer data on a customer's request with certain regulated financial institutions or firms authorised as financial information service providers (FISPs) under a new dedicated authorisation regime. FIDA is expected to be adopted Q4 2024/Q1 2025 and to apply from 2026/2027.

Under FIDA, 'customer data' is the data collected, stored and otherwise processed by a financial institution as part of its normal course of business with customers. It includes both personal data (as defined in the GDPR) and other data that does not fall within the definition of personal data, such as that relating to business entities or financial product (contract) features.

CASPs are included in FIDA's list of 'data holders' and will therefore need to comply with FIDA's obligations on data holders, which include:

- putting in place the required technical infrastructure to make customer data available to data users;
- providing customers with a data access permission dashboard and strong protection of their personal data in line with EU data protection law; and
- becoming members of one or more financial data sharing schemes, governing access to customer data.

As the obligations on data holders arise on request of other institutions, in practice it will be necessary to be able to comply with the relevant requirements. This will require building internal systems to ensure that data is categorised and stored in a manner where it can be made available which in turn will require putting in place new systems and processes.

Of course, FIDA also represents an opportunity for CASPs to act as data users and obtain information from other financial services providers or FISPs in order to enhance the provision of the services they are offering. Where CASPs decide to make use of this, they will need to comply with FIDA requirements on data users; for example, they must access customer data only for the purpose they have been granted permission, prevent the transfer of non-personal data when unlawful, and comply with customer security and storage limitation requirements.

Traceability of funds and crypto-asset transfers – extension of the travel rule to crypto-assets from December 2024

Regulation (EU) 2015/847 on information accompanying transfers of funds, known as the Revised Wire Transfer Regulation (revised WTR) aims to prevent terrorists and other criminals from accessing payment systems for transferring their funds. The Revised WTR has applied since 26 June 2017. It sets out requirements, known as the 'Travel Rule', for payment service providers (PSPs) to send information on the payer and payee with transfers of funds and to ensure that this information is transmitted throughout the payment chain.

There has been much debate in the industry in respect of how the Travel Rule will apply to CASPS. However, CASPs will be obliged to comply with the Travel Rule with respect to crypto-asset transfers. Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (known as the Wire and Cryptoasset Transfer Regulation, or WCTR) extends the Travel Rule to crypto-asset transfers. It came into force on 20 June 2023 and applies from 30 December 2024.

CASPs involved in the transfer of crypto-assets will be required to comply with obligations to ensure the information on the originator and beneficiary of crypto-asset transfers accompanies these transfers throughout the payment chain, and is available to competent authorities. The obligations for CASPs resemble the obligations on PSPs under the revised WTR, but are slightly different to reflect the fact that the transfer is of crypto-assets rather than funds. For example, there are no derogations for low-value transfers, and the WCTR requirements reflect the FATF requirement that all crypto-asset transfers are treated as cross-border transfers. As with other applicable frameworks, any processing of personal data for the purposes of the WCTR must comply with the GDPR.

In practice, for a while CASPs have been working hard to put in place relevant compliance measures for the Travel Rule in reliance on relevant technical solutions made available in the industry. The interpretation of these requirements and expectations in different member states may not be fully aligned, which means that it will be necessary to closely follow how industry guidance and approaches develop.

Internal controls for compliance with sanctions and other restrictive measures

Union restrictive measures[2] are binding on any person or entity under the jurisdiction of EU member states, and their violation might constitute a criminal offence. Restrictive measures applicable to financial institutions comprise targeted financial sanctions and measures, as well as sectoral measures (e.g. economic and financial measures). The EBA has been concerned that not all institutions understand or address their exposure to risks associated with restrictive measures, and that weaknesses in internal governance, screening systems and risk management systems expose financial institutions to legal risks, reputational risks and the risk of significant fines for non-compliance.

The EBA has finalised two sets of guidelines (the EBA Guidelines) to ensure uniform implementation of internal policies, procedures and controls for compliance with restrictive measures across the EU:

- One set of guidelines (EBA/GL/2024/14) are guidelines EBA has adopted on its own initiative under EU banking, payments and e-money legislation, and address all financial institutions within the EBA's supervisory remit and specify the governance arrangements and internal policies, procedures and controls these financial institutions should have in place to be able to comply with restrictive measures.
- A second set of guidelines (EBA/GL/2024/15) apply specifically to PSPs and CASPs and support Article 23 of the WCTR, specifying what PSPs and CASPs should do to be able to comply with restrictive measures when performing transfers of funds or crypto-assets.

Both sets of EBA Guidelines are intended to apply from 30 December 2025.

To comply with the EBA Guidelines, CASPs will need to put in place policies, procedures and controls to ensure compliance with restrictive measures. These must be proportionate to the nature and size of the CASP, the nature, scope and complexity of their activities, and their exposure to restrictive measures. The Guidelines introduce detailed requirements including:

- CASPs must select a screening system that is adequate and reliable to comply effectively with their restrictive measures obligations - this should include considering whether they have access to the resources necessary to use the chosen system effectively.
- CASPs must define the dataset to be screened against restrictive measures adopted by the EU on the basis of EU Treaties and, where relevant, national restrictive measures. Data held must be sufficiently accurate, up to date and detailed to enable them to determine if a party to the transfer, their beneficial owner or any person purporting or being authorised to act on their behalf is subject to restrictive measures. A CASP's internal systems should ensure this dataset is updated immediately after a new restrictive measure enters into force, or an existing restrictive measure is updated or lifted.
- CASPs should screen their entire customer database regularly and determine the frequency of that customer screening (including appropriate trigger events) based on their restrictive measures exposure assessment. The EBA Guidelines provide details of the minimum customer information that they should be screening. Screening should comprise:
  - verifying whether a person, entity or body is designated;
  - managing the risks of violation of restrictive measures; and
  - managing the risks of circumvention of restrictive measures.
- CASPs should also screen all transfers of crypto-assets before making the crypto-assets available to the beneficiary, whether they are carried out as part of a business relationship or

2 Restrictive measures are defined in Article 2(1) of Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures and amending Directive (EU) 2018/1673.

as part of a one-off transaction. The EBA Guidelines specify the minimum data that should be screened to assess whether a transaction could be affected by applicable restrictive measures.

- CASPS must have in place internal policies and procedures to freeze transfers of crypto-assets when an internal analysis of an alert confirms that the possible match is the designated person or entity, or owned, held or controlled by a designated person.
- Where CASPs propose to outsource screening activity, the EBA Guidelines also specify the key principles that should be applied to the outsourcing arrangements. The ultimate responsibility for complying with the restrictive measures lies with the CASP.

AUTHORS

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

Sara Evans
Senior Associate Knowledge Lawyer
T: +44 207006 2557
E: sara.evans@cliffordchance.com

Yolanda-Alma Ghita-Blujdescu
Senior Associate
T: +352 48 50 50 489
E: yolanda.ghita-blujdescu@cliffordchance.com

CONTACTS

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

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

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

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

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

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

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

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

Francisco Pizarro
Abogado
T: +34 91 590 4150
E: francisco.pizarro@cliffordchance.com

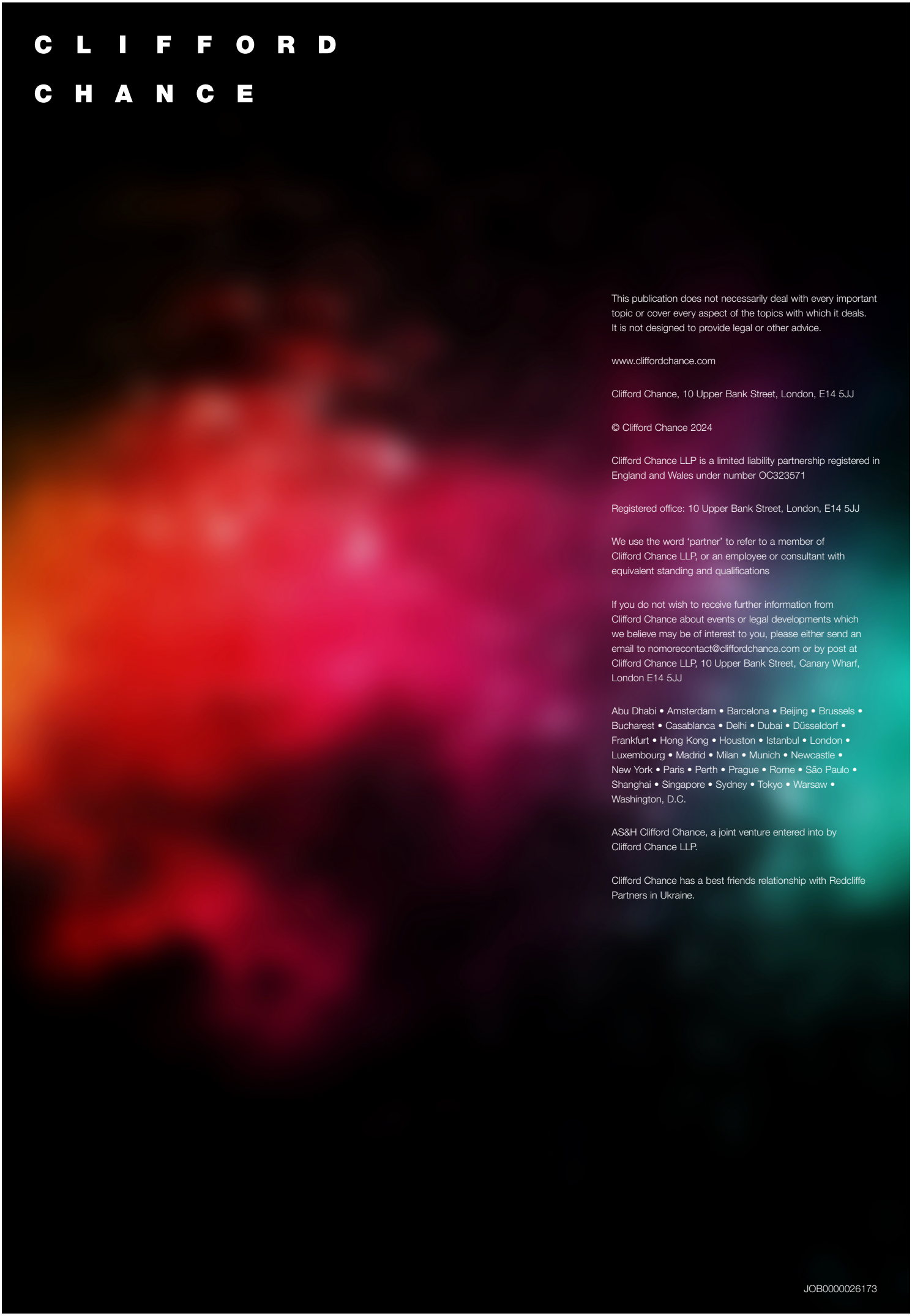
Monica Sah
Partner
T: +44 207006 1103
E: monica.sah@cliffordchance.com

Marina Sarkisjan
Senior Associate
T: +31 20 711 9517
E: marina.sarkisjan@cliffordchance.com

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

CLIFFORD

CHANCE



www.cliffordchance.com

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

JOB0000026173