CLIFFORD
CHANCE

PAYMENTS TRENDS 2023

— THOUGHT LEADERSHIP

MARCH 2023

PAYMENTS TRENDS 2023

Regulation of the payments sector continues to evolve as technology drives further changes to consumer and wholesale payments, from blockchain-based central bank digital currencies and stablecoins to operational resilience and new embedded finance offerings. We explore seven payments areas where we will see regulatory change, or renewed focus on enforcement, from global regulators over the next 12 months.

1 Cross-border payments

International efforts to address challenges and frictions in cross-border payments are ongoing. In February 2023, the Financial Stability Board (FSB) published a report detailing actions to be taken on payment system interoperability, legal, regulatory and supervisory frameworks and cross-border data exchange for the next phase of work under the G20 Roadmap for Enhancing Cross-Border Payments. The FSB makes clear that much remains to be done to enhance the cost, speed, access and transparency of cross-border payments ahead of the G20 Roadmap's 2027 target date.

What's next?

- We will see regulators forcing change, for example around instant euro payments in the EU. Given the slow uptake in the market of technology to process euro payments instantly, the Commission is proposing to introduce the so-called Instant Payments Regulation. This would require payment service providers that provide credit transfers in euro to offer instant payments in euro, with an equivalent, or a lower, charge than that applicable to non-instant euro credit transfers.
- Global regulators and market players will work to drive payment system interoperability in line with the G20 Roadmap's priorities, including interlinking arrangements for payment systems that reduce reliance on intermediaries by allowing banks and other payment service providers to transact directly.
- Developments in the domestic space will also allow the focus to move overseas. For example, in the US, the Federal Reserve expects to launch the FedNow Service, a new instant payment service that would enable consumers and businesses to settle payments nearly instantaneously through deposit accounts with banks that maintain a master account at a Federal Reserve Bank. The Federal Reserve has stated that, at launch, the FedNow Service will support only domestic payments between US depository institutions, but the service could potentially be used to facilitate cross-border payments if access is expanded to non-US financial institutions in the future.

2 Central bank digital currencies

Currently, more than 114 countries, representing over 95 percent of global GDP, are exploring the opportunities that central bank digital currencies (CBDCs) – a digital representation of fiat money issued by a central bank – might bring. A few countries, including the Bahamas and Jamaica, have already launched CBDCs, while the majority are still in pilot or research stages. While some CBDCs are based on blockchain or distributed ledger technology (DLT), many jurisdictions are exploring multiple technology possibilities.

Many CBDC projects have a domestic, retail focus. However, international standard-setting bodies such as the Bank for International Settlements (BIS) are pushing for the use of CBDCs to facilitate cross-border payments. Solving the issue of interoperability between initiatives is key.

What's next?

- We will see the next big updates coming from key jurisdictions. China's pilot is set to expand in 2023, while the ECB is over halfway through its two-year investigation into a digital euro, with a decision expected later this year. In the UK, a Bank of England consultation on the possible introduction of a digital pound is open until 7 June 2023, following which the Bank and Government will make a decision whether to proceed.
- Other jurisdictions will take a more cautious approach. The US remains nominally supportive of a US digital dollar, but two significant hurdles remain: the US Congress has yet to act on authorising legislation for a US CBDC; and there remains widespread scepticism among policymakers as to whether a US CBDC is necessary, with concern around purported risks (for example, drain on commercial bank liquidity during stress, privacy concerns), and a view that improvements to existing payment systems will deliver similar benefits.
- A focus on co-operation between central banks to ensure interoperability, for example through participation in international cross-border payments initiatives such as the BIS's mBridge project. The Monetary Authority of Singapore's Project Ubin+, which launched in November 2022, is another example of an international collaboration involving the Banque de France and the Swiss National Bank exploring the cross-border exchange and settlement of Swiss franc, Euro and Singapore dollar wholesale CBDCs. For future projects, we expect to see payments coupled with innovation in financial market infrastructure more generally, such as the issuance of digital securities.

For more, watch our recent presentation The future of banking – can CBDCs change the financial markets?

Stablecoins

3

In contrast to publicly issued CBDCs, stablecoins are a privately issued type of cryptoasset based on DLT which include a mechanism to minimise price fluctuations and 'stabilise' their value. Their aim is to provide an alternative form of low-risk digital unit which could be used directly by businesses and consumers. The most common potential stabilisation option is the collateralised stablecoin model, where stability is achieved by linking the currency to a reserve of stable real assets such as fiat currencies or commodities. Alternatives include crypto-collateralised stablecoins (where a reserve is made of other cryptocurrencies) or uncollateralised stablecoins (which do not have any reserve but instead use central bank-like monetary policy to maintain a fixed price by controlling supply with algorithms which respond to market conditions).

Global regulators have been closely watching stablecoin market developments since the failed Libra/Diem coin, and last year's collapse of USD Terra raised further concerns. This has led several jurisdictions, including the UK, in its draft Financial Services and Markets Bill, to prioritise crafting a regulatory framework for stablecoins ahead of other cryptoassets. Japan is currently in the process of introducing regulatory framework for issuing and distributing stablecoins in addition to the regulatory framework for cryptoassets and security tokens implemented in 2020. In contrast, the EU's new Markets in Crypto-Assets Regulation (MiCA) will introduce a comprehensive new regulatory framework for issuing and offering all cryptoassets, while layering on significant additional requirements for the offering of stablecoins.

In the US, several bills have been proposed to regulate stablecoin issuers, each imposing variations of bank-like requirements (such as FDIC insurance, chartering framework, liquidity requirements), though none have made it to a vote on the floor of the US Congress.

What's next?

- 2023 will see the formal adoption of the EU's MiCA, with its provisions likely to apply from certain points in 2024. The UK Financial Services and Markets Bill is also anticipated to be passed in 2023. With the introduction of these regimes, the pathway is open for using stablecoins in more traditional consumer and wholesale environments.

- We will also see further legislative and regulatory developments in additional jurisdictions. In the US, we anticipate the introduction of new bills and continued debate on the proper regulatory framework for stablecoin issuers, including on how to address uncollateralised or algorithmically-stabilised stablecoins such as USD Terra and the extent to which stablecoin issuers may be regulated like banks.

For more, read our briefings Central bank digital currencies and stablecoins – how might they work in practice? and Japan to have world's first clear regulatory framework for stablecoins.

Operational resilience

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. The financial, reputational and societal impact of high-profile IT failures means that operational resilience (or ensuring the continuity of key business services) remains a high priority for boards, regulators and consumers alike.

In October 2022, following a G20 request, the FSB published a consultation on Achieving Greater Convergence in Cyber Incident Reporting. The FSB proposals include recommendations to address the challenges to achieving greater international convergence in cyber incident reporting, work on establishing common terminologies related to cyber incidents and a proposal to develop a common format for incident reporting exchange.

The EU's new Digital Operational Resilience Act (DORA) is intended to establish uniform requirements for the security of network and information systems of companies operating in the financial sector, including cryptoasset service providers, as well as any critical third parties which provide information communication technologies services to them.

Following its departure from the EU, the UK has introduced a Financial Services and Markets Bill which includes proposals to regulate cloud service providers and other critical third parties supplying services to UK regulated firms and financial market infrastructures. Under the Bill, HM Treasury would have powers to designate service suppliers as 'critical' and the UK regulators would have new powers to oversee designated suppliers directly, which would be subject to new minimum resilience standards. Absent an intervening general election, the Bill should be passed and become law by the end of the current Parliamentary session (expected to be in May 2023). While the UK proposals have the same ambitions as the requirements under DORA, there are a number of differences between them including in relation to the 'critical' designation criteria and the enforcement regime.

What's next?

- Intranational efforts to streamline global standards will continue. In April 2023, the FSB is scheduled to publish a revised report to the G20 slated to include expectations for financial authorities' oversight of financial institutions' reliance on critical service providers, including "Big Tech" and fintech firms.
- Businesses providing payments technology will be faced with the significant legal burden of dealing with the requirements under DORA and the new UK regime (once in force) for contracting with payment service providers. DORA's introduction of a new incident reporting mechanism, including a requirement for "major" incidents to be reported to competent authorities within strict time frames, will require significant investment in processes.
- In the US, we expect the banking agencies to finalise proposed guidance on "third-party risk management", originally proposed in 2021, which will set supervisory expectations for risks raised by third-party relationships as well as heightened standards for providers of "critical services". Among other items, the guidance expects covered institutions to conduct due diligence and provide ongoing oversight of a third party's information security programme and information systems, as well as assessing the third party's ability to continue delivering services during a disruption event.

- We will see additional global regulators launching comprehensive regulatory regimes to ensure that financial institutions have appropriate internal governance and control frameworks around ICT use, including the use of third-party technology providers. We are also likely to see an increase in enforcement action by regulators relating to operational disruptions - TSB Bank plc was recently fined £48.65 million by UK financial regulators for operational risk management and governance failures relating to its IT upgrade programme. In parallel, the same technology disruption events are likely to give rise to civil claims and litigation – whether for breach of contract, negligence or data breaches.

For more, read our recent briefings DORA: What the new European framework for digital operational resilience means for your business and the UK Financial Services and Markets Bill: new rules for 'critical third parties'.

Where next for open finance?

5

Various jurisdictions have introduced open banking regimes, allowing third-party payment service providers (TPPs) to initiate payments or access account information on behalf of customers. Regulators expect that firms will meet their regulatory responsibilities while competing on quality and value.

Some jurisdictions have taken this further, applying the same approach to other types of accounts and financial products under a broader "open finance" initiative. Developing comprehensive legislative frameworks for such initiatives takes time but is critical to ensure that TPPs are regulated to provide clarity around i security, consent, data use, privacy and ethics and to build customer trust. In the EU, the rules on TPP access, strong customer authentication and secure communication standards under the recast EU Payment Services Directive address some of these concerns in the context of Open Banking and may provide a blueprint for expansion.

In the US, the Consumer Financial Protection Bureau (CFPB) is in the process of developing an Open Banking rule proposal, which would give consumers more control over their financial data by allowing them to access and share it with other providers. The rule is designed to encourage competition by making it easier for consumers to "walk away" from existing providers and port their financial data to other providers via application programming interfaces (APIs).

What's next?

- We will see a renewed focus on open finance with more innovative use cases being developed. We will see novel delivery of payment services channels for consumers, with web 3.0 and metaverse applications raising a new set of legal and regulatory questions.
- In the EU, publication of a new framework for Open Finance is scheduled for Q2 2023 following a consultation in 2022.
- In the US, we anticipate a proposed Open Banking rule to be issued by the CFPB later this year. Significant issues remain outstanding, including the extent to which the rule would apply to non-banks as well as privacy and data security concerns. Smaller banks, in particular, have urged the CFPB to phase-in a prohibition on "screen scraping", in which a third party uses a customer's log-in credentials to access their account information, as they do not have the tech resources to build a library of APIs.

The evolution of embedded finance

6

Embedded finance allows retailers and other (traditionally) non-financial companies to improve the customer experience by incorporating payments and financing options into their products and services. This is typically achieved by using technology solutions such as banking as a service (BaaS) and API-driven platforms.

Embedded lending, including the "buy now, pay later" (BNPL) model popularised by firms such as Klarna, has seen significant growth. With regulators concerned by the possible impact on consumer finances, scrutiny is growing.

What's next?

- We will begin to see BNPL specifically brought into regulatory frameworks. In the UK, in February 2023 HM Treasury published a consultation on draft legislation to bring BNPL products within the scope of the UK regulatory regime. And in the EU, a revised version of the consumer credit directive that would bring BNPL within its scope is going through the final stages of the legislative process.
- Data flows related to the provision of embedded financial services will be impacted by the evolving legal landscape for cross-border data transfer. New privacy laws and changes to data governance regimes are on the horizon in 2023 – including in the USA, the UK, the EU, India and Saudi Arabia. The year ahead will also see international cooperation efforts, such as the EU-US Data Privacy Framework, seeking to ease some of the current challenges in international data transfer.
- In the US, we will see further scrutiny of bank-fintech partnerships from the banking agencies, particularly for "rent-a-charter" arrangements where a non-bank partners with a sponsor bank to offer financial services. Regulators have cited such arrangements as raising safety and soundness concerns and have criticised banks for deficient monitoring of fintech partners, including in relation to AML requirements. The CFPB has signalled that it may exercise its authority under the Dodd-Frank Act to examine non-bank financial companies that pose risks to consumers, which would include fintechs and providers of embedded finance offerings.

For more, read our recent briefings UK regulatory developments in the buy-now-pay-later space and Digital regulation and strategy.

7

Antitrust authorities scrutinising payments sector

In 2022, antitrust authorities around the world closely scrutinised payments firms, looking at both "Big Tech" entrants and more traditional forms of payment. In the EU, the European Commission issued Apple with a Statement of Objections regarding Apple Pay, in particular looking at Apple limiting access for third-party developers to technology used for contactless payments. As cash usage has declined, competition authorities have assessed mergers, co-operation agreements and fee arrangements relating to cash and ATMs in the Netherlands, Spain, Italy, Australia and other jurisdictions.

What's next?

- In 2023, we will see the impact on the payments sector of new antitrust legislation in several jurisdictions. The EU's Digital Markets Act came into force towards the end of 2022, including rules on in-app payment mechanisms and access to near-field communication technology used for payments. In the UK, new legislation is expected to be passed and in force by the end of 2023, giving new powers to the Competition and Markets Authority's Digital Markets Unit. In the US, new antitrust legislation has also been proposed, but the future of this is less certain.
- Fintech mergers and acquisitions will continue to be closely scrutinised by competition authorities. This follows high-profile deals being abandoned due to concerns raised by competition authorities, such as Visa's acquisition of Plaid and the proposed merger of Crowdcube and Seedrs.
- In the UK, we will see the UK Payment Systems Regulator's interim findings from its market reviews into card scheme fees and cross-border interchange fees. The Financial Conduct Authority will also publish its feedback statement following its Discussion Paper on competition impacts of "Big Tech" entry into retail financial services, including payments.

For more information, read our Financial Services Antitrust Bulletin and our articles on Competition Policy for Fintech M&A, Central Bank Digital Currencies and Competition Laws and FCA explores competition impacts of "Big Tech" entering Retail Financial Services.

CONTACTS

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

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

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

Zayed Al Jamil
Partner
London
T: +44 207006 3005
E: zayed.aljamil@cliffordchance.com

Philip Angeloff
Counsel
Washington, D.C.
T: +1 202 912 5111
E: philip.angeloff@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

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

Andre Da Roza
Consultant
Hong Kong
T: +852 2825 8000
E: andre.daroza@cliffordchance.com

Steven Gatti
Partner
Washington, D.C.
T: +1 202 912 5095
E: steven.gatti@cliffordchance.com

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

Jack Hardman
Partner
Dubai
T: +971 4503 2712
E: jack.hardman@cliffordchance.com

Young Kim
Counsel
New York
T: +1 212 878 4902
E: young.kim@cliffordchance.com

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

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

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

Daniel Schwarz
Senior Associate
London
T: +44 207006 8924
E: daniel.schwarz@cliffordchance.com

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

CLIFFORD

CHANCE

www.cliffordchance.com

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

2303-005093