CLIFFORD
CHANCE

FINTECH: INTERNATIONAL TRENDS AND REGULATORY RESPONSES

— THOUGHT LEADERSHIP

OCTOBER 2019

FINTECH: INTERNATIONAL TRENDS AND REGULATORY RESPONSES

Technological innovation, the rise of fintech firms and the entry of big tech companies, such as Facebook and Amazon into financial services, are all driving the shift towards a digital economy. As new financial products and services emerge, policy makers and regulators have to keep up with the pace of change and address new risks. At an international level, whilst they recognise the need for a coordinated response to these developments, so far, this has been largely limited to addressing money laundering and terrorist financing risks.

Current trends and developments

Cryptoassets and Distributed Ledger Technology

Cryptoassets are continuing to evolve as established financial players and big tech companies enter the market. Financial players and big tech companies are increasingly entering the market. For example, in February 2019, JP Morgan launched its own digital coin (JPM Coin), designed to make instant payments using distributed ledger technology (DLT) and in June 2019, Facebook announced plans to launch a new global digital currency called Libra that would enable users to transfer value on a peer-to-peer basis via digital wallets within Facebook applications. For an overview of the current global regulatory response to cryptoassets see the box on page 4.

Crowdfunding and P2P lending

Crowdfunding and peer-to-peer (P2P) lending has experienced rapid growth in recent years. This is one of the more mature fintech sub-sectors and some jurisdictions have already implemented specific regulatory frameworks for crowdfunding and P2P lending.

In the EU, the proposed Crowdfunding Regulation is expected to introduce a harmonised licensing and passporting regime for lending-based and investment-based P2P platforms across the EU, possibly from mid-2020. However, more generally, the approach to regulation of these activities differs across jurisdictions.

Open Banking, APIs and secure data sharing

Payment services have seen significant change in recent years, with the advent of internet and mobile banking and the growth of fintechs offering innovative payment services and solutions. At the same time, there has been a focus on the role of competition in payment services, with open banking initiatives in the UK and EU requiring payment account providers to open up access to customer's accounts in order to allow these new players to provide their services.

The UK Open Banking initiative requires payment account providers to provide this access via Application Programming Interfaces (APIs), with various other jurisdictions requiring or encouraging use of APIs for similar data sharing purposes. The UK government's Smart Data consultation, published in June 2019, also proposes extending Open Banking-style secure data sharing to other financial services.

Cloud computing

Cloud computing – where software, hardware and maintenance are offered as a service by the software vendor and delivered to the customer over the internet – is growing rapidly, with more than half of all business computing now taking place in the cloud. We have seen shifts in both financial institutions' and

regulators' attitudes towards cloud computing over the past couple of years, as it has become increasingly common. Nevertheless, cloud computing continues to pose a number of regulatory challenges for financial services firms, including compliance with outsourcing and data protection requirements. The vast majority of cloud services are also provided by three major vendors, leading to regulatory concerns around concentration and lock-in risks.

AI and machine learning

Artificial intelligence (AI) and machine learning is playing an increasingly prominent role in financial services, and is used in areas as diverse as robo-advice, detecting fraud and market abuse, algorithmic trading, devising fund investment strategies and analysing customer behaviour for marketing purposes.

Financial regulators recognise the benefits of AI and machine learning for issues such as fraud monitoring, but are also alive to new risks. Ensuring effective human oversight and the 'explainability' of decisions made using AI will be crucial for firms as they seek to exploit this new technology. For example, using machine learning and AI does not absolve firms from assessing the suitability of products for their clients. The current focus in many jurisdictions on corporate culture and the responsibilities of senior management may also drive the need for boards to focus on oversight and ethical questions regarding their use of this technology.

Regtech

Regulators are also turning to technology to help them monitor and supervise the industry effectively. Regulators have more data available than ever before, in part due to recent regulatory changes, such as the enhanced transaction reporting requirements under MiFID2 in the EU. However, this is only useful to regulators if they can effectively analyse and interpret the data.

Advanced analytics and AI may also help regulators identify the most efficient way to use their scarce resources, or even allow them to identify and address potential issues before they arise.

Global regulatory responses

Global standard setting

To date, there has been limited global standard setting for cryptoassets and other fintech-related developments. The Financial Action Task Force (FATF) has issued international recommendations on extending AML and CTF measures to cryptoasset exchanges and wallet providers.

However, other international standard setting bodies have not yet issued recommendations or principles for regulation of cryptoassets, on the basis that they do not currently pose a material risk to global financial stability. The Financial Stability Board (FSB) continues to monitor fintech developments, including the competitive impact that big tech firms may have on financial markets and reliance by financial institutions on third-party data service providers (e.g. cloud service providers).

Regulatory collaboration: A global sandbox?

The Global Financial Innovation Network (GFIN) is an international network or financial regulators and related organisations, which launched in January 2019. It will provide firms with a sandbox environment in which to trial innovative products across multiple jurisdictions. It also seeks to create a framework for cooperation between financial services regulators on innovation-related topics.

However, not all regulators support a sandbox approach, (for example, the German BaFIN has indicated it does not), with some expressing concerns about the ethical implications of offering preferential regulatory treatment or waiving rules for a small number of hand-picked start-ups.

Focus on cryptoassets

The market for cryptoassets and tokens issued in initial coin offerings (ICOs) has grown significantly over the past few years. This is a global phenomenon and the decentralised nature of (public) blockchain networks raises particular legal and regulatory challenges, such as the application of conflict of laws rules to assets held on the blockchain.

Market participants have faced uncertainty as to whether certain types of cryptoassets fall within the scope of existing regulations or how these regulations ought to apply in practice. Recent enforcement actions, notably in the US, have also illustrated the broad extra-territorial application of some national regulatory regimes. Therefore, market participants will often need to navigate multiple regulatory regimes in relation to cryptoasset activities.

At an international level, FATF has recommended that cryptoexchanges and wallet providers should be required to implement AML and CTF controls and should be licensed or registered and supervised or monitored by national authorities. The FSB and other international bodies also continue to monitor developments in cryptoasset markets. However, they have not proposed broader global standards for regulation of cryptoassets on the basis that they do not (yet) pose risks to financial stability. Nevertheless, recent developments such as Facebook's Libra announcement could change this assessment and catalyse the development of global standards for the regulation of cryptoassets.

At a national level, various regulators have published their assessments of when cryptoassets will fall within existing financial services regulatory frameworks. In some cases, they have also identified gaps in existing frameworks, potentially paving the way for future regulatory change. Some jurisdictions, such as France, have gone a step further and have proposed new laws to regulate cryptoassets.

Regulators and lawmakers around the globe are grappling with many of the same issues and questions about how to apply existing laws and regulations to cryptoassets. These include:

- Which types of cryptoassets fall within the scope of existing financial regulatory frameworks?
- What is the territorial reach of those existing frameworks and the extent of regulators' jurisdiction?
- How do existing rules on custody and settlement (including settlement finality rules) apply to holding and transferring cryptoassets via a DLT network?
- Which law(s) will apply to proprietary aspects of holding and transferring cryptoassets that are native to the blockchain (i.e. where there is no single account or record of legal title to the asset located in a particular jurisdiction)?

Due to the cross-border nature of cryptoasset activity, there is potential for conflict if policymakers in different jurisdictions arrive at different answers to these questions. In turn, this could lead to increased regulatory and legal risk for firms as they seek to comply with multiple different regimes or where it is unclear which set of rules would apply. It could also allow firms to engage in regulatory arbitrage, exploiting the differences between regimes. However, there are calls both from regulators and from industry to foster international cooperation and supervisory convergence in this area.

Given the decentralised, international nature of cryptoassets and related activities, we expect to see international collaboration around enforcement activity. Questions of jurisdiction and applicable law will feature prominently as courts struggle to apply existing precedent to public and private blockchains and their international participants.

Will regulation act as brake on the globalisation of fintech?

Regulation can act as a brake on globalisation and lead to market fragmentation, particularly where duplicative or potentially conflicting rules have extraterritorial impacts. In particular, overarching data protection regulations and the expansion of the scope of existing anti money laundering (AML) regimes to capture cryptocurrency exchanges and wallet providers may hinder cross-border activity.

AML

In October 2018, FATF recommended that crypto exchanges and wallet providers should be required to implement AML and CTF controls and should be licensed or registered and supervised or monitored by national authorities. The EU had already committed to bringing many crypto changes and wallet providers within the scope of AML and CTF requirements through the fifth anti-money laundering directive (AMLD5), which Member States are due to implement by 10 January 2020.

When these rules come into effect they will require in-scope cryptocurrency exchanges and wallet providers to have in place policies and procedures to detect, prevent and report money laundering and terrorist financing, to the extent not already required to do so under national law. These entities will also become subject to registration or licensing requirements (if this was not already the case under national law) and persons that own or hold a management function in these entities will be subject to fitness and propriety requirements.

However, AMLD5 does not apply to crypto-to-crypto exchanges, which are within scope of the FATF recommendation. The UK government has therefore indicated that it intends to gold-plate AMLD5 by extending the same rules to crypto-to-crypto exchanges. Again, this is an example of how internationally agreed standards may be implemented in different ways.

Data protection

The ability to share and transfer data across borders is a significant issue for fintech firms, given the cross-border nature of much fintech activity and increasing reliance on third-party data service providers. However, the EU GDPR and similar regimes in jurisdictions such as China have introduced greater protections for personal data, bringing with them new challenges and barriers for data flows across borders. The extraterritorial application of some of these regimes may also pose particular challenges for firms with global business operations.

In its February 2019 Report on fintech and market structure in financial services, the FSB noted that restrictive data protection regimes may also hinder regulators' ability to supervise foreign firms operating in their jurisdiction, but that this issue "would be mitigated if data protection frameworks offer a mechanism that ensures that third-country authorities have access to the personal data needed to conduct their supervisory and enforcement activities."

NOTES

CONTACTS

Peter Chapman
Partner
London
T: +44 20 7006 1896
E: peter.chapman@cliffordchance.com

Laura Douglas
Senior Associate
Knowledge Lawyer
London
T: +44 20 7006 1113
E: laura.douglas@cliffordchance.com

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

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

Paul Landless
Partner
Singapore
T: +65 6410 2235
E: paul.landless@cliffordchance.com

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

Jesse Overall
Associate
New York
T: +1 212 878 8289
E: jesse.overall@cliffordchance.com

Monica Sah
Partner
London
T: +44 20 7006 1103
E: monica.sah@cliffordchance.com

Jurgen van der Meer
Partner
Amsterdam
T: +31 20 711 9340
E: jurgen.vandermeer@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

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

1910-000149