CLIFFORD
CHANCE

PAYMENTS TRENDS 2021: WHAT WILL THE NEW YEAR MEAN FOR REGULATION AND ENFORCEMENT?

— THOUGHT LEADERSHIP

JANUARY 2021

PAYMENTS TRENDS 2021: WHAT WILL THE NEW YEAR MEAN FOR REGULATION AND ENFORCEMENT?

There has been a renewed focus on the payments sector and its regulation. COVID-19 and its impact on spending habits and the Wirecard scandal are two of the contributing factors. But what's next? We explore five themes likely to drive regulatory change for payments, as well as shape the enforcement policies of global regulators over the next 12 months.

1

A new roadmap for cross-border payments

2021 will bring renewed international efforts to address challenges and frictions in cross-border payments, which are still significantly slower, more expensive and less transparent than domestic payments. Correspondent banking (a key channel for cross-border payments) continues to decline, limiting access to cross-border payments despite the Financial Stability Board's (FSB) work since 2015 to address this issue.

Frictions and challenges facing cross-border payments include:

- fragmented data standards and lack of interoperability between jurisdictions;
- practical challenges in meeting global anti money laundering/ counter terrorist financing and other regulatory requirements;
- high transaction costs; and
- different operating hours across time zones.

While improved efficiency of existing systems can reduce some of these frictions, the focus is increasingly shifting towards how new infrastructures such as global stablecoins and central bank digital currencies (CBDCs) could offer more radical solutions to these deep-seated issues. Both public and private sector innovation and cooperation, based on internationally agreed standards, will be key to success.

Recent international publications on cross-border payments, global stablecoins and CBDCs indicate how policy makers intend to address these challenges, both through short-term steps to improve efficiency and in the longer term through considering the role global stablecoins and CBDCs could play in cross-border payments.

The FSB published its **Stage 3 Roadmap** for cross-border payments in October 2020, building on a **CPMI Report** to the G20 on the building blocks of a global roadmap for enhancing cross-border payments from July 2020. Alongside the Roadmap, the FSB also published **high-level recommendations** for regulation, supervision and oversight of "global stablecoin" arrangements in October 2020.

Also in October 2020, BIS and a group of several central banks published their **Report on foundational principles and core features of CBDCs**. As envisioned by the FSB Roadmap, we expect work on these issues to continue during 2021.

At a domestic level, we will see more economies experimenting with, and getting ever closer to wide-scale issuance of, CBDCs. In January 2021, it has already been confirmed that the People's Bank of China's pilot programme to test and promote its CBDC (the digital Renminbi) has been extended to Beijing and other cities, following large-scale trials in Shenzhen and Suzhou. While China has prohibited private crypto issuance and trading onshore, legislators are amending the law to establish digital Renminbi as legal tender, treading a cautious but steady path to country-wide adoption. In the US, a private organisation, named the Digital Dollar Project, **published a whitepaper in May 2020** making a case for US lawmakers and public officials to support a US CBDC. The US Federal Reserve later acknowledged that it is actively

investigating distributed ledger technologies and how they might be used to digitise the dollar. The Dubai Government is also exploring its first approved blockchain-based digital currency, EmCash, which is intended to be pegged to the value of the UAE dirham.

Diem, or the Facebook-associated stablecoin formerly known as Libra, is also anticipated to launch in 2021 once it has received Swiss regulatory approval. With several changes since its original June 2019 multicurrency-backed incarnation, it is expected initially to launch a single dollar-backed coin alongside other compliance enhancements made to satisfy regulatory concerns.

Diem would enter the market at a time when US banking regulators appear to be warming to stablecoins. The US Office of the Comptroller of the Currency "(**OCC**)" issued a 2020 **interpretive letter** affirming that OCC-regulated banks can provide digital asset custody services to customers, and a 2021 **interpretive letter** explicitly allowing the use of stablecoins to engage in and facilitate payment activities. The OCC also **recently announced** its first conditional granting of a national trust bank charter to the well-known digital asset custodian, Anchorage Trust Company. The national bank charter will make it easier for Anchorage to partner with banks and other financial institutions that want to provide customers with stablecoin custody services.

Legislative regimes for stablecoins and other cryptoassets are also being developed internationally, including in the UK, as outlined under an **HM Treasury consultation** published in January 2021 and in Hong Kong, as outlined in a **consultation** launched in November 2020.

In September 2020, the European Commission published its **Digital Finance Package**, which builds on its **EU Fintech Action Plan** published in 2018. The Digital Finance Package introduced the EU's Digital Finance Strategy and a **renewed strategy for modern and safe retail payments**. Crucially, it also introduced legislative proposals for:

- a Markets in Cryptoassets Regulation, to facilitate their use while mitigating risks for investors and financial stability (**MiCA** - see our take **here**); and
- a regulatory framework on digital operational resilience (**DORA**) (see further below).

There have also been some significant recent developments in relation to crypto regulation across the Middle East. In the United Arab Emirates (UAE), the Securities and Commodities Authority has recently published new cryptoasset regulations (which Clifford Chance are pleased to have assisted in the drafting of), setting out the onshore licensing regime for offering cryptoassets, including participating in initial coin and security token offerings and providing custody services and other financial activities in relation to cryptoassets. The regime covers stored value stablecoins and other digital tokens across the payments and investment space.

The UAE's financial free zones, the Abu Dhabi Global Market and Dubai International Financial Centre, have also issued comprehensive updated regulatory frameworks governing money services businesses which will also pick up Financial Action Task Force or FATF standards for virtual currency providers and regulate stablecoins and other digital assets relating to payments.

Antitrust and the taming of Big Tech

2

Big Tech remains high on global regulators' agendas. Major digital technology firms such as Facebook, Google and Apple have continued to find themselves under increased scrutiny in relation to their data use and alleged anti-competitive behaviour generally, including in financial products. For example, the European Commission announced in June 2020 that it had opened an antitrust investigation into Apple Pay for potentially anti-competitive agreements and the abuse of a dominant position by limiting access to its "tap and go" functionality on iPhones for payments in stores and refusing rival companies access to Apple Pay.

The next step is the creation of new "Big Tech" regulators and the establishment of

dedicated regulatory regimes that will impact the ability of key tech players to wield market power in rolling out new financial products. The European Commission recently unveiled its far-reaching proposals for regulation of digital platforms and online intermediaries. The Digital Markets Act (DMA) will require digital platforms that are designated as "gatekeepers" to refrain from a long list of practices that are considered to limit competition or otherwise to be unfair. In contrast, the Digital Services Act (DSA) focuses on regulating the way that providers of online intermediary services interact with their customers and users, and their obligations in respect of harmful or illegal content, in order to create "uniform rules for a safe, predictable and trusted online environment".
In combination, the two pieces of proposed legislation will create Europe's most interventionist sector-specific regulatory regime in decades, and would require significant changes to the business practices of large digital sector players, as well as, potentially, smaller competitors. While it is likely to take 18-24 months for final texts to be agreed with the European Parliament and Council of the EU, 2021 will see a flurry of activity and amendments to the proposals.

In the UK, in December 2020, the CMA issued **advice** to the UK government on the design and implementation of the UK's new pro-competition regime for digital markets. If implemented, the new regime will govern the most powerful tech firms with strategic market status (SMS) and see the creation of a new Digital Markets Unit (DMU) with powers to set clear rules and impose penalties. The regime will include a new legally binding code of conduct tailored to each firm, the introduction of data access and interoperability requirements, and mandatory merger filings for businesses designated with SMS. The FCA will also be given enforcement and implementation powers in regulated sectors. As with the DMA and the DSA, while the SMS regime is expected to apply to only a limited number of the most powerful digital firms, its overall impact is likely to be much further reaching.

The government has committed to establishing and resourcing a new DMU from April 2021 and is to consult on proposals for a new pro-competition regime in early 2021.

Also in the UK, the Payment Systems Regulator is currently conducting an industry-wide consultation with respect to its September 2020 interim report on the supply of card acquiring services and related competition issues.

In the U.S., companies can expect continued scrutiny of Big Tech as well as greater focus on the financial sector. In autumn 2020, the Antitrust Division of the Department of Justice (DOJ) announced its intended focus, highlighting rapid change occurring in the financial sector and the potential for anti-competitive conduct. In November 2020, the DOJ sued to block Visa's acquisition of Plaid, a fintech company, and the companies abandoned the transaction in early 2021. Visa's and Plaid's decision to abandon their transaction will likely encourage future challenges of US acquisitions by a dominant company of an emerging competitor.

3

Operational resilience and personal accountability

High profile IT failures and the impact of COVID-19 meant that operational resilience (or ensuring the continuity of key business services) was a high priority for regulators during 2020. This will continue throughout 2021. Growing digitisation of customer experiences, greater automation of internal processes and increased use of third-party providers all make firms increasingly susceptible to technology disruption events.

In September 2020, the European Commission unveiled its proposal for an EU regulatory framework on digital operational resilience (**DORA** – see our take **here**), to better align financial entities' business strategies with the conduct of internet and communication technology (ICT) risk management and to prevent and mitigate cyber threats, published as part of the EU's **Digital Finance Package**.

DORA requires firms to have internal governance and control frameworks that ensure an effective and prudent management of all ICT risks.

Management bodies will be required to define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework. It takes a "sliding scale" approach to compliance with critical businesses having greater compliance obligations than others. 2021 will see DORA continue through the EU legislative process, with approval from the European Parliament and Council of the EU still required.

We anticipate that domestic regulators will also increasingly look to formalise existing operational resilience guidance into specific regulations throughout 2021. In the UK, the FCA, the Prudential Regulation Authority and the Bank of England will finalise rules and policy statements on a new operational resilience framework for financial services firms, following several consultations which closed last year.

The final rules are likely to be implemented by firms by late 2021/early 2022 and will require firms to identify their important business service and impact tolerances with a strict liability offence for failing to remain within impact tolerance levels. Enhanced governance obligations and a greater emphasis on the responsibilities of the current senior manager function, will reinforce personal accountability at board level with clear links between oversight responsibilities and decision making. Firms will need to put in place systems and controls to implement a robust communications strategy, expand self-assessment testing capacities, assess the systemic materiality of third party partnerships, and carry out mapping exercises of resources required to deliver each of the core business services.

In Singapore, to address growing technology and cyber risks for financial institutions becoming increasingly reliant on technology, the MAS recently issued a set of revised Technology Risk Management (TRM) Guidelines (TRM Guidelines), setting out the regulator's higher expectations in the areas of technology risk governance and security controls in financial institutions. It provides additional guidance on the roles and responsibilities of the board of directors and senior management in managing technology and cyber risks, making it clear that both are expected to set the tone from the top and cultivate a strong culture of technology risk awareness and management.

The TRM Guidelines also require the board of directors and senior management to ensure that a Chief Information Officer, a Chief Technology Officer or Head of Information Technology, and a Chief Information Security Officer or Head of Information Security, are appointed. In parallel, an individual accountability regime, that will take effect from September 2021, will also require the identification of senior managers with core management functions, such as a chief technology officer, who must be fit for their roles.

The MAS has also proposed to introduce new powers to issue rules on TRM on any financial institution in relation to its systems, irrespective of whether the systems support a regulated activity. The MAS views this as necessary as systems that do not support regulated activities can pose contagion cyber risk to systems that do, due to inter-linkages. To highlight the importance of compliance with TRM rules, the MAS has proposed to set the maximum penalty for breaches of the TRM rules at S$1 million.

Globally, we are also likely to see an increase in enforcement action relating to operational disruptions. Regulators may seek to hold firms accountable for failures in their responses to the challenges resulting from COVID-19, particularly where disruptions arise from cost-cutting in any economic downturn brought on by the pandemic. In parallel, the same technology disruption events (and any criticism from regulators,) are likely to give rise to civil claims – whether for breach of contract, negligence or data breach litigation.

Firms will need to act swiftly to factor new regulatory requirements into existing operational resilience frameworks and to ensure that any policy changes required for compliance can be implemented in time, to reduce the chance of suffering a significant operational disruption and the risk of associated enforcement action.

4

Safeguarding and prudential risk management

Robust safeguarding arrangements are integral to ensuring that funds are returned to customers in the event of an insolvency of a payment services or an e-money firm. The COVID-19 pandemic and the collapse of Wirecard in 2020 have brought payments firms' prudential risk management and safeguarding arrangements into the spotlight as a key supervisory priority for 2021.

In the UK, the Financial Conduct Authority (FCA) had already been focusing on safeguarding rules for payment institutions. The FCA carried out a review of non-bank payment service providers' compliance with safeguarding requirements in early 2019, resulting in a **Dear CEO letter** that required all electronic money institutions and authorised payment institutions to review their safeguarding arrangements. However, the COVID-19 pandemic led the FCA to look at this with renewed focus, quickly introducing new **Guidance** in July 2020 to strengthen payment firms' prudential risk management and arrangements for safeguarding customers' funds in light of the exceptional circumstances of the pandemic.

We expect that the status of safeguarded funds will continue to attract attention. The FCA considers that firms hold safeguarded funds on trust for their customers, even though this is neither expressly stated in the Second Payment Services Directive nor in the UK Payment Services Regulation 2017. The FCA cited the ruling in ***Supercapital (in administration)*** **[2020] EWHC 1685 (Ch)** where the judge stated that the Payment Services Regulation 2017 creates a statutory trust. It is possible that this view may be subject to further challenge in subsequent court cases.

Regulatory scrutiny of the prudential risk management of payment and electronic money institutions is also likely to continue during 2021.

In the UK, the need for strong risk management and governance arrangements can be seen from the results of the FCA's **Covid-19 financial resiliency surveys** (published on 7 January 2021), which found financial resilience concerns in some members of the payments and e-money sector. As part of satisfying the FCA that there are robust governance arrangements, firms are required to have a wind-down plan to manage their liquidity and resolution risks. Alongside this, the UK is expected to introduce a new "special administration regime" for payment institutions and e-money issuers to enhance the protection for customers if a payment or electronic money institution enters into insolvency. An HM Treasury **consultation** on the proposed regime published on 3 December 2020 notes that, in six recent insolvencies involving payment and electronic money institutions, five firms have not returned funds to customers.

In Singapore, the MAS currently has the power to impose safeguarding requirements on major payment institutions in respect of certain payment services, which include merchant acquisition services. In view of the changing payment token landscape and to allow the regulator to act swiftly in this space when needed, there are also legislative proposals to extend 'the MAS' s power to impose user protection measures on certain digital payment token service providers, and these measures may include anti-commingling measures, ring-fencing measures and maintaining customers' assets in a prescribed manner.

In Japan, the Japanese Financial Services Agency (JFSA) introduced a robust mechanism for safeguarding customer money kept by FTSPs when the FTSP regulatory framework was established in 2010. The June 2020 reform of the Payment Services Act will make the current single licence regime more flexible by creating three categories of FTSP licence and requiring different safeguarding measures to be taken by FTSPs, depending on the maximum limit of the payment reflecting a principle of regulating based on risk. Other parallel legislative changes are also designed to reduce customer risk in the case of insolvency of FTSPs. The amended regulations will be implemented in spring 2021.

Continued expansion of Open Banking and Open Finance

Various jurisdictions have introduced (or are in the process of introducing) Open Banking regimes, allowing third-party payment service providers (TPPs) to initiate payments or access account information on behalf of customers. Competition is a key concern and driver for regulators overseeing such initiatives, with regulators expecting that firms will meet their regulatory responsibilities while competing on quality and value.

The UK

In the UK, initial take-up of Open Banking has been slow but steady, with over 2 million users at the start of 2021 (doubling in a year). We expect this to continue in 2021, as TPPs launch new products and customers become more confident about sharing data with regulated TPPs.

Perhaps more significant is the potential expansion of Open Banking to other types of accounts and financial products under a broader "Open Finance" initiative. For example, the UK Pensions Schemes Bill introduced in Spring 2020 includes a legislative framework that would enable individuals to view all their existing pension pots in a single dashboard format. The UK has also been considering other similar initiatives as part of its Smart Data review and the UK government published its proposed **Next steps for Smart Data** in September 2020. However, it will inevitably take time to develop legislative frameworks for further initiatives, which will be needed to ensure that third party providers are regulated where appropriate and to provide clarity around important issues such as security, consent, data use, privacy and ethics.

The rules on TPP access, strong customer authentication (SCA) and secure communication standards under the recast EU Payment Services Directive address some of these concerns in the context of Open Banking.

Following delays in implementation due to the impact of COVID-19, 2021 will see the SCA rules being applied in the UK. The FCA expects firms to be working towards their compliance milestones in line with the agreed UK Finance SCA **implementation plan** well in advance of the 14 September 2021 deadline. The FCA has stated *"any firm that fails to comply with the [SCA] requirements … will be subject to full FCA supervisory and enforcement action."* Firms are required to have reached a state of 'market readiness' by 31 May 2021 and 'full ramp up' by 13 September 2021, all with minimum customer disruption. UK Finance has stated that issuers will need to start checking randomly if e-commerce transactions are SCA compliant, and soft decline them if they are not. This means that payment service providers, gateways, e-merchants, and technology providers will need to be ready for SCA by the end of May 2021, to avoid any unnecessary declines.

For broader Open Finance initiatives, the FCA proposed "a new rights framework" in its December 2019 **Call for Input on Open Finance**, consisting of seven principles for data protection, complaints handling and customer consent tools. Responses to the call have outlined concerns that it would be very costly to extend the Open Banking access and consent model to other financial products, and that the proposed consent and tracking tools may be better provided by third parties. This indicates that we are likely to see further FCA consultation on this topic in 2021.

Singapore

In Singapore, Open Banking has been largely facilitated by the Monetary Authority of Singapore (MAS), which has encouraged banks to adopt application programming interfaces (APIs) since 2016 with the development of a financial industry API playbook. To promote Open Banking and facilitate the adoption of open APIs, the MAS has also led several other initiatives, such as the 2018 launch of the API Exchange, an open architecture API marketplace and sandbox platform.

In December 2020, Singapore also saw the launch of the Singapore Financial Data Exchange (SGFinDex), the world's first public digital infrastructure, jointly developed by the public sector in collaboration with the banking industry. The SGFinDex uses a national digital

identity and centrally managed online consent system to allow individuals to access the financial information held across different government agencies and financial institutions. As a public digital infrastructure, stringent security measures are in place to safeguard personal data, and the authentication and authorisation process is underpinned by the use of the national digital identity. Participating financial institutions continue to be subject to existing personal data protection legislation when participating in this initiative. In the next phase of SGFinDex, it is envisaged that individuals will be able to access information on their insurance policies held with insurers and their holdings of stocks at the Central Depository of Singapore.

In 2021, we expect to see increased digital innovation and competition between financial services providers in Singapore arising from the use of SGFinDex, and further government initiatives to support the push towards Open Banking.

Japan

In Japan, the Open Banking regime was introduced from June 2018 to regulate electronic payment service providers (EPSPs), which initiate payments or access bank account information on behalf of customers. However, broader Open Banking principles have been reflected for non-bank fund transfer service providers (FTSPs) that offer payment services using funds cashed out from customers' bank accounts since that licensing system was established in 2010. Although these new payment services have blossomed with government support, there has been tension with banks. In the wake of a scandal, where customer money was stolen from bank accounts which were breached via FTSP accounts in September 2020, the level of customer authentication and cyber security management requested of regulated EPSPs and FTSPs has become stricter. While the Fair Trade Committee of Japan noted in an April 2020 report that the current level of fees charged by banks could be an impediment to EPSPs or FTSPs building sustainable businesses, and encouraged banks and the Japanese Bankers Association to resolve these issues, payment service providers will face increased costs arising from a higher standard of establishing and maintaining security measures to access the banking system.

The Middle East

Whilst still in its infancy in the Middle East, local regulators are placing an increasing focus on Open Banking and several regimes are being developed. The Central Bank of Bahrain (CBB) has taken the lead in introducing Open Banking regulations in the region, with amendments to the CBB rulebooks made in December 2018. Following the 2018 establishment of a regulatory sandbox, in January 2021 the Saudi Central Bank (SAMA) announced the issuance of its new Open Banking policy. SAMA plans to launch a new Open Banking regime during the first half of 2022.

Related developments have also taken place in the UAE in respect of the regulation of electronic payment and stored value systems such as e-wallets and mobile payments. 2020 saw an overhauling of the regulatory framework for digital payments across the UAE. The UAE Central Bank replaced its 2017 stored value regulations and introduced detailed provisions on licensing and operating digital payment businesses onshore in the UAE, as well as an express prohibition on the operation and marketing of foreign stored value facilities. It has also proposed a further draft regulation on retail payment services and card schemes, setting out a comprehensive regime for the regulation of payment services and seeking to align with international standards. The UAE's financial free zones, the Abu Dhabi Global Market and Dubai International Financial Centre, similarly issued updated and comprehensive regulatory frameworks governing money services businesses, to bring their standards broadly in line with the EU Payment Services Directive.

Whilst these new frameworks bring the UAE and its financial free zones closer to international standards in this area, the barriers to entry into the UAE market have been raised. Whereas firms previously did not require a formal licence, there is now a comprehensive framework in line with international standards.

CONTACTS

Authors

Samantha Ward
Partner
London
T: +44 207006 8546
E: samantha.ward@cliffordchance.com

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

Cheryl Jones
Senior Associate
Knowledge Lawyer
London
T: +44 207006 2386
E: cheryl.jones@cliffordchance.com

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

Belgium

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

China

Kimi Liu
Counsel
Beijing
T: +86 10 6535 2263
E: kimi.liu@cliffordchance.com

Yan Li
Associate
Beijing
T: +86 10 6535 2284
E: yan.li@cliffordchance.com

France

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

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

Germany

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

Dr. Christian Hissnauer
Senior Associate
Frankfurt
T: +49 69 7199 3102
E: christian.hissnauer@cliffordchance.com

Hong Kong

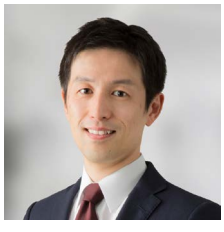
Rocky Mui
Partner
Hong Kong
T: +852 2826 3481
E: rocky.mui@cliffordchance.com

Matthew Wan
Associate
Hong Kong
T: +852 2826 3562
E: matthew.wan@cliffordchance.com

Italy

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

Japan



Yusuke Abe
Partner
Tokyo
T: +81 3 6632 6332
E: yusuke.abe@cliffordchance.com

Hitomi Kurokawa
Senior Associate
Tokyo
T: +81 3 6632 6632
E: hitomi.kurokawa@cliffordchance.com

CONTACTS

Luxembourg

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

Netherlands

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

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

Poland

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

Singapore

Lena Ng
Partner
Singapore
T: +65 6410 2215
E: lena.ng@cliffordchance.com

Sheena Teng
Senior Associate
Singapore
T: +65 6506 2775
E: sheena.teng@cliffordchance.com

Spain

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

UAE

Jack Hardman
Counsel
Dubai
T: +971 4503 2712
E: Jack.Hardman@cliffordchance.com

United Kingdom

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

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

Laura Nixon
Senior Associate
Knowledge Lawyer
London
T: +44 207006 8385
E: laura.nixon@cliffordchance.com

Kate Scott
Partner
London
T: +44 207006 4442
E: kate.scott@cliffordchance.com

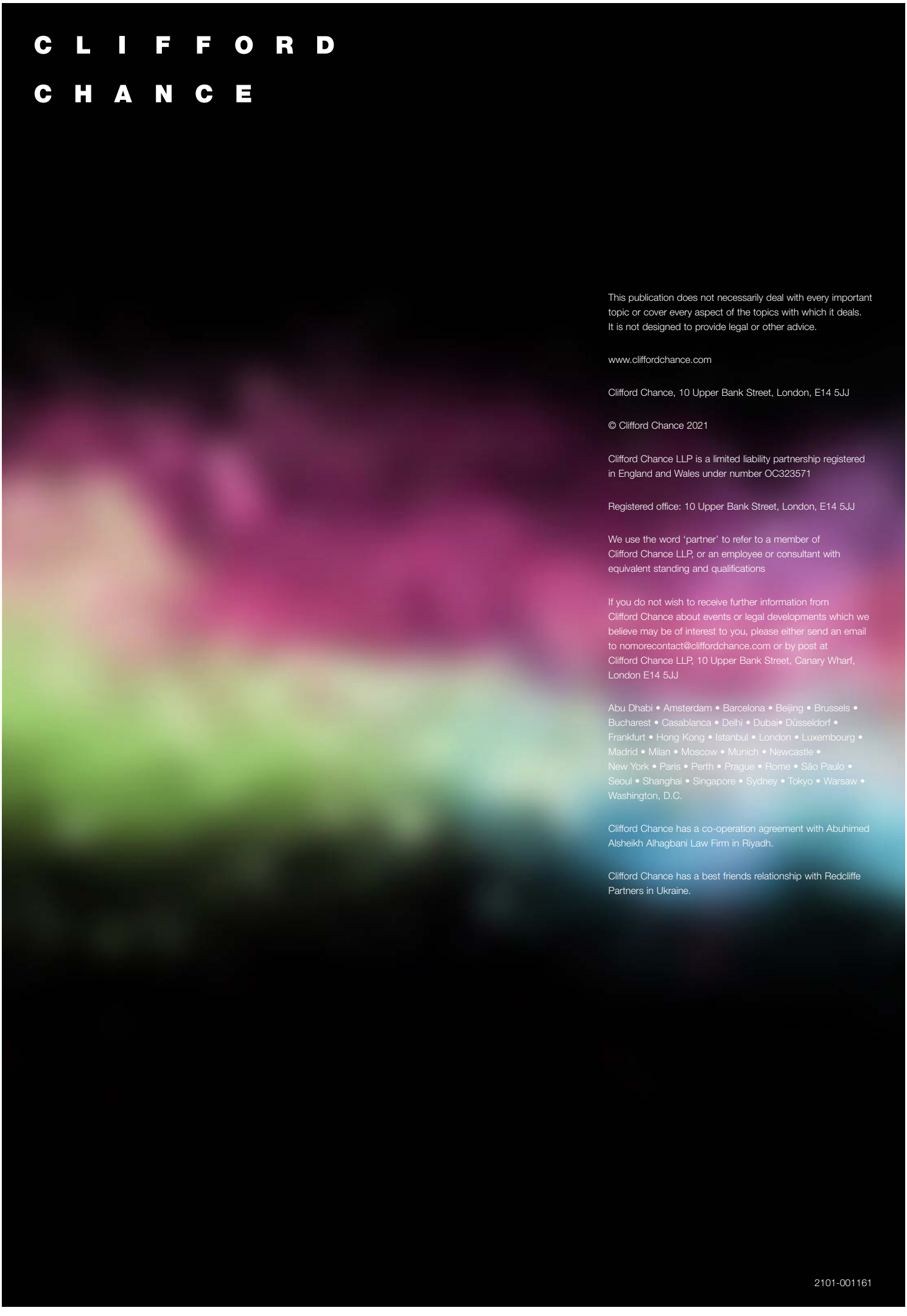
Washington DC

André Duminy
Partner
London
T: +44 207006 8121
E: andre.duminy@cliffordchance.com

Steve Gatti
Partner
Washington
T: +1 202 912 5095
E: steven.gatti@cliffordchance.com

Megan Gordon
Partner
Washington
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Philip Angeloff
Counsel
Washington
T: +1 202 912 5111
E: philip.angeloff@cliffordchance.com



C L I F F O R D

C H A N C E

www.cliffordchance.com

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

2101-001161