



Fintech Global

Year in review 2019 | Year to come 2020

GLOBAL PREDICTIONS 2020

01

Regulatory response to stablecoins and other new payment models

05

India and China to continue fight for top spot as Asia's hub for online payment services

02

Improvements to legacy payment systems – tackling inefficiencies in cross-border payments

06

More guidance for firms around the ethical deployment of AI

03

Increasing use of DLT and smart contracts in the capital markets

07

Scrutiny of the financial sector's resilience to cyber risk including potential fines for previous IT failures

04

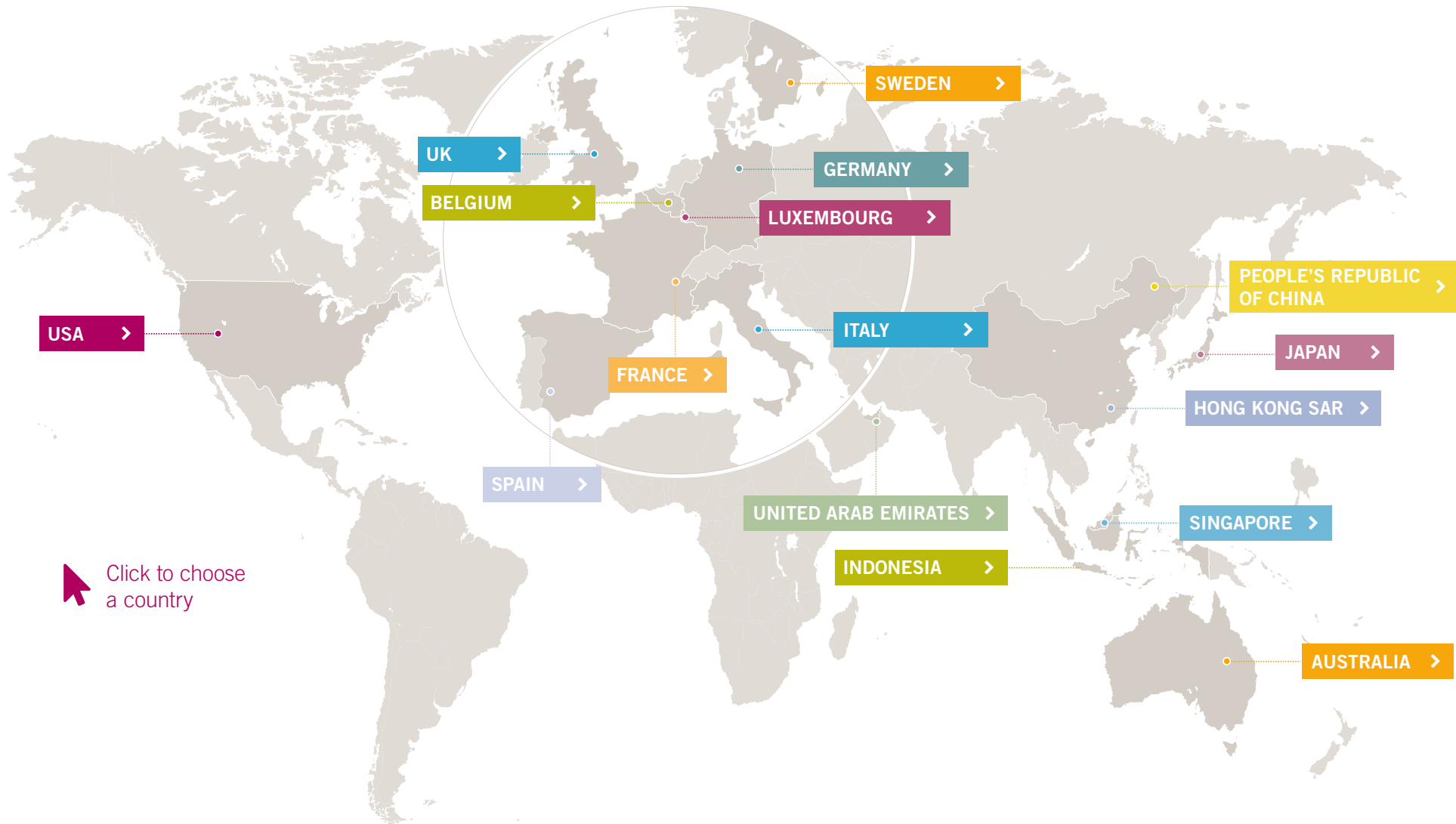
Greater scrutiny of Big Tech in finance

08

Increasing industry and policymaker collaboration on tackling cyber crime in financial services



GLOBAL FINTECH



AUSTRALIA

Year in Review 2019

Year to come 2020

Open Banking

Initially expected to start on 1 July 2019, the commencement of the open banking scheme has been deferred to 1 February 2020. In the interim, the Australian Government is conducting a pilot scheme involving Australia's major banks, consumers and other fintech industry participants. The new regime will afford individual and business consumers the right to access specified categories of data about or related to them that is held by designated banks, and direct the transfer of such data to accredited third parties.

The rise of neobanks

Neobanks are exhibiting an increasing interest in the Australian market. The past year has seen the Australian Prudential Regulatory Authority (APRA) issue licences to four neobanks (Xinja, Volt, 86400 and Judo), with other international players considering forays in Australia. The provision of full, unrestricted banking licences to these challenger banks demonstrates a clear regulatory shift, which has the potential to have significant impacts on the Australian banking landscape.

ASX increasingly attractive for tech

2019 saw the Australian Securities Exchange (ASX) become an increasingly attractive place for foreign fintechs to raise capital. While the ASX has not traditionally been a focus for technology stocks, more foreign fintechs looked to Australia when raising capital this year than ever before.

Increased regulatory focus on privacy

Throughout 2019, Australia's information and privacy regulator, the Office of the Australian Information Commission (OAIC), has significantly expanded its enforcement activities. This year's Australian Government budget saw the OAIC's funding increase AUD25.1 million over three years for the OAIC to "facilitate timely responses to privacy complaints and support strengthened enforcement actions in relation to social media and other online platforms that breach privacy regulations". Simultaneously, we have seen the OAIC's regulatory approach shift from conciliatory to one that makes greater use of its enforcement powers. In June 2019, the OAIC accepted an

enforceable undertaking from a major Australian bank in response to privacy breaches dating back several years, which included far more detailed and far-reaching obligations than previously seen. This reflects the increasingly pro-enforcement stance taken by the OAIC.

Regtech

Australian regulators are investigating the potential of "regtech" to transform the compliance landscape, particularly with regard to financial service providers. The Australian Securities and Investments Commission (ASIC) is actively seeking engagement from regtech providers and hosted several industry events to promote awareness of regtech options and knowledge sharing. ASIC hopes that increased adoption of regtech will help detect misconduct, improve regulation and promote a culture of compliance in Australia's financial services industry.

AML/KYC considerations in the fintech market

The complex or novel business models of many fintechs has historically presented a challenge in respect of the sector's compliance with anti-money laundering and counter-terrorism financing (AML/CTF) legislation. However, as the fintech market expands, Australia's financial intelligence regulator, AUSTRAC, is taking an increasingly active approach when it comes to non-traditional financial services. The message seems to be that Australian fintechs should carefully consider what designated services they are providing, and what AML/CTF processes (including the extent of 'know your customer' identity verification) are required for their products from day one. Entities cannot treat AML/CTF controls as a culture of compliance as an afterthought.

Contributed by Allens





AUSTRALIA

Year in Review 2019

Year to come 2020

Consumer Data Right to expand

In 2019, we saw the Consumer Data Right (CDR) commence in the form of Open Banking and receive legislative backing in the form of the Treasury Laws Amendment (Consumer Data Right) Act 2019. In 2020, we expect to see greater moves towards expanding the CDR regime. This will include not only an expansion of the Open Banking regime to new information and entities, but also an expansion to other industries, including energy and telecommunications.

Stricter data regulations

The Australian Government has indicated its intention to bring Australian privacy laws and associated penalties in line with “community expectations”. This could see radically increased financial penalties and new powers for the OAIC, in light of a growing consensus that Australia’s privacy legislation has fallen behind global developments, including the EU’s General Data Protection Regulation (GDPR).

Proposed reforms include increasing the maximum penalties for serious breaches of the Privacy Act from AUD2.1 million to the larger of AUD10 million, three times the value of any benefit or detriment avoided, or 10% of annual domestic turnover, as well as introducing new powers for the OAIC to issue infringement notices for failure to co-operate with efforts to resolve minor breaches. Increased penalties were one of the many Australian Competition and Consumer Commission’s (ACCC) recommendations in the Digital Platforms Inquiry final report.

The Federal Government is currently considering a number of the ACCC’s other recommendations, which include expanding the definition of personal information to capture all technical data such as “IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual”, as well as introducing a right of erasure, stronger data collection notification requirements, stronger consent requirements and a tort for serious invasions of privacy.

Blockchain and digital currencies: more use and more regulation

Globally, 2020 is expected to be the year of the digital currency. Following the launch of Australia’s national blockchain strategy and China passing cryptocurrency legislation to facilitate a national digital currency (see People’s Republic of China Year to Come 2020), we expect that digital currencies and blockchain technology in financial services will be a key focus both globally and in Australia. This trend has already been seen in Australia with the Big Four Banks and ASX beginning to invest more heavily in blockchain technologies. This growth is also expected to attract the attention of Australian lawmakers.

ASX replacing CHES with distributed ledger technology

The ASX is on track to replace its Clearing House Electronic Subregister System (CHES) with a new system based on Digital Asset’s distributed ledger technology (DLT). The ASX has been an early mover in blockchain technology, deciding in 2015 to replace its core clearing, settlement and asset registration system, CHES, with a DLT-enabled system. Over the past year, the ASX has engaged in significant stakeholder consultation and on 15 November 2019, the ASX released a consultation paper on the first of three tranches of operating rule amendments required to facilitate the implementation of the new system that will replace CHES in April 2021.

Contributed by Allens



BELGIUM

Year in Review 2019

Year to come 2020

Belgium remains strong in fintech – in all different shapes and sizes

Innovation in financial services

Along with its thriving fintech start-up scene, we have seen the major Belgian financial institutions and financial market infrastructures investing heavily in innovation, with a clear interest in the various and often wide-ranging applications of blockchain technology. Digitalisation projects are also high on the agenda of traditional players who are often assisted by software providers and software vendors to realise their objectives.

The payments revolution and beyond

Belgian start-ups and challenger banks aim to use the new possibilities offered by the EU's second Payment Services Directive (PSD2) to revolutionise payments. These include Cake, a soon-to-launch payment initiation app, and Payconiq, a popular banking app now supporting POM QR codes, which can be found on an increasing number of Belgian invoices. We have seen payment apps gain strongly in popularity in Belgium this last year. Innovation also goes beyond the world of payments: the Belgian scale-up Silverfin is re-inventing the principles of cloud-accounting and Cashforce leverages artificial intelligence and machine learning to help companies in predicting their future cash flow needs.

Strong customer authentication in payments

Following a European Banking Authority (EBA) opinion on the elements of strong customer authentication (SCA) under PSD2, the National Bank of Belgium (NBB) announced that it will postpone enforcement to allow co-ordination among industry stakeholders. Payment service providers (PSPs) not complying with the SCA requirements after 14 September 2019 benefit from this regulatory forbearance, provided that they follow a migration plan which is yet to be published by the NBB. The EBA has set the final deadline for full compliance to 31 December 2020.

SWIFT ISO 20022 – hybrid application solutions

SWIFT recently launched a Proof-of-Concept of an e-Voting application to improve shareholder voice and corporate decision-making. The Belgian co-operative company intends to demonstrate the interoperability of its existing infrastructure and interface with DLT-applications through the implementation of the ISO 20022 data standards, which were inspired and co-developed by SWIFT. ISO 20022 allows for data-rich communication on the SWIFT network and serves as a common foundation that may standardise application program interfaces (APIs) going forward.

Cyber security – Belgian coalition against cyber crime

During its annual meeting in September, in which Linklaters Brussels also participated, the Belgian Cyber Security Coalition (a partnership between the public authorities, the academic world and the private sector in the fight against cyber crime) suggested that, based on the available figures, Belgium is proportionally the most targeted country in respect of cyber attacks directed both at companies and individuals. As a result, cyber security is particularly high on the list of priorities for companies active in the Belgian fintech space. Among others, innovative campaigns have been launched towards the public to prevent phishing attacks.



BELGIUM

Year in Review 2019

Year to come 2020

Regulators – increased awareness for scale-ups

As fintech companies gradually transition from start-ups into mid-market providers of financial services, we expect an increasing degree of regulatory scrutiny in respect of the robustness of their organisations, especially as regards their compliance and anti-money laundering and counter-terrorism financing policies and procedures. Scaling companies should invest in maturing internal processes to meet the increasing regulator expectation as they continue to grow.

APIs – further development and standardisation

PSD2 fuels the creation of open banking through APIs, allowing third-party providers (TPPs) to provide services which integrate with the payment accounts held by the institutions. While nearly all banks have established sandbox environments, the integration of third-party companies with bank APIs requires some further progress. We expect increased regulatory attention on APIs in the year to come: to ensure interoperability and compliance by established payment institutions with PSD2; the Regulatory Technical Standards on strong customer authentication and common and secure communication; and publications of the EBA working group on APIs which we expect to provide policy recommendations.

Brexit – Belgian licence to ensure continuity

A specific application procedure has been established for authorised institutions that seek to relocate their business to Belgium in the context of Brexit. This procedure allows existing institutions to start with their original foreign application file and modify that document to meet the requirements of Belgium specific legislation, such as AML. A number of UK fintech companies have decided to set up a Belgian entity to continue providing services in the EU market after Brexit, regardless of the final exit deal. For instance, PrePay Solutions has obtained an e-money licence from the NBB while TransferWise and WorldRemit obtained a licence as a payment institution, which they can passport throughout the EU. Depending on the outcome of Brexit negotiations, this trend could continue in 2020.

ePrivacy – additional data rules

During 2020 the EU could potentially adopt an ePrivacy Regulation to supplement the GDPR. The draft Regulation contains specific rules on the use of electronic communications, cookies and electronic marketing. If adopted, it would provide a uniform framework directly applicable in the EU member states. This would be of particular relevance to fintech companies, which often offer their services online, use online tracking technologies and communicate electronically with existing and prospective customers. However, the fate of the Regulation remains uncertain as the draft has thus far failed to get the approval of all member states.



FRANCE

Year in Review 2019

Year to come 2020

Progressive new regulatory frameworks for ICOs and digital asset service providers

In May, France enacted two new regulatory regimes intended to provide legal certainty, support and greater access to private capital for the crypto sector. The first is an optional visa regime to enable issuers of utility tokens that meet certain requirements (including AML/CFT requirements) to differentiate their offering with a stamp of approval from the French financial regulator (the AMF). The second regulates digital asset service providers. It sets out certain mandatory minimum standards (including around governance and AML/CFT) for digital asset custodians and digital asset-to-fiat exchange platforms, and also allows these, and a broad range of other, digital asset service providers to apply for an optional licence administered by the AMF, provided that they meet certain core rules (including capital, internal control, cyber security, and AML/CFT requirements) as well as rules specific to the types of services offered. Certain implementing measures were enacted in November. ([Read more...](#))

Right to a bank account for utility token issuers and digital asset service providers

The new French regulatory regimes (outlined above) provide the right for utility token issuers which have obtained the AMF approval for their ICOs and digital asset service providers which are either registered or licensed by the AMF to have access to deposit and payment accounts with credit institutions on an objective, non-discriminatory and proportionate basis. Measures to implement this right were enacted in November 2019.

Implementation of laws allowing DLT for unlisted securities and minibons

Provisions that allow for the representation and transfer of unlisted securities and the issuance and transfer of minibons to be recorded using distributed ledger technology (DLT) ([Read more...](#)) were implemented just before the start of the 2019. “Unlisted securities” includes equity and debt securities that are not traded on a trading venue, negotiable debt securities and shares or units in a collective

investment undertaking. “Minibons” are not financial instruments, but a particular type of debt instrument offered to the public in the context of crowdfunding transactions.

The implementing provisions impose certain requirements around the design of the DLT and clarified the process for pledging securities recorded on a distributed ledger.

Strong customer authentication under PSD2

In June, the European Banking Authority allowed national regulators to give payment service providers additional time to meet “strong customer authentication” security measures under the EU’s revised Payment Services Directive (PSD2), provided that they have agreed a plan for meeting these new rules with their national regulators. ([Read more...](#))

As a result, in September, the French authorities (acting through the Observatory for the Security of Payment Means – a body attached to the Banque de France) announced that they will postpone enforcement provided that the industry complies with a two-part migration plan. Under the migration plan: (i) card issuers will gradually replace single-use SMS verification procedures with more advanced payment protection for online transactions (and this is expected to reach at least 75% of consumers by December 2020); and (ii) by March 2021, all payment service providers in the payment chain should have migrated to version 2 of the 3D-Secure infrastructure for card payments, to comply with the operational requirements under PSD2.

Data protection – sanctions for Google under GDPR

In January, the French data protection regulator (the CNIL) used its increased powers under the EU’s General Data Protection Regulation (GDPR) to issue the first significant financial penalty under the regime, in response to various group claims against Google. Under its decision, the CNIL sanctioned Google with a EUR50 million fine for a lack of clarity and accessibility of information provided to users of its services, as well as a lack of valid consent for processing carried out for targeted advertisement purposes. The sanction may be of relevance to fintechs which utilise personal data. ([Read more...](#))



FRANCE

Year in Review 2019

Year to come 2020

Further implementation and guidance for digital asset service providers

In 2020, the AMF will enact further regulations and guidance to fully implement the new regulatory regime for digital asset service providers. In particular, they will detail the requirements and procedures that the digital asset service providers must comply with to be registered and/or licensed by the AMF.

Digital currencies – industry and public sector response

France has emphasised its willingness to tackle the challenges raised by Libra and other so-called stablecoin projects. In 2020, we may see further regulatory action in this area, with the FSB reporting to the G20 in April on the adequacy of existing regulatory approaches to global stablecoins and possible multilateral approaches. ([Read more...](#))

The Banque de France is also considering issuing a wholesale central bank digital currency, which would be available to financial intermediaries only.

Capitalising on the revenue-generating opportunities of PSD2

Whilst many banks will still be working to meet their compliance obligations under PSD2 (e.g. strong customer authentication, APIs, open-banking, etc), we are likely to see more focus next year on the revenue-generating opportunities that this legal regime allows for. Banks and third parties alike will be exploring how to capitalise on the regulatory framework of PSD2 in order to serve real consumer needs. ([Read more...](#))

Regulatory scrutiny on the use of AI and cloud computing for the provision of financial services

In 2020, the Banque de France, the French banking regulator (the ACPR) and the AMF will continue to regularly conduct, through their Fintech-Innovation Units, analysis on the use of AI and cloud computing for the provision of financial services to better assess the impact of these new technologies on the regulation and supervision of financial services, such as investment advice and insurance services.

Data protection – new ePrivacy Regulation

During 2020 the EU could potentially adopt an ePrivacy Regulation to supplement the GDPR. The draft Regulation contains specific rules on the use of electronic communications, cookies and electronic marketing. If adopted, it would provide a uniform framework directly applicable in the EU member states. This would be of particular relevance to fintech companies, which often offer their services online, use online tracking technologies and communicate electronically with existing and prospective customers. However, the fate of the Regulation remains uncertain as the draft has thus far failed to get the approval of all member states.

More action from the competition authority

In 2020, we could see the French Competition Authority (FCA) taking more enforcement action in the fintech sector, for example around the use of pricing algorithms. This follows a number of reports from the FCA, the European Commission and other G7 competition authorities on competition issues raised by the digital economy.

GERMANY

Year in Review 2019

State of fintech & DLT projects

It has been a busy year for fintechs in Germany. We have seen a first wave of consolidation and mergers while at the same time challenger banks, in particular, have risen to prominence and have accelerated their growth. While Frankfurt, Berlin, Hamburg and Munich are battling for the crown to be THE German fintech capital, each of these cities is slowly emerging with its own focus but, admittedly, Berlin is going very strong. For DLT, the German scene is thriving. We have seen successful live DLT projects for many aspects of capital markets transactions with more and more very successful technology enablers. Collaboration has been found to be key for many projects and are pushing DLT to be taken more seriously.

The German government introduces its Blockchain Strategy

Following a consultation in March 2019, the German government has adopted its national blockchain strategy comprising of 44 measures which are intended to promote blockchain technology in Germany. While many aspects in the strategy are still quite abstract, a focus point of several concrete legislative measures relate to DLT applications in finance (for more information, see year to come).

Besides finance, the strategy focuses on the digitalisation of the energy revolution. The measures adopted include various research initiatives on applications in the industry and the introduction of a smart contract register for the energy industry. One objective is to “mature innovation” by supporting pilot projects and real laboratories. **(Read more...)**

Payments

The EU's second Payment Services Directive (PSD2) was implemented in German national law, first phase in 2018, second in 2019. With the second phase in force, PSD2 induces the obligation to execute what is known as “strong customer authentication”. However, due to difficulties in the industry to comply with these measures, BaFin (and the EU regulators) have postponed the applicability of certain requirements in connection therewith.

From a fintech perspective, we are still seeing payments as one of the fastest growing areas for not only fintech but also challenger bank offerings. One of the key drivers is, in our view, the disintermediation of the value chain in finance, which allows (and requires) that payment services move away from finance, becoming increasingly integrated into other, often technology heavy products such as mobiles or cars.

Focus of BaFin on digitalisation

In 2019, the Federal Financial Supervisory Authority (BaFin) further engaged in discussions around digitalisation topics and named digitalisation as one of its focus areas for the year. Amongst others, BaFin published guidance on prospectus and licence requirements in connection with the issuance of crypto tokens under the current law.

BaFin is keen on getting a better overview on the issues connected with digitalisation and the topics which concern market participants. Thus, BaFin is intensifying its dialogue with market participants and has taken up to regularly organising industry conferences such as the BaFin Tech.

Also, BaFin focuses on enforcing anti-money laundering and has thus been paying increasing attention to challenger banks and fintechs in this area.



GERMANY

Year in Review 2019

Year to come 2020

Regulation of AI in financial services

In the financial sector, innovation and efficiency are increasingly driven by big data and artificial intelligence (together BDAI). BaFin has explored the risks and opportunities connected with these innovations in depth. It has conducted a comprehensive consultation together with the Fraunhofer Institute and the Boston Consulting Group, and shared the results in its detailed BDAI report. Notably, first indications regarding proper algo-governance structures are discussed as well as raising the question if tech-companies ought to be regulated if they provide systemically important financial market infrastructure.

Cyber security

Every year, an increasing number of targeted cyberattacks are perpetrated on the IT systems of German commercial enterprises of which around 10% are successful. Against the background of the damages and fines foreseen by GDPR, cyber security has received ever growing attention. For example, if payment information or other personal customer data is stolen due to a cyber attack, the companies subject to the attack could be subject to material claims for damages under private law pursuant to Art. 82 DSGVO – as well as administrative fines of up to EUR20 million.

Furthermore (or because of this), there is an increasing interest in cyber security insurance products in the market.

Data privacy and AI

The German Data Protection Supervisory Authorities have determined seven data protection requirements that artificial intelligence must comply with. Those requirements are stipulated in the so-called “Hambach Declaration on Artificial Intelligence (AI)” (“Hambacher Erklärung zur Künstlichen Intelligenz”) as follows: (1) AI must not turn human beings into objects, (2) AI may only be used for constitutionally legitimate purposes and may not abrogate the requirement of purpose limitation, (3) AI must be transparent, comprehensible and explainable, (4) AI must avoid discrimination, (5) the principle of data minimisation applies, (6) AI needs responsibility and (7) AI requires technical and organisational standards.

Algorithm regulation

The German Data Ethics Commission has published proposals for risk-based regulation of algorithms. As the regulatory focus on algorithms has been increasing, these proposals are interesting and provide one of the most structured approaches to date. It suggests risk-based tiering of regulation and that these proposals should be implemented as a new directly effective EU Regulation on Algorithmic Standards. ([Read more...](#))

Algorithms and antitrust

The debate surrounding regulation of algorithms is accompanied by a joint publication by the German and French competition authorities regarding competition issues associated with algorithms, considering the ability of the current framework to deal with issues such as collusion through third-party algorithms, increased transparency from algorithms and self-learning algorithms. ([Read more...](#))





GERMANY

Year in Review 2020

Maturing of fintechs & DLT

Fintech (and emerging technologies) will continue to be one of the hottest topics in finance. However, the availability of later-stage financing to enable true scaling remains rather scarce in Germany. We predict that the fintech exuberance of the last years will start to fade away a bit, shifting to more maturity in the market. Reconciliation will pick up speed, but there remains plenty of room for new fintechs as long as they are focusing on true innovation and added value. Overall, the market is seeing a hint of a possibly needed sobering up with an emerging focus not on buzzwords such as “innovation” but on real value. Also, players from other industries such as telecoms, Big Tech and energy will increasingly venture into finance, combining it with their specific tech.

Payments

The current trend of the integration of payment services into different kinds of products and services will continue, further fostering growth in the payment sector. This will also continue to be a promising area for providers of white label banking services.

Upcoming regulation in connection with digital assets

On a legislative and policy level, (EU as well as on national), regulators and governments are starting more and more to enhance (regulatory) frameworks for the innovative business models of fintechs and, more importantly, enabling the full potential of emerging technologies such as blockchain and AI. However, this might still take some time.

Anti-money laundering – implementing AMLD5

The draft law to implement the EU's fifth Anti-money laundering directive (AMLD5) into German law will enter into force early 2020, introducing a definition for crypto-values for the first time. There is no equivalent on a European level yet as AMLD5 only defines cryptocurrencies. Furthermore, the draft law also introduces a new licence requirement for “the custody, management and safekeeping of crypto-values or private cryptographic keys used to hold, store and transmit crypto-values for others” (so-called crypto custody business). The draft suggestion of such licence being a standalone licence (meaning that such licence can only be granted if no other financial services or banking business is offered) was removed again during the legislative process. In any case, this law will make Germany a frontrunner in regulating DLT assets. Even though it has to be classified as gold plating in comparison to the amendments introduced by EU law, the EU has already stated that it will also introduce EU-wide crypto asset regulation. ([Read more...](#))

Upcoming regulation in connection with the Blockchain Strategy

The German Blockchain Strategy, introduced in 2019 by the German Federal Government, announced several draft laws for 2020. These will, amongst other things, tackle the introduction of electronic bonds (getting rid of the physical paper form requirement under the current regime) and provide a regulatory framework for the public offer of certain crypto tokens. As a next step, the digitisation of equity products and investment fund units is also being considered. ([Read more...](#))



GERMANY

Year in Review 2019

Year to come 2020

DLT infrastructure in finance

We expect to see more pilots of DLT use cases in finance in 2020. These will be ever-increasing in size and relevance due to the reach of the sponsors and number of participants. Some of the bigger projects will be hard to classify “only” as pilots. Also, some projects currently on hold due to regulatory uncertainty (see draft AMLD5 implementation) will be built out. Overall, DLT will start to make its way as a serious infrastructure alternative in finance.

However, we will see continuous discussions together with political as well as regulatory efforts to deal with international blockchain-based currency projects (e.g. Libra). It will be interesting to see whether the first calls for officially supported “fiat money on chain” will lead to government (or central bank) activity. Even though unsure about this, we hope that we will see some of the promising DLT-based digital identity projects to succeed as this is, in our view, one of the missing links in digital finance.

Stablecoins

Germany is still sceptical about so called “stablecoins” but aims to tackle challenges raised by these as well as by cryptocurrencies in general. Concerns especially relate to financial security, investor protection, prevention of money laundering and terrorism financing, data protection and financial and monetary sovereignty. Together with France, Germany urges European central banks to further analyse solutions for a public digital currency.

Data privacy

The Federal Government of Germany will conduct a roundtable discussion on blockchain and data protection issues. One of the roundtable sessions in the first half of 2020 will be dedicated to questions of data protection law regarding blockchain technology. One of the main purposes of such session is to discuss the application of existing guidelines used by data protection authorities to the current blockchain technology. If such existing guidelines are not applicable, suggestions for additional guidelines will likely be discussed.

Cyber security

The so-called “German IT Security Act 2.0” (“IT-Sicherheitsgesetz 2.0”) may enter into force in 2020. It will increase fines for infringements of security obligations to the level known from the General Data Protection Regulation (GDPR) and apply to operators of “critical infrastructure”, such as banks and financial service providers.

Fintech dispute resolution

Arbitration as a dispute resolution mechanism is slowly gaining ground for international fintech and blockchain disputes, whilst the first court decisions (e.g. Gerechtshof, Amsterdam, Case no. 200.234.175/01, 29 January 2019) have stressed the importance of due process to allow for enforcement.



HONG KONG SAR

Year in Review 2019

Year to come 2020

Continued caution on virtual assets

Regulators continue to remain cautious regarding virtual assets and have taken steps which aim to ensure investor protection while recognising the developments in, and importance of, this sector. The Hong Kong Monetary Authority (HKMA) has requested that banks discuss plans to engage in activities relating to crypto-assets with the HKMA and have appropriate risk management systems in place.

The Securities and Futures Commission (SFC) published a set of terms and conditions which are imposed on SFC-licensed fund managers that manage funds which include virtual assets, as a condition of their licence. ([Read more...](#)) The SFC also issued a “reminder” statement about the legal and regulatory requirements applicable to security token offerings and warning investors to be aware of the risks associated with virtual assets generally, including security token offerings and a separate specific warning on virtual asset futures contracts.

The launch of virtual banks and insurers

The HKMA and the Insurance Authority have both been granting licences to “virtual” applicants. A total of eight virtual banking licences have been granted by the HKMA as it pushes forward with its Smart Banking initiative, with the first virtual banks expected to commence operations during 2020. The Insurance Authority granted the first authorisation of a non-life insurer in October 2019, following the first life virtual insurer in December 2018.

Guidelines for financial services advisory platforms

The SFC’s Guidelines on Online Distribution and Advisory Platforms took effect this year. The Guidelines apply to SFC-licensed persons which conduct regulated activities such as order execution, distribution and advisory services via online platforms. The Guidelines set out six core principles for the operation of online platforms, as well as specific requirements on areas including robo-advice and the suitability requirements applicable to transactions via online platforms.

Guidance on ethical use of personal digital data for banks

In response to the continued development of fintech in the banking sector, the HKMA issued a circular encouraging banks to adopt and implement the “Ethical Accountability Framework for Hong Kong, China” previously issued by the Office of the Privacy Commissioner for Personal Data. The Framework provides guidelines on the proper use of personal data in the online environment.

High-level principles for the use of AI

The HKMA has issued guidance in the form of high-level principles on the use of artificial intelligence (AI) applications. The HKMA issued this guidance following the results from a recent HKMA survey which showed that many banks are adopting or planning to adopt AI applications, and the growing use of AI presents some new risk management challenges to banks. The guidance in the form of high-level principles is due to the fact that the HKMA wants to ensure that there is flexibility in the guidance to allow for further development in the field of AI. ([Read more...](#))

Consumer protection in the banking sector

The HKMA rounded out the year by publishing several documents covering consumer protection and guiding principles for banks when using technology in providing services to clients. The HKMA issued a circular for banks setting out guiding principles on consumer protection aspects when using big data analytics and artificial intelligence, which followed hot on the heels of its publication of high-level principles to be considered when designing and adopting artificial intelligence applications. The HKMA also issued a circular to banks on consumer protection requirements when using the open API framework.



HONG KONG SAR

Year in Review 2019

Year to come 2020

Regulation of virtual asset trading platforms

The SFC published a paper in November 2019 which sets out a regulatory framework for virtual asset trading platforms that operate in Hong Kong providing trading, clearing and settlement services for virtual assets. The framework will only apply to platforms which choose to include virtual assets or tokens for trading which would meet the definition of a “security” under the Securities and Futures Ordinance. The SFC has acknowledged that there are some regulatory gaps identified in the paper and therefore further legislative change will be needed in the future to address these issues.

The implementation of this new framework allows the SFC close supervisory interaction with this fast developing area and should assist the SFC in formulating a future regulatory strategy for virtual assets, potentially including virtual assets which currently fall outside the regulatory remit of the SFC.

HKMA development of open API framework

One of the HKMA's Smart Banking initiatives is the development of an Open Application Programming Interface framework. The open API will allow third-party access to systems of banks, i.e. open banking, and the HKMA is following a phased implementation approach. In 2020, the HKMA will publish a set of technical standards for the final two phases, followed by an implementation timetable.

Greater Bay Area data laws

One key emphasis of the Guangdong-Hong Kong-Macao Greater Bay Area initiative, for greater co-operation on the economic development, is to facilitate data flow within the region. However, the difference in the existing data protection regimes between mainland China (which has a national security focus) and Hong Kong (which has a privacy focus) has the potential to pose challenges for businesses in the protection, processing and management of personal data within the Greater Bay Area. Therefore to truly facilitate data flow, discussions and negotiations on creating a mutual data protection framework will be necessary over the coming year.

Use of cloud and other virtual data storage

In November 2019, the SFC issued a circular for licensed corporations clarifying its expectations on their use of cloud and other virtual data storage. All licenced corporations using external electronic data storage providers should be taking steps from the end of 2019 and into 2020 to meet the SFC's requirements in respect of these third-party arrangements and to ensure compliance without delay. ([Read more...](#))

INDONESIA

Year in Review 2019

Year to come 2020

Regulation – Business activities of financing companies

At the end of December 2018, the Indonesia Financial Services Authority (*Otoritas Jasa Keuangan* or ‘OJK’) enacted OJK Regulation No. 35/POJK.05/2018 on the Implementation of Business Activities of Financing Companies (“New OJK Regulation”), which revoked the previous OJK Regulation on the same matter.

The New OJK Regulation can be seen as OJK’s attempt to keep up with the rapid increase of the use of technology by players in the financial industry all over the globe. Under the New OJK Regulation, financing companies are now permitted to utilise information technology for some aspects of their business (i.e. promotion and marketing, customer application submissions and monitoring instalment payments).

However, in order to prevent abuse, OJK also requires financing companies that use information technology to comply with certain requirements, one of which is to have data and disaster recovery centres located in Indonesia. Failure to do so may lead to administrative sanctions by OJK, including the revocation of business licences.

Peer-to-peer lending regulation

Peer-to-peer lending (“P2P”) businesses came under more onerous licensing requirements in February 2019 with the new registration, licensing and change of ownership application checklist for P2P operators per introduced in February 2019.¹ To register and apply for a licence from OJK, lenders must meet strict naming requirements and their shareholders, commissioners and directors must undergo an assessment of their fitness and propriety at a regulatory interview.

The OJK also endorsed standards set by the Indonesian Fintech Association (*Asosiasi Fintech Pendanaan Bersama Indonesia* or “AFPI”) by requiring new P2P companies to be members of AFPI and to have received the AFPI’s recommendation before being eligible to apply for a business licence.

P2P lending sector growth and increased regulatory intervention

The number of P2P accounts more than doubled in 2019. Statistics published by the OJK in September 2019 show that, compared to the end of 2018, the number of P2P borrower accounts has increased by 229.4% and the number of P2P lender accounts has increased by 169.28%. The OJK’s investment watchdog division stated that, among the 2,000 estimated existing P2P operators in Indonesia, only 127 operators are registered or licensed. OJK said that 1,733 illegal P2P operators are doing business in violation of the prevailing fintech regulation. The most commonly found violations are: (i) P2P operators lending their own funds (OJK only allows off-balance sheet P2P lending); and (ii) P2P operators imposing coercive debt-collection methods. In light of this, OJK is actively seeking out and shutting down P2P operators which commit such violations whilst educating the general public on how to avoid these illegal P2P operators.

Regulatory sandbox development

In September, the OJK launched the Electronic Gateway for Digital Finance Information Systems to better facilitate registrations and promote effective supervision of digital financial institutions. The system is part of OJK Infinity – the regulatory sandbox launched in 2018 – which seeks to build the fintech ecosystem to benefit the community and encourage economic growth.

¹ <https://www.ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/-Checklist-Dokumen-Pendaftaran,-Perizinan,-dan-Perubahan-Kepemilikan-Penyelenggara-Fintech-per-Februari-2019.aspx>

INDONESIA

Year in Review 2019

Year to come 2020

Market growth

The year-on-year growth in the number of users of technology for electronic payments is expected to continue as Indonesia's young population continue to embrace e-commerce and further cross-sector collaboration creates innovative digital solutions for Indonesia's largely unbanked population. With the regulatory sandbox operated by OJK and Bank Indonesia, and the continued growth of electronic payment and fintech business players in general, ever more rapid development in technology-based business in Indonesia is foreseeable in the years to come.

Regulatory approach

It remains to be seen whether efforts to reduce consumer harm from illegitimate fintech providers will result in an increased regulatory burden on licensed operators or whether the lighter touch approach to regulation will prevail to promote continued growth. Former Minister for Economic Affairs, Darmin Nasution, said at the Indonesian Fintech Summit & Expo 2019 that the government was focused on "light touch and safe harbour approaches"², although there has been no further comment on this since the October cabinet reshuffle.

Peer-to-peer lending licencing

Following the designation of AFPI as the official P2P association, AFPI is expected to play an increasing role in actively supporting the OJK and new operators planning to register with or obtain a P2P licence from OJK. AFPI, with staff from the Ministry of Communications and Informatics and the Indonesian Police Force, hold regular certification seminars and training aimed at directors, commissioners and shareholders to develop better knowledge of the P2P industry ecosystem and best practice. Participation in this training has become one of the prerequisites of registration as a P2P operator with OJK.



² <https://markets.businessinsider.com/news/stocks/indonesian-fintech-association-announces-indonesia-fintech-summit-expo-2019-1028569938>



ITALY

Year in Review 2019

Completion of the payment services regulatory framework

In 2019, the Bank of Italy completed its revision of the Italian regulatory framework on payment services by issuing a revised version of its Supervisory provisions on payment institutions and e-money institutions, new regulatory measures to prevent incumbent banks from denying the opening of payment accounts to payment institutions, an updated version of its Banking transparency regulations (to co-ordinate implementing measures under PSD2 and PAD) and certain instructions on the possible exemption from the duty to setup a “fall-back solution” for the access of third-party providers to payment accounts.

Strong customer authentication extension

The Bank of Italy has also given payment service providers additional time (until 31 December 2020) to migrate to “strong customer authentication” measures for e-commerce card-based payment transactions. This enhanced regulatory regime will pave the way for further developments in the context of the payment services sector in Italy, fostering competition and the development of new business models while ensuring protection of consumer rights.

Italian AML rules capture custodian wallet providers (in addition to the exchanges)

The transposition of the EU’s fifth Anti-money Laundering Directive (AMLD5) into Italian law has broadened the scope of the providers of services related to the use of virtual currencies that are subject to the Italian AML regulations, by including: (i) persons who provide services relating to the use, exchange, recording and conversion of virtual currencies into other virtual currencies (before the definition considered only the conversion of virtual currencies from or into currencies having legal tender); (ii) persons who provide services related to the issuance, offer, transfer and settlement and any other service related to the acquisition, trading and intermediation in the exchange of virtual currencies; and (iii) “custodian wallet providers”, i.e. persons who provide the services of safeguarding private cryptographic keys on behalf of customers with a view to holding, storing and transferring virtual currencies.

To carry out their business in Italy, all qualifying persons must inform the Ministry of Economy and Finance (MEF) and register with a (newly-established) section of the Italian Register of currency exchange operators. The decree providing the relevant implementing rules is expected to be formally issued in 2020.

Proposal for regulation of initial offerings and exchanges of crypto assets and cryptocurrencies

The regulatory approach to adopt in respect of crypto assets and cryptocurrencies has been a trending topic in Italy in 2019. In March, CONSOB published a discussion paper seeking stakeholders’ views on its proposal for the regulation of initial offerings and exchanges of crypto assets. The intention was to launch a national debate on these topics, given the absence of a harmonised approach in the EU, with a view to using this feedback for drafting a regulation that would ensure the high protection of customers without hindering financial innovation. The call for evidence was followed by a public hearing in June, but a final regulation has not yet been issued.

In parallel, the Bank of Italy has addressed this phenomenon, publishing a paper where it analyses the economic, accounting and prudential aspects of bitcoin-type “crypto assets” and summarises the regulatory approach that has been so far adopted in the various jurisdictions over crypto-exchange platforms.



ITALY

Year in Review 2019

Year to come 2020

Anti-money laundering obligations re virtual currencies

The Italian FIU has also published additional guidance on the most common illicit behaviours connected to the misuse of cryptocurrencies (based on the experience gained through the analysis of the suspicious transactions), renewing its request to the AML obligations recipients to pay maximum attention when dealing with or assessing transactions involving virtual currencies.

Cyber security

In late 2019 Italy has adopted stringent supervisory measures for the “cyber security” of several governmental agencies, public administrations and private companies active in the national strategic sector which, for these purposes, have been included in the newly-established “National Cybersecurity Perimeter”. In particular, these subjects have been required to comply with a detailed set of information and procedural standards, including obligations on outsourcing and business continuity, aimed at guaranteeing high levels of security and minimising any “cyber” risk for their networks and information systems.



ITALY

Year in Review 2019

Year to come 2020

Legal effectiveness of DLT and smart contracts

Law No 12/2019 introduced, in the Italian framework, the definitions of Distributed Ledger Technologies and Smart Contracts, setting out for the first time the legal effects of adopting such technologies: storing “data” in a DLT shall produce the legal effects of an “electronic time stamp” under Article 41 of eIDAS Regulation (meaning that it will be possible to use it as evidence in legal proceedings), while smart contracts have been recognised as satisfying the requirement of the written form (*forma scritta*, that is a requirement necessary for the validity or probation of many transactions under Italian law). [\(Read more...\)](#)

Technical standards for DLT and smart contracts

It is expected that, in 2020, the public body, Agenzia per l'Italia digitale (AgID), will outline the technical standards that DLTs and smart contracts will have to meet to produce the legal effects just described. This will be a significant development as it will pave the way to the adoption of blockchain in all those sectors where, to obtain certain legal consequences, it is fundamental that the existence of data or information at a certain point in time (date/hour) can be enforced against third parties.

Regulatory sandboxes for fintech firms

To encourage entrepreneurship and facilitate the development of technological solutions in the financial sector, the so-called “Growth Decree 2019” has established the creation of regulatory sandboxes where fintech companies can test and refine their innovative business models without being burdened from the outset by the usual regulatory requirements which would otherwise apply to their activities.

These sandboxes are set to take off in 2020 and will allow fintech firms to offer their products and services for a maximum 18-month timeframe within a partially deregulated environment, whilst mitigating risks to customers and the market more broadly. The application criteria and the

rules of these sandboxes will be set out in one or more decrees to be issued by the Ministry of Economy and Finance (MEF) upon consultation with the Italian supervisory authorities (Bank of Italy, CONSOB, IVASS).

FinTech Committee

The Growth Decree 2019 has also established a new committee at the MEF, the FinTech Committee, that has been entrusted to identify the objectives, define the programs and implement the actions to foster the development of fintech in Italy, as well as to make regulatory proposals and facilitate the contacts between market players and authorities.

Italian national strategy for AI and blockchain

The 30 experts appointed to the “Blockchain” group in late 2018 by the Ministry of Economic Development (MISE) will continue their work during 2020. Two sets of proposals – one relating to artificial intelligence (AI) and one to blockchain – have already been prepared and published for public consultation, and we expect these soon be turned into “national strategies” in 2020.

Italian Presidency of the European Blockchain Partnership

The deepening of the knowledge of these topics and the increase in related public and private investments remains a fundamental priority for Italy, as testified also by the appointment of Italy in July 2019, for the duration of one year, as President of the European Blockchain Partnership (alongside Sweden and Czech Republic) – a European initiative aimed at promoting co-operation amongst Member States to exchange expertise and define a common strategy for the implementation of blockchain technologies. The leadership role obtained in this project will allow Italy to further promote awareness and utilisation of blockchain technologies.



JAPAN

Year in Review 2019

Regulatory sandbox

Japan introduced a regulatory sandbox system in 2018 under the Act on Special Measures for Productivity Improvement (*seisansei koujou tokubetsu sochi hou*). In January 2019, the Financial Services Agency of the Japanese government (JFSA) announced that Crypto Garage, Inc.'s application to participate in the regulatory sandbox had been approved.

Crypto Garage develops blockchain financial services focusing on a blockchain based delivery-versus-payment (DvP) settlement system between JPY and crypto assets. Under this project, Crypto Garage will provide the participating crypto-exchanges with "SETTLENET", which allows the exchanges to issue a stablecoin pegged to the Japanese yen (JPY-Token) on the "Liquid Network", and trade against Liquid Bitcoin (L-BTC) that are pegged to Bitcoin on a Bitcoin sidechain launched by Blockstream Corporation, headquartered in Victoria, Canada.

DvP settlement system between Japanese yen and crypto assets

By utilising atomic swap technology (a technology that enables peer-to-peer simultaneous exchange of crypto assets from one party to another, without counterparty risk and going through a third-party service without any counterparty risk or intermediaries), "SETTLENET" allows the exchanges to simultaneously deliver L-BTC in exchange for the receipt of JPY-Token on the "Liquid Network". This will enable rapid, secure and confidential transfer of the crypto assets while eradicating counterparty risk. In addition, SETTLENET will provide the regulatory authorities with the functionality to monitor any unlawful trade, including money laundering. The sandbox testing period will be one year from 21 January 2019 and only licensed cryptocurrency exchanges in Japan will be able to participate in Crypto Garage's pilot.

Characterisation and licensing of stablecoins

Various market participants, including banks and tech market players, have announced their intention to issue stablecoins whose value is pegged to the Japanese yen. Also, the Japanese Bankers Association has run a trial of interbank use of stablecoins. In Japan, stablecoins could, in terms of their legal nature, be different from more typical forms of crypto assets. For example, fiat-collateralised stablecoins may not be characterised as crypto assets under the Fund Settlement Act where their value is pegged to the price of a statutory currency. They may potentially be regarded as prepaid payment instruments, or the function of payment associated with stablecoins could be regarded as money transfer.

The necessary licence required to issue or otherwise deal with stablecoins will therefore vary and depend on the legal nature and characteristics of the particular stablecoin.

Data sharing by financial institutions

In Japan the scope of business of financial institutions including banks, insurance companies and securities firms and investment managers is strictly regulated, but in 2019 the relevant financial laws were amended, to allow financial institutions to provide customer information to third parties (with customer consent) if such information contributes to the advancement of such financial institutions' main businesses or to the enhancement of user convenience. This includes permitting transmission of other companies' advertisements to customers, providing services in co-operation with other companies, and conducting management and handling of information between customers and business operators (information trust functions, or so-called Information Banks).

JAPAN

Year in Review 2019

Year to come 2020

Protected data

In July 2019 the Unfair Competition Prevention Act (UCPA) was amended to enhance the legal protection available to certain data including so-called big data by adding the wrongful acquisition, disclosure and use of “Protected Data” to the list of acts of unfair competition. “Protected Data” means technical or business information accumulated in a significant quantity by electromagnetic means as information provided to specific persons on a regular basis. The courts can issue injunctions and award monetary damages in respect of the wrongful acquisition, disclosure or use of protected data where this amounts to an act of unfair competition under the UCPA. See the Ministry of Economy, Trade and Industry (METI) Guideline on Protected Data published in January 2019, which provides practical guidance¹.

Developments in regtech

Under the Financial Instruments and Exchange Act (FIEA), listed companies are required to submit Annual Securities Reports (ASRs), which are made available via EDINET³. These reports include information about their business model, operations and financial results. The JFSA is planning a push into the world of artificial intelligence (AI) via a project suggested by its own staff. The project that the JFSA is launching would check whether AI can be used for efficient examination of ASR and will start with reports published on EDINET. The JFSA is looking for companies that have an interest in AI and that are willing to co-operate in this experiment.

Cyber security

The Basic Act on Cybersecurity 2014 provides the basic framework for the responsibilities and policies of the national and local governments to enhance cybersecurity in Japan. The Amended Basic Act on Cybersecurity introduced in late 2018 aims to ensure cyber security while Japan hosts the Tokyo Olympics & Paralympics in 2020.

The Amended Basic Act on Cybersecurity sets up the Cybersecurity Council to promote cybersecurity measures. The council, which was established in April 2019, consists of national government agencies, local governments, critical information infrastructure operators, cyberspace-related business entities, and educational and research institutions and will be responsible for overseeing the establishment standards for cybersecurity measures for national administrative organs; the promotion and implementation of evaluative measures, including audits; and the co-ordination with relevant stakeholders in Japan and abroad when cyber security breaches and threats occur.

³ Electronic Disclosure for Investors' Network

JAPAN

Year in Review 2019

Year to come 2020

Digital tokens regulated securities

Amendments to the Act on Settlement of Funds (Act No. 59 of 2009, the Amended Fund Settlement Act) and the Financial Instruments and Exchange Act (Act No. 25 of 1948, the Amended FIEA) will come into force on or before 7 June 2020.

From a fintech perspective the Amended Fund Settlement Act regulates fund transfer businesses, prepaid payment instruments businesses (e-money) and crypto-asset transfer businesses. The Amended FIEA regulates as securities, rights or interests to receive distributions of profits generated from partnership-type investment funds, so-called collective investment schemes, which are represented by electronically transferable and recorded proprietary values (i.e. digital tokens) are defined as “Electronically Transferable and Recorded Rights” (ETRRs).

Security-type digital tokens not crypto assets for fund settlement purposes

Under the Amended FIEA, security-type digital tokens that fall under ETRR are categorised as Type 1 Securities⁴ because such digital tokens are electronically recorded and can be easily transferred and could be widely disseminated to the public. Considering that security-type digital tokens which constitute ETRR will be categorised as Type 1 Securities and therefore regulated by the FIEA, in order to avoid overlapping regulations, security-type digital tokens will be excluded from the definition of crypto assets under the Amended Fund Settlement Act.

Security Token Offerings requirements

Under the Amended FIEA, as ETRRs will be categorised as Type 1 Securities as mentioned above, in principle, when offering security tokens which fall under ETRRs, the issuer thereof must file a securities registration statement (SRS) unless the relevant private placement requirements can be satisfied. The issuer must also file annual reports and be subject to other continuous public disclosure obligations after the filing of the SRS. The public disclosure requirements are strict compared with those applicable to Type 2 Securities.

The Amended FIEA requires distributors/intermediaries of security token offering (STO) to register as Type 1 Financial Instruments Business Operators (FIBOs), which are subject to stricter registration

requirements and regulations than Type 2 FIBOs (the type of registration required for intermediaries of Type 2 Securities⁴). Accordingly, current crypto asset exchangers registered under the Settlement Act are not permitted to handle STOs or security tokens unless and until they obtain Type 1 FIBO registration in accordance with the amended FIEA. On the other hand, the issuers of such security tokens must generally be registered as Type 2 FIBOs if they make the solicitation themselves.

The Amended FIEA will add crypto-assets to the scope of “financial instruments”; therefore, derivatives transactions in which (i) a crypto-asset is the underlying asset; or (ii) an index relating to a crypto-asset is the reference index shall be categorised as “financial instruments businesses” that are subject to regulations under the Amended FIEA.

Regulation of crypto derivatives

The Amended FIEA will add crypto-assets to the scope of “financial instruments”; therefore, derivatives transactions in which (i) a crypto-asset is the underlying asset; or (ii) an index relating to a crypto-asset is the reference index shall be categorised as “financial instruments businesses” that are subject to regulations under the Amended FIEA.

Provision of fintech or insurtech services by insurance companies

Under the amended Insurance Business Act enacted in May 2019, restrictions on the scope of businesses that can be conducted by subsidiaries of insurance companies were relaxed in order to enable the subsidiaries of insurance companies to conduct fintech and insurtech businesses. Going forward, insurance companies may, with authorisation from relevant authorities, as an exception to the so-called 10% rules, acquire or hold up to 100% of the voting rights of companies providing services that contribute or are expected to contribute to the advancement of the insurance business, by using information and communication technology and other technologies or by improving the convenience of users.

⁴ Rights that would be deemed as securities as defined in Article 2, paragraph 2 of the FIEA, including beneficial interests in trusts (excluding beneficial certificates in investment trusts), interests in investment partnerships, interests in collective investment schemes or membership rights of juridical companies, etc.).





LUXEMBOURG

Year in Review 2019

Year to come 2020

Open banking under PSD2 and strong customer authentication

The regulatory technical standards governing open banking under the EU's second Payment Services Directive (PSD2) entered into effect in September 2019, marking the beginning of a new era of open banking in Luxembourg. Firms have generally been well-prepared in view of complying with the new requirements on day 1. It now remains to be seen what the impact of the new requirements will be on the ecosystem. The Luxembourg financial sector regulator (CSSF) has also confirmed that it will extend the implementation period of Strong Customer Authentication (SCA) beyond 14 September 2019. The extension applies only to the category of e-commerce card payment transactions.

Market evolution

We have seen an ever-increasing number of fintech players (start-ups and established players) setting up base in Luxembourg, including in the context of Brexit. We also see increased co operation between fintechs and traditional players, and increased funding of smaller actors.

CSSF White Paper on use of AI in the financial sector

The CSSF has published a White Paper on AI in the financial sector, laying out opportunities, risks and recommendations on the subject matter. While the paper is non-binding, it shows the increased interest of the regulator in the subject matter and appetite for dialogue with market participants.

New Law on the registration and holding of securities through distributed ledger technology

The Law of 1 March 2019 amended the Luxembourg law of 1 August 2001 on the circulation of securities. The amendment enlarges the scope of the 2001 Law, to permit the holding and registration of transfers of securities via distributed ledger technology, such as the blockchain. The wording of the 2001 Law is technologically neutral, by making reference to "secure electronic registration devices, including distributed electronic registers or databases".

Update of the CSSF Circular on cloud outsourcing

On 27 March 2019 the CSSF updated CSSF Circular 17/654 on cloud outsourcing, taking into account industry feedback and providing for a more comprehensive and pragmatic regulatory framework. It notably decreases regulatory requirements where an outsourcing to the cloud qualifies as non-material. The Circular was very much welcomed by the industry for its pragmatic approach.

Increased number of industry forums on fintech matters

We have seen an increased number of industry-wide working groups seeking to develop regulatory frameworks/standards regarding various fintech subject matters (payments, stablecoins, blockchain, ownership of digital assets, etc.).



LUXEMBOURG

Year in Review 2019

Year to come 2020

Regulatory developments

We could see further regulatory developments in key areas, such as the issue of securities via blockchain (and distributed ledger technologies more generally), stablecoins, and digitalisation of AML/KYC processes.

Open banking

Developments in open banking are likely to result in further regulatory guidance, the development of industry practices and the appearance of new disruptive market players.



PEOPLE'S REPUBLIC OF CHINA

Year in Review 2019

Year to come 2020

Financial sector reforms driving fintech and wider industry digitalisation

In July, the Chinese government issued 11 new measures to boost foreign participation in the financial sector in product lines including wealth management, asset management, money brokerage and insurance businesses. Whether striving for cross-border efficiencies by implementing global management networks or entering into collaborations with China's own roster of fintech powerhouses, greater foreign participation can be expected to further drive the digitalisation of China's financial sector.

Licensing of foreign payment platforms

More than a year after China announced plans to open payment services to foreign firms, PayPal Holdings became the first foreign payment platform licensed (directly or indirectly) to provide online payment services in China, following its acquisition of a 70% equity interest in Guofubao Information Technology Co. (GoPay), Ltd., a PRC-incorporated holder of a payment business licence and the company behind the GoPay payment platform.

Blockchain regulation

China has gradually embraced blockchain technology with new regulations on blockchain. These aim to clarify responsibilities of blockchain information service providers, establish a mechanism to monitor and evaluate the provision of blockchain technology and related services, and prevent the security risks associated with such services.

Fintech M&A and funding

Ant Financial acquired 100% of the currency exchange and payments company WorldFirst for USD700 million. This marks the most important acquisition made by a Chinese financial technology company to date in the global fintech market. It shows the growing confidence of China's digital champions to seek expansion outside of the protective domestic ecosystem, which some commentators argue has allowed them to develop unchecked.

Regulation of Big Tech in finance

The year 2019 witnessed tightened regulation of e-payment platforms, with the release of several new rules and hefty fines being imposed on more than 80 payment institutions. In August, the People's

Bank of China ("PBOC") alerted e-payment platforms to what the banking regulator sees as the main risk points for fintech, including bulk transfer of customer data, lack of verification of merchants' authenticity, and connecting to illicit online platforms.

To ensure the safety and reliability of fintech products, the PRC regulators issued the Financial Technology Product Certification Catalogue (First Batch) and the Rules for Certification of Financial Technology Products. These list 11 fintech products that will require third-party certification (including client software, security chips, security carriers, embedded application software, bank card ATM terminals, point of sale (POS) terminals, mobile terminal trusted execution environment (TEE), Trusted Applications (TA), barcode payment acceptance terminals (including display devices and scanning devices), voice recognition systems and cloud computing platforms), as well as specific product definitions and benchmarks for certification.

Cross-border information transfers in AML/ internet information services

Regulators have enhanced scrutiny on cross-border transfer of KYC and transaction data by imposing an onshoring requirement on client identity information and transaction information collected by banking financial institutions. It is yet to be clarified under what circumstances a foreign-invested bank may transfer KYC and transaction data to an offshore recipient.

Personal information rules in financial sector

Protection of personal information in the financial sector has been reinforced, and draft rules are being formulated to specifically regulate the collection, processing, use and sharing of "personal financial data" by financial institutions. Based on the official timetable published by the PBOC, a final version of these rules is expected by the end of 2019.

Blueprint for big data, cloud computing and AI technology in finance

The PBOC released a three-year fintech development plan, aiming to develop tech and safety specifications for AI, big data, cloud computing and other applications in the financial sector, and to define the application of these new technologies within a safe and controllable scope.



PEOPLE'S REPUBLIC OF CHINA

Year in Review 2019

Year to come 2020

Financial sector reforms driving fintech and wider industry digitalisation

In July, the Chinese government issued 11 new measures to boost foreign participation in the financial sector in product lines including wealth management, asset management, money brokerage and insurance businesses. Whether striving for cross-border efficiencies by implementing global management networks or entering into collaborations with China's own roster of fintech powerhouses, greater foreign participation can be expected to further drive the digitalisation of China's financial sector.

Illegal crowdfunding activities

The regulatory storm in the Chinese crowdfunding, and especially the peer-to-peer lending, industry is likely to continue in order to address what is widely seen as chaos in this industry. Following a comprehensive clean-up of the industry and the regulatory regime having been refined, it is expected that this industry will shift towards transparency and sustainability, to create real value to the Chinese market.

National digital currency

The People's Bank of China (PBOC) has put forward proposals for a national digital currency, based on its digital currency electronic payment (DC/EP) system, which has been under development for five years. China may, therefore, be the first sovereign territory in the world to launch a digital currency to replace bank notes and coins. Unlike other cryptocurrencies, the proposed digital currency will remain under the management of a central monetary authority (which may give it more credibility than its rival private digital currencies).

Officials are proposing the currency's issuance to be governed by a two-tier system, where the PBOC issues the currency to authorised commercial institutions, and those institutions then proceed to circulate the currency to the public. It has been reported that the first tier could be in operation as early as next year.

Cryptography

The Cryptography Law, which will come into effect from 1 January 2020, is the first national law that expressly protects encrypted technology and systems from invasion. The new law will be the first step towards a regulatory framework which gives private enterprise the confidence to develop cryptographic technology and standards in China. The new law is expected to encourage more extensive use of cryptography to protect networks and information. It also has wide potential application to blockchain technology, and given the central role cryptography plays in blockchain, has the potential to aid the development of blockchain technology itself.

Blockchain regulation

2020 is likely to see more regulation of administration and provision of blockchain services, as those blockchain service providers which have registered the provision of their services under the new blockchain regulation increasingly roll out their public networks for commercial use and blockchain technology becomes more integrated into the real economy.

Cloud outsourcing by financial institutions

With the ever-increasing emphasis on risk prevention and control in the financial sector, IT service providers to securities and funds business institutions are required to have strong risk management and information protection capabilities. Outsourcing of cloud computing services in the financial industry has also been on the regulators' radar, and detailed regulations on this are expected to be released in short order.

Greater Bay Area data laws

One key emphasis of the Guangdong-Hong Kong-Macao Greater Bay Area initiative for greater co-operation on economic development, is to facilitate data flow within the region. However, the difference in the existing data protection regimes between mainland China (which has a national security focus) and Hong Kong (which has a privacy focus) has the potential to pose challenges for businesses in the protection, processing and management of personal data within the Greater Bay Area. To truly facilitate data flow, therefore, discussions and negotiations on creating a mutual data protection framework will be necessary over the coming year.



SINGAPORE

Year in Review 2019

Year to come 2020

AI, data and ethics

The Monetary Authority of Singapore (MAS) and the Personal Data Protection Commission have both released guidelines and frameworks for companies looking to use AI tools in their business operations. These guidelines cover issues such as fairness, ethics, accountability and ethics when using AI.

Data portability and innovation

The Personal Data Protection Commission consulted on changes to the Personal Data Protection Act to incorporate provisions mandating data portability (i.e. the ability for data subjects to direct an organisation to transfer personal data about them held electronically to another organisation). The consultation also proposes changes that will encourage and make it easier for organisations to conduct data analytics on personal data they have collected.

MAS opens applications for digital bank licences in Singapore

The MAS has opened applications for up to five digital bank licences, marking a new chapter in Singapore's banking liberalisation journey and ensuring the continued resilience, vibrancy and competitiveness of its banking sector. Licences are available to digital players who demonstrate an innovative and sustainable business model, even if they have yet to establish a track record in banking. Applications will close at the end of 2019. ([Read more...](#))

MAS launches Sandbox Express

The MAS has launched Sandbox Express, a "spinoff" from its current fintech regulatory sandbox, which provides financial firms with the option to test innovative financial products and services in the market. Under Sandbox Express, firms are able to commence market testing within 21 days of applying to the MAS, a drastically shortened approval process. The new platform reflects the MAS's continued commitment to encouraging experimentation and adoption of innovative technologies in the financial sector.

ASIFMA publishes roadmap for Tokenised Securities

ASIFMA has published a paper titled "Tokenised Securities – A Roadmap for Market Participants and Regulators". Focusing on tokenising traditional regulated securities such as shares and bonds, the paper discusses key aspects of the end-to-end tokenised securities lifecycle (i.e. structuring, issuance, distribution, primary listing, secondary trading, custody, portfolio management, advisory and market making) and how this compares to traditional securities. It also outlines how tokenisation could impact market participants (including incumbent financial institutions and issuers) and presents areas market participants need to consider in the various stages of the securities lifecycle. Finally, the paper also considers what a benign, enabling environment for tokenised securities requires from a regulatory, tax, technology and liquidity perspective. ([Read more...](#))

Singapore International Commercial Court considers cryptocurrency to be "property"

In *B2C2 Ltd vs Quoine Pte Ltd* [2019] SGHC(I) 03, Simon Thorley J considered it "right" that "cryptocurrencies may be treated as property" as they "have the fundamental characteristic of intangible property as being an identifiable thing of value". While not in issue in the case, this was one of the first instances where a court of law has made a statement on the question of whether cryptocurrencies may be considered to be property. ([Read more...](#))



SINGAPORE

Year in Review 2019

Year to come 2020

The Payment Services Act: What to look out for in 2020

The Payment Services Act (PS Act) is expected to come into force in January 2020, and will regulate key payments activities in Singapore such as e-money issuance, domestic and cross-border money transfer services, and digital payment token services. The aim of the new legislation is to enhance user protections through a risk-based framework while still facilitating innovation and encouraging the adoption of e-payments. The MAS has consulted on subsidiary legislation, Notices and Guidelines under the PS Act and is expected to finalise these shortly. ([Read more...](#))

MAS proposals to on update Technology Risk Management and Business Continuity Management guidelines

The MAS has consulted on proposed changes to their Technology Risk Management and Business Continuity Management guidelines for financial institutions. The proposed updates include measures that financial institutions are expected to implement in order to strengthen their operational resilience (an increasing area of global regulatory focus) in light of rapidly evolving cyber threats. We expect the amended guidelines to be issued in 2020.

SPAIN

Year in Review 2019

Year to come 2020

Digital transformation bill

On 22 February 2019, the Spanish Council of Ministers approved a draft bill on the “digital transformation of the financial system”. This draft bill aims to create a legal environment which will foster digital financial innovation while protecting consumers.

Regulatory sandbox

Among other things, the draft bill creates a “regulatory sandbox” for businesses to test out new products or services and additional measures relating to digital transformation, such as a direct communication channel between the financial authorities and companies. Accordingly, companies will be able to submit to the authorities their questions related to new applications, processes, products and business models.

International co-operation mechanism

The draft bill also sets forth an international co-operation mechanism for the Spanish authorities to be able to make arrangements with other authorities in foreign countries in the fintech sector.

Yearly reporting on digital transformation

Under the draft bill, the Secretariat of the Treasury and International Financing (a body of the Ministry of Economy) will also prepare a yearly report on the digital transformation of the financial system in Spain, including new technological developments, international evolution in the sector, the impact on consumer protection, and financial stability and supervision. ([Read more...](#))



SPAIN

Year in Review 2019

Year to come 2020

Progress on digital transformation

Following its approval by the Spanish Council of Ministers, the draft bill was set to continue its legislative process and was introduced in Parliament for debate. However, Parliament was dissolved twice for new elections and no ordinary sessions have been held for most of 2019. If parliamentary activity resumes as expected, it is likely that the draft bill will continue its course through the legislative process during 2020. As the bill is still in draft form, it may undergo changes as a result of this process.

Fintech-specific regulation

Spain has not yet regulated the use of cryptocurrencies which are not prohibited or restricted – or recognised as legal currency. No active fintech legislative or government action has been taken other than approval of the transposition of the EU PSD2 directive in Spain and the regulation of crowdfunding and crowdlending platforms. However, Spanish regulators have indicated that they are receptive to fintech activities and the Spanish Fintech and Insurtech Association (Asociación Española de Fintech e Insurtech) is calling for a review of the current regulatory environment to promote the development of fintech businesses in Spain. There may therefore be further developments towards the specific regulation of fintech in 2020.





SWEDEN

Year in Review 2019

Year to come 2020

Open banking

September 2019 saw the regulatory technical standards governing open banking under the EU's second Payment Services Directive (PSD2) entering into effect. A report conducted by Tink revealed that Sweden has the second highest positive opinion out of all Member States towards open banking. The Swedish Financial Supervisory Authority (SFSA, Sw. Finansinspektionen) has also confirmed that it will extend the implementation period of Strong Customer Authentication (SCA) in line with the EBA opinion in October. This builds on the provision of additional flexibility through migration plans that the SFSA implemented in light of the earlier EBA opinion in June.

Real-time payments

The owners of P27 Nordic Payments Platform AB recently announced that they have taken the first major step in the realisation of the Nordic region's first real-time payments system (P27). P27 will enable real-time, batch, domestic and cross-border payments, allowing payments to flow instantly between people and businesses within the countries of Denmark, Finland and Sweden. It is anticipated that P27 will launch during the course of 2021.

Market evolution

In February 2019, the inaugural Stockholm Fintech Week was launched, highlighting the breadth of fintech, regtech and insurtech players in Sweden and the Nordics.

The Swedish consumer agency is currently consulting on how consumer credit is provided, in part, due to the myriad new ways in which consumers can now access credit through fintech solutions.

Digital assets

Progress continues with the Swedish Central Bank's (Sw. Riksbanken) e-krona project to digitalise the Swedish krona, given the decline in the use of banknotes and coins. The project currently envisages that the e-krona would be for smaller payments and would constitute a direct claim on the Central Bank. It is intended to be accessible in real time, 24/7/365. A register-based e-krona would be combined with a

value-based solution that makes offline payments of small amounts possible and increases their availability for groups that do not want to or cannot have e-krona accounts. The Central Bank has launched a procurement process for a strategic partner to assist them with further development, including practical solutions and a better understanding of the technological possibilities. The procurement process is due to be completed by the end of the year.

Anti-money laundering supervision

Over the past year, the SFSA has taken several initiatives to strengthen its anti-money laundering (AML) supervision, including the establishment of a permanent working group together with other Nordic and Baltic supervisory authorities this spring. The SFSA has also increased its supervisory resources, planning to have three times the capacity of money laundering supervision at the end of 2020 than in 2018.

Swedish fintech firms have been assisting the Swedish police with the Black Wallet project, which is a platform for collaboration between the public and the private sector to identify AML risks in the evolving fintech market and to develop risk-mitigating measures.

Online lending and alternative non-bank mortgages

At the start of the year, in the context of online lending and other alternative non-bank mortgage provision, the SFSA clarified that investors in such mortgages must be professional investors. In addition, the SFSA has provided a set of guidelines for adequate management of liquidity risks, as well as clarifying that, where a bank establishes a mortgage structure outside its group (a so-called peribank structure) that is not fully consolidated, the bank needs to assess and manage any flowback risks itself, for example within the framework of the bank's stress tests of capital and liquidity.



SWEDEN

Year in Review 2019

Year to come 2020

Anti-money laundering

In 2020 we expect a continued focus on AML. Domestically, we are likely to see continued developments following the AML issues in the Baltics with certain Nordic banks, including some changes to the Swedish AML regime that are due to come into force in January 2020 and the likely output from increased resources in AML supervision. From a European perspective, the implementation of EU's fifth Anti-money Laundering Directive (AMLD5) is due in January 2020 and AML is one of the European Banking Authority's (EBA) strategic priorities for 2020. Those entities in scope of AMLD5 will need to ensure that their systems and controls are up to date. Further compliance requirements are likely to lead to opportunities for regtech firms.

Regulatory supervision

The SFSA in its supervisory priorities has flagged that it is anticipating the need for more in-depth supervision of those firms providing financial products to consumers as that market grows and develops. Swedish fintech firms in that space will need to ensure that their policies and procedures are in good shape.

Digital assets

With the procurement process for the e-krona due to be completed in 2019, we expect to see additional technical feasibility progress on the e-krona during the course of 2020.

Fintech code of conduct

We are expecting to see the conclusion of the consultation on a Code of Conduct for fintech firms led by the Swedish Fintech Association.

Data privacy in electronic communications

During 2020, the EU is could potentially to adopt the ePrivacy Regulation to supplement the General Data Protection Regulation (GDPR) with specific rules on the use of electronic communications, cookies and electronic marketing which will apply in financial services. The ePrivacy Regulation will be a uniform framework directly applicable in the EU, including Sweden, and is particularly relevant for fintech companies given that these companies usually offer their services online, use online tracking technologies and communicate electronically with existing and prospective customers, using for instance Internet of Things and mobile applications. However, the fate of the Regulation remains uncertain as the draft has thus far failed to get the approval of all member states.

UNITED ARAB EMIRATES

Year in Review 2019

Year to come 2020

Digital assets – regulation and inter-bank payments

In the past year, the UAE regulatory authorities have continued their efforts to create a comprehensive regulatory regime for blockchain and crypto-assets. The UAE's Securities and Commodities Authority (SCA) announced plans to regulate digital tokens as securities and to introduce a framework to regulate crypto-assets, including ICOs, cryptocurrency exchanges and other cryptocurrency trading infrastructure. This will affect entities seeking to issue, promote or market ICOs or token offerings in onshore UAE.

Additionally, the ADGM's Financial Services Regulatory Authority (FSRA) issued guidance supplementing the existing regulatory framework for crypto-assets in the ADGM. This sets out the FSRA's approach to the regulation of digital securities in primary and secondary markets, including in relation to offers, listings and market infrastructure.

Investment Managers and Digital Banks – new framework

The FSRA announced its regulatory framework for Digital Investment Managers (robo-advisors). The guidance covers the following key areas: (i) regulatory permissions that may be required to provide digital investment services in or from the ADGM; and (ii) how the FSRA will apply its authorisation criteria in key existing areas of technology governance, suitability and disclosure, and newer areas such as algorithm governance.

Additionally, the FSRA released its regulatory framework for digital banks. This sets out base capital requirements, governance requirements, compliance and risk management policies, as well as covering data protection.

New cryptocurrency

Together with Saudi Arabia, the UAE announced plans in January 2019 to launch a new common cryptocurrency, known as Aber. In its pilot phase, the use of the new cryptocurrency is expected to be restricted to the central banks of the two countries and a small number of banks in each of the UAE and Saudi Arabia. It is intended to allow blockchain-powered financial settlements between financial institutions, including cross-border payments.

Data protection

The UAE Telecommunications Regulatory Authority (TRA) has reformed its approach to data protection with the introduction of a new Internet of Things regulatory framework, including a new policy and procedures and new data protection rules. The new data protection provisions draw on international best practice (specifically the EU's GDPR), placing stricter obligations on those processing and controlling personal data.

Guidance to support API ecosystem

The FSRA issued guidance on the development and use of Application Programming Interfaces (APIs) in the ADGM in October. The purpose of the guidance is to promote a common set of technology and data standards for the use of APIs in the financial services sector, to enable different systems to connect and share data securely. This kind of collaboration is valuable for banks and fintech firms (such as those participating in the ADGM's Digital Sandbox) to facilitate open innovations using API architecture, which can enable them to deliver better services to the end customer.





UNITED ARAB EMIRATES

Year in Review 2019

Year to come 2020

Increased regulation and investment

The UAE Government is committed to making the country a regional and world leader for fintech. We therefore expect the Government's strategy of moving early to implement regulations and making significant amounts of capital available to fintech start-ups to continue in the year ahead.

As referred to in the Year in Review, the UAE's SCA released the initial draft of its Regulation for Issuing and Offering Crypto Assets in October 2019 for feedback from interested parties. In the coming year, this regulation will be finalised and brought into law, making the UAE one of the first countries in the world to have a comprehensive legislative approach to crypto assets.

The UAE Central Bank has announced that it will be creating a fintech office. This office will legislate at a federal level and aim to co-ordinate across the UAE's various jurisdictions and fintech initiatives.

Smart Courts – increased efficiency

There is significant focus in the UAE on offering smart and electronic services to promote the efficient resolution of disputes and the UAE has an ambitious agenda to become a world leader in legaltech and judicial innovation. We therefore expect further developments in this respect during 2020.

By way of example, the Dubai Government intends to run 100% of applicable government transactions on blockchain by 2020. As part of this strategy, the DIFC and Smart Dubai, a government initiative, are working together on a new "Court of the Blockchain". This taskforce is intended to be the first step in "creating a blockchain-powered future for the judiciary" of the DIFC.

Moves towards open banking

Increasingly UAE regulators are looking to develop and implement regional "open banking" standards to promote interoperability and innovation. It is likely that the standards adopted will be in line with the approach being developed in the UK (where "Open Finance" was a feature of the Bank of England's Future of Finance report in 2019 ([Read more...](#))), the European Union, where the Revised Payment Service Directive (PSD2) requires banks to open up data, functionality and APIs to third-party companies offering financial services (read individual country reviews for more on how PSD2 has been implemented in EU countries), and in Australia, which moved towards open banking in 2019. ([Read more...](#))



UNITED KINGDOM

Year in Review 2019

Review of the payments landscape

In June, the government announced a Treasury-led review of the payments landscape, with a view to ensuring the UK's regulation and infrastructure keeps pace with new payment models. At the same time, the Bank of England released its Future of Finance report and set out its plans to facilitate a diversity of payments options ([Read more...](#)). The Bank's Financial Policy Committee also developed three principles for assessing how UK regulation should respond to developments in the payments sector ([Read more...](#)). Earlier in the year, the Payment Systems Regulator (PSR) launched a review into the supply of card-acquiring services (which merchants need to buy in order to accept card payments). And meanwhile, Pay.UK, the operator of the UK's retail payment systems, has continued its project to develop the UK's shared retail payments infrastructure. ([Read more...](#))

Protecting access to cash

In March, an independent review on access to cash called for the government and regulators to step in urgently to ensure cash remains a viable means of payment for those who rely on it. As a result, the Treasury, Bank of England, PSR and FCA have prioritised protecting access to cash. ([Read more...](#))

Strong customer authentication requirements in payments

The effect of new EU security authorisation requirements was delayed to allow more time for payment service providers and merchants to adopt SCA-compliant technology, but firms must keep up with migration plans to benefit from the revised timetable for compliance ([Read more...](#)). UK account providers were also granted more time to prepare for SCA as it applies to online payments. ([Read more...](#))

Clarification around legal status of crypto assets, DLT and smart contracts

In November, the UK Jurisdiction Taskforce issued a legal statement on the status of crypto assets, distributed ledger technology and smart contracts under English law following a market-wide consultation supported by Linklaters ([Read more...](#)). The statement confirmed for the first time that, under English law, crypto assets are capable of being owned and smart contracts can be, or be part of, binding legal contracts. ([Read more...](#))

Perimeter and tax guidance for crypto assets

The FCA finalised its guidance on how different types of crypto assets are regulated under existing laws in the UK. Its final report categorised the market into security tokens, e-money tokens and unregulated tokens, but flagged that any type of token which facilitates payment services may also be regulated ([Read more...](#)). HMRC released guidance around the tax treatment of transactions in "exchange tokens". ([Read more...](#))

Focus on digital currencies

There has been a global focus on so-called "stablecoins" since June, when Facebook formally unveiled its plans to launch digital currency, Libra. UK authorities were quick to recognise the potential benefits Libra could bring, whilst emphasising that the highest standards of prudential regulation and consumer protection would need to be met *in advance* of any launch ([Read more...](#)). That message was reiterated by EU authorities as well as the G7 working group on stablecoins, which released a report outlining the key risks and challenges developers and regulators would need to address ([Read more...](#)). On the prospect of a central bank digital currency, the Bank of England said it has no current plans to develop one but is continuing its research in this area. ([Read more...](#))



UNITED KINGDOM

Year in Review 2019

Increased scrutiny of Big Tech in finance

Financial supervisors, including the Financial Stability Board ([Read more...](#)) and the European Banking Authority ([Read more...](#)), expressed concern about Big Tech's move into financial services and the sector's over-reliance on a small pool of cloud service providers. Competition authorities are increasingly sharpening their focus on Big Tech. In particular, a range of competition authorities, across the EU (France and Netherlands) and globally (Japan) are launching market studies to understand how the entry of digital payment companies may affect the existing business landscape. The European Commission has reportedly initiated both financial and anti-trust regulatory scrutiny of Apple Pay and Libra/Facebook. Hindering of access, market leveraging and information sharing concerns are on the EU regulator's agenda.

Fintech M&A and funding

In 2019 fundraising by fintechs fuelled acquisitions and international expansion with Europe maintaining the lead over Asia in fintech funding. Towards the end of 2019 we were seeing decreased volume but increased deal size in fintech M&A. We looked at the benefits of the consortia investment model in fintech. ([Read more...](#))

Global Regulatory Sandbox

The FCA-led Global Financial Innovation Network was launched with a view to creating a "global sandbox" to facilitate the interaction by innovative firms with regulators and they look to scale globally. Four US regulators, including the SEC and CFTC, joined the network in October. ([Read more...](#))

Prudential regulation of Neobanks

The Prudential Regulatory Authority raised concerns about the financial resilience of Neobanks given their rapid rate of growth. ([Read more...](#))

EBA outsourcing guidelines

The European Banking Authority (EBA) issued revised guidelines on outsourcing (including cloud outsourcing) arrangements which sit on top of the outsourcing rules in MiFID II and PSD2. Separate rules for outsourcing in the insurance industry are set out in Solvency II and the soon to be finalised EIOPA outsourcing guidelines. This proliferation of regulation and guidance reflects growing regulatory interest in the proper supervision and resilience of outsourcing arrangements.

The EBA Guidelines contain new obligations on firms to manage their outsourcings (including creating a detailed register of outsourcings) and new provisions that must be included in outsourcing contracts. The Guidelines apply to outsourcings "entered into, reviewed or amended" after 30 September 2019. Existing outsourcing arrangements must comply with the Guidelines at first renewal or, at the latest, 31 December 2021.

Regulatory scrutiny of artificial intelligence and machine learning

2019 saw increasing take-up of AI in financial services and consequent increased regulatory attention. James Proudman from the Bank of England directly addressed the governance implications of adopting AI and machine learning technologies within the financial services sector in a speech ([Read more...](#)) and the Bank of England and FCA published a survey of regulated firms' adoption of machine learning which indicated that firms are looking for more regulatory guidance around the deployment of AI solutions in financial services. ([Read more...](#))



UNITED KINGDOM

Year in Review 2019

Year to come 2020

Operational resilience

As digital financial systems have developed, operational resilience is increasingly becoming as important as financial resilience. European supervisors proposed adding explicit operational resilience and cybersecurity requirements in EU law ([Read more...](#)). The Bank of England's "Future of Finance" report made recommendations for protecting financial services from cyber risks. ([Read more...](#))

Following a number of high-profile service disruption incidents in the financial services sector, the House of Commons Treasury Committee published a damning report on IT failures in the financial services sector which concluded that the current level and frequency of disruption and consumer harm in financial services is "unacceptable" and "prolonged IT failures should not be tolerated". It set out a series of recommendations for UK financial regulators to respond to. ([Read more...](#))

Cyber security

Linklaters issued a report identifying that global cyber incidence has soared by 63% in the last three years with a new trend emerging in the dual use of AI as both a cyber threat as well as a cyber security solution ([Read more...](#)). Cyber threats were also a key discussion theme at the Sibos conference in London. Digitalisation of banking has made banks more vulnerable to cyber attacks, meaning that new types of controls are required. Regulators also confirmed that cyber risk in the finance industry is now systemic – an issue which becomes more account as the financial system becomes more interconnected. ([Read more...](#))

Anti-money laundering and counterterrorism standards

UK regulators considered regulating a broad spectrum of crypto service providers in implementing EU and global anti-money laundering and counterterrorism standards ([Read more...](#)). If finalised, the proposed new rules would go beyond the minimum requirements of the EU's fifth Anti-money Laundering Directive (AMLD5) to reflect the global standards set by the Financial Action Task Force. AMLD5 will bring various service providers, such as token exchanges and token issuers, within the scope of AML/CTF regulation for the first time. The UK Treasury also considered how best to implement proposals on electronic identification of customers and the regime for e-money providers. ([Read more...](#))

Regtech

The FCA published a report on the first phase of its digital regulatory reporting project ([Read more...](#)) which is exploring how to automate firms' reporting obligations ([Read more...](#)). The second phase aims to understand the economic viability of digital regulatory reporting and how it could apply to different product groups. ([Read more...](#))



UNITED KINGDOM

Year to Come 2020

Next generation payments regulation

The Treasury's review of the payments landscape is expected to lead to regulatory changes that respond to different types of payment provider and business model and seek to close any gaps in regulatory oversight. If non-bank payment providers are allowed access to the Bank of England's balance sheet (see below), we are likely to see new prudential requirements for these firms. ([Read more...](#))

Broadening access to Bank of England's balance sheet

The Bank of England has said it will be consulting on broadening access to its balance sheet in 2020. This could result in alternative payment providers being able to hold interest-bearing accounts at the Bank of England, which may in turn allow them to compete on a more level playing field with incumbent banks. ([Read more...](#))

Reducing frictions in cross-border payments

Global authorities and the financial industry have recognised that they need to address ongoing inefficiencies in cross-border payments ([Read more...](#)). The Bank of England has said it will continue its work in this area, for example through the reconfiguration of its real-time gross settlement system and its collaborations with other central banks ([Read more...](#)). Improvements to SWIFT's infrastructure – e.g. its Global Payment Initiative and ISO 20022 messaging standards – are also expected to help.

Capitalising on the revenue-generating opportunities of open banking

Whilst many banks will still be working to meet their compliance obligations under the EU's second Payment Services Directive (PSD2), we are likely to see more focus next year on the revenue-generating opportunities that this legal regime allows. Banks and third parties alike will be exploring how to capitalise on the regulatory framework of PSD2 – potentially through building their own client platforms – in order to serve real consumer needs. ([Read more...](#))

Strong customer authentication migration milestones

The migration to strong customer authentication under PSD2 must be completed by the end of 2020, with several milestones to be met along the way. ([Read more...](#))

Proposal to apply the Senior Managers Regime to market infrastructure

The Treasury Committee has urged the Government to extend individual accountability rules for banks and insurers to also apply to financial market infrastructure overseen by the Bank of England such as payment systems. ([Read more...](#))

Competition regulation of Big Tech in finance

In his speech on competition rules and digital platforms, Business Secretary Greg Clarke recommended that “Competition rules must change as platforms and big data are disrupting the basic plumbing of markets – and despite the high benefits they have brought, they sometimes create new forms of harm, especially for ordinary customers”. Meanwhile, the EU has set its sights on Apple Pay over antitrust concerns around preferencing of cards available on Apple Wallet.

Further regulation and guidance around digital assets

The FCA's proposal to ban the sale, marketing and distribution of crypto-derivatives to retail consumers is expected to be finalised in early 2020 ([Read more...](#)). And during the course of the year we may see further steps to extend the regulatory perimeter around crypto assets and crypto asset service providers, as UK and EU regulators, as well as global standard-setting bodies, continue to consider the need for this. The Financial Stability Board's report to the G20 on the adequacy of existing regulatory approaches to stablecoins will be one to watch out for ([Read more...](#)). We can also expect guidance from HMRC on the tax treatment of security tokens and utility tokens. ([Read more...](#))



UNITED KINGDOM

Year in Review 2019

Year to come 2020

Fintech M&A and funding

We expect Chinese companies to look increasingly to EU markets for fintech M&A investment opportunities in 2020. Continued uncertainty around Brexit and the UK political landscape is starting to have an impact on the UK fundraising climate with investors mindful of that UK businesses may soon sit outside the EU regulatory framework. Investors are also being increasingly selective when investing in fintechs at the later stage funding rounds with greater scrutiny on financial valuations, governance and a continued focus on the route to exit. 2020 may continue to see increased consolidation in the sector as the bigger players continue to make acquisitions to achieve scale or broaden their offering into adjacent services.

Regulation of ethics and AI

We anticipate a continued and more co-ordinated focus by regulators in the finance, data and competition spheres on the use of existing regulatory frameworks to ensure the ethical deployment of AI – focusing on fairness, accountability and transparency and the explainability problem. ([Read more...](#))

Data ethics and AI

In the October 2018 Budget, it was announced that the Centre of Data Ethics and Innovation would be exploring the use of data in shaping people's online experiences and the potential for bias in decisions made using algorithms. These two large-scale reviews form a key part of the CDEI's 2019/2020 Work Programme. The CDEI is also planning to develop an "AI Barometer" to identify the highest priority opportunities and risks associated with data-driven technology within the CDEI's remit.

Regulation of AI and machine learning in financial services

The BOE and FCA recognise that machine learning will be an important part of the way financial services are designed and delivered in the future and will consult further with financial firms on use of machine learning in financial services. They also plan to create a new public-private working group on AI to keep the conversation going ([Read more...](#)). Regulators have been urged by the Treasury Committee to monitor the discriminatory potential of artificial

intelligence and machine learning and set clear guidance for the sector on the basis that firms should not be using this technology if these risks cannot be rigorously identified and mitigated.

Regulating cloud service providers in financial services

The market for cloud services has been identified as a source of concentration risk and the Treasury Committee has argued that the case for the regulation of cloud service providers is "overwhelming". It will be interesting to see how the financial regulators respond on this recommendation. ([Read more...](#))

Supervision of operational resilience

The UK financial regulators are consulting on draft rules and guidance for firms to apply to improve their operational resilience which focus on setting impact tolerances for important business services. ([Read more...](#)) This will remain a top priority for the regulators who are likely to investigate senior managers for IT failures in parallel with investigations into their firms. Regulators have been encouraged to use their enforcement tools to hold individuals and firms to account for their role in IT failures and poor operational resilience as the Treasury Committee is concerned that the lack of individual accountability to date is indicative of a lack of "an ineffective enforcement regime". ([Read more...](#))

Collaboration on cyber

Increased collaboration by cyber criminals has increased pressure on the finance industry to collaborate in order to meet the escalating threat. The creation of a Financial Sector Cyber Collaboration Centre (FSCCC) was first announced in 2018 by industry body UK Finance, progress continued to operationalise the FSCCC in 2019 and we anticipate a formal launch in 2020. The stated aim of this organisation of 20 banks, insurers and securities exchanges is to collaborate on and work with the National Cyber Security Centre and National Crime Agency to fight cyber crime. At an international level the UK financial authorities will also formally collaborate with the Monetary Authority of Singapore to strengthen cyber security in their financial sectors.

Cyber security collaboration is likely to be a significant consideration in firms seeking to ensure their operational resilience.



UNITED STATES

Year in Review 2019

Uncertainty continues as to US regulatory approach to digital assets

A key theme this year was the “lack of clarity” regarding US regulatory guidance in the area of digital assets. Although the SEC Staff released a “[Statement on Framework for ‘Investment Contract’ Analysis of Digital Assets](#)” in April 2019 announcing the publication of an analytical token framework, and issued its first digital asset sale-focused [no-action letter](#), some – including certain US federal legislators and market participants – remained dissatisfied. Indeed, some have criticized the SEC and its Staff as unfairly “regulating through enforcement” and providing insufficient and, at times, inconsistent guidance concerning important threshold securities law questions, including: When is the sale of a digital asset the sale of a security, and, perhaps just as importantly, when and how does a digital asset initially is sold as a security, as a legal matter, “morph” into a non-security?

Some of 2019’s key events underscoring this regulatory uncertainty include:

- > Messaging service Telegram Inc., whose offering of “Gram” digital tokens the SEC halted in October 2019, after Telegram allegedly raised more than USD1.7 billion in investor funds, argued that the SEC failed to provide clear guidance and engaged in improper “regulation by enforcement.” ([Read more...](#))
- > Throughout 2019, the SEC continued to bring enforcement actions against digital asset issuers and other market participants for violating the US federal securities laws. ([Read more...](#)) In addition, with the issuance of no-action letters to [TurnKey Jet](#) and [Pocketful of Quarters](#), the SEC began to create a very limited path for initial sales of certain digital assets to proceed as sales of non-securities. Notably, those no-action letters were controversial, as such proposed token sales bore very little resemblance to traditional 2017-style ICOs. Indeed, some believe that TurnKey Jet’s offering should not have required an SEC no-action letter.

- > In October 2019, the CFTC [signalled](#) its greater focus on Fintech by elevating its LabCFTC to become an independent operating office of the CFTC that reports directly to the CFTC chair. On the same day, the CFTC also released its primer, [Artificial Intelligence in Financial Markets](#). ([Read more...](#))
- > The New York Attorney General also took action this year, obtaining a court order preventing iFinex Inc., which operates the Bitfinex virtual asset trading platform, and Tether Limited, which issues the “tether” “stablecoin” virtual currency, from further violating New York law. Yet Bitfinex and Tether arguably have achieved partial victories, as well, this year. For instance, in May 2019, Bitfinex won a motion to modify the injunction obtained by the NYAG, among other things, allowing Bitfinex and Tether to continue to operate. ([Read more...](#))
- > Meanwhile, on the legislative side, two ambitious bipartisan companion bills were introduced in the US House of Representatives, with the express aims of supporting the US blockchain industry and providing clarity for when the sale of a digital asset is not the sale of a security: the [Token Taxonomy Act of 2019](#) (H.R. 2144) and the [Digital Taxonomy Act](#) (H.R. 2154). Certain provisions contained within the bills generated some controversy and led to ongoing discussions, and we understand that the bills will be revised and reintroduced.
- > In May 2019, the US House of Representatives Committee on Financial Services announced the creation of two task forces covering a wide range of issues, including regtech, payments, big data and more. ([Read more...](#))
- > The CFTC confirmed that ether, the native token of the Ethereum blockchain, presently is a commodity. ([Read more...](#))

First token offering under Regulation A

In July 2019, Blockstack launched a USD23 million token public offering, the first offering of digital tokens qualified under Regulation A and a potentially groundbreaking moment for the cryptocurrency markets. Notably, Blockstack took the position that its token was the



UNITED STATES

Year in Review 2019

Year to come 2020

sale of an investment contract (and, hence, a security), but not an equity or debt security, meaning a transfer agent was not needed. By contrast, in the Gladius case and several 2018 enforcement actions (e.g. Airfox and Paragon), the SEC required Gladius to register its tokens as a class equity securities, without analysis, in addition to providing initial purchasers with notice of rights to rescission ([Read more...](#)). Gladius, the only token issuer announced by the SEC to have self-reported its failure to comply with US federal securities laws in connection with its token sale, reportedly has ceased operations ([Read more...](#)), leading some to question the viability of the SEC's proposed path to compliance for token sellers.

CFTC allows trading of physically settled Bitcoin futures on Bakkt

In August 2019, Bakkt, a subsidiary of the Intercontinental Exchange (which owns the NYSE), was granted the first approval from the CFTC for physically settled Bitcoin futures. Contracts began trading in September 2019. In October 2019, Bakkt announced that it would "launch the first regulated options contract for bitcoin futures" on December 9, 2019. Bakkt's CEO described the options launch as being a response to customer feedback and said that ICE Futures US self-certified the contract through the CFTC. ([Read more...](#))

Joint regulatory reminder of AML obligations re. digital assets

In October 2019, the SEC, CFTC and FinCen issued a [joint statement](#) to remind persons engaged in activities involving digital assets of their anti-money laundering and countering the financing of terrorism obligations under the Bank Secrecy Act.

SEC/FINRA statement on broker-dealer custody of digital asset securities

A June 2019 [joint statement](#) by the SEC and FINRA highlights three main areas for broker-dealers to consider – the customer protection rule, books and records requirements, and insolvency protections – but stopped short of providing concrete guidance. ([Read more...](#))

FinCEN addresses convertible virtual currencies (CVCs)

In May 2019, FinCEN published [new guidance](#) affirming its regulatory framework of CVCs. While the new guidance merely consolidates and summarizes previous rules and interpretations dating back to 2011, it provides an important resource for the financial industry in determining when dealing in CVCs will fall under FinCEN's authority and how to comply with subsequent regulatory obligations. FinCEN issued an [advisory alert](#) to assist financial institutions in identifying and reporting suspicious activities concerning dealings in CVCs. ([Read more...](#))

IRS issues controversial cryptocurrency tax rulings

In October 2019, the Internal Revenue Service released long-awaited guidance concerning the tax treatment of "hard forks" and "airdrops." Some market participants were dissatisfied with the IRS's guidance and expressed the view that the IRS had mis-described airdrops and hard forks, in addition to disagreeing with the IRS's specified tax treatment for airdrops.



UNITED STATES

Year in Review 2019

Year to come 2020

Clearer “paths forward” for compliant digital asset sales

We expect to see a continuing evolution of regulators’ (including the SEC’s) determinations of approved “paths forward” for compliant digital asset sales, both those digital assets expressly sold as securities and those that are deemed not to be sales of securities. Among other things, we anticipate an uptick in the number of Reg A+ offerings for digital assets, particularly given the recent Blockstack Reg A+ offering.

Stablecoins

In addition, we anticipate that so-called “stablecoins” will continue to rise in popularity, as some market participants argue that a “stable” (or in any event, less volatile) price may cause there to be no “reasonable expectation of profit” (i.e., one of the requirements under the *Howey* test for there to be an investment contract). Nonetheless, we also expect that regulators and legislators will remain cautious about stablecoins, both because there is no single type of stablecoin, and because of concerns about certain stablecoins supplementing, disrupting or replacing central bank fiat currencies.

Libra (or a competitor) likely to proceed outside the US

2020 is likely to be the year of the “payment token” or “social media coin.” Although Facebook CEO Mark Zuckerberg has said that Facebook would not move forward with the Libra project anywhere in the world until it gets approval from US regulators, he also said it was inevitable something like Libra would be launched either by the independent Libra Association, which includes a number of US companies as members, or by China, which has said that it was looking into a similar digital currency project. There could be a “race to the moon” if China issues a digital yuan, or a major non-US company issues a popular stablecoin, and US legislators realize that these types of digital assets are coming irrespective of whether Libra itself succeeds or moves forward.

Kik, Telegram and other high-profile litigated enforcement actions may answer some outstanding securities law questions

Several SEC enforcement actions relating to initial coin (token) offerings are on course to be litigated in 2020. The results of litigation may help to resolve critical issues in the regulation of cryptocurrencies, including whether, and under what circumstances, US federal securities laws apply to ICOs and related promotional activities by issuers and other market participants. While litigation often takes years to reach a final and non-appealable judgment, we believe it likely that at least some important threshold questions regarding digital asset sales will be answered. ([Read more...](#))

New data privacy laws

New York’s Stop Hacks and Improve Electronics Data Security Act (the SHIELD Act) will become effective in March 2020 and it expands the scope of covered entities required to notify New York residents whose personal information has been implicated in a data breach and lowering the standard for determining when a notification is required. Because the SHIELD Act has such a broad reach is critical that persons and entities – wherever located – that collect, process or store private information of New York residents continually assess and review their incident response plans and data security programs to ensure compliance with the SHIELD Act’s rigorous requirements. ([Read more...](#))

i https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/guidelines_on_protected_data.pdf

Key Contacts

Australia



Valeska Bloch (Allens)
Partner
Tel: +61 2 9230 4030
valeska.bloch@allens.com.au



Simun Soljo
Partner, Allens
Tel: +61 2 9230 4635
simun.soljo@allens.com.au

Belgium



Guillaume Couneson
Counsel
Tel: +32 2501 9305
guillaume.couneson@linklaters.com



Maurice Demeyer
Associate
Tel: +32 2501 9277
maurice.demeyer@linklaters.com



Jellen Rasquin
Managing Associate
Tel: +32 2501 9098
jellen.rasquin@linklaters.com

France



Sonia Cisse
Counsel
Tel: +33 15 643 5729
sonia.cisse@linklaters.com



Véronique Delaittre
Partner
Tel: +33 15 643 5885
veronique.delaittre@linklaters.com



Laurent Benoit
Managing Associate
Tel: +33 15 643 5839
laurent.benoit@linklaters.com



Sophia Le Vesconte
Senior Professional Support
Lawyer
Tel: +33 15 643 5763
sophia.le-vesconte@linklaters.com



Marc Petitier
Partner
Tel: +33 15 643 5761
marc.petitier@linklaters.com

Germany



Daniel Pauly
Partner
Tel: +49 697 100 3570
daniel.pauly@linklaters.com



Florian Reul
Head of Fintech Germany
Tel: +49 697 100 3194
florian.reul@linklaters.com



Christian Storck
Global Co-Head of Innovation
Tel: +49 697 100 3531
christian.storck@linklaters.com

Hong Kong SAR



Clara Hackney
Managing Professional Support
Lawyer
Tel: +852 2901 5611
clara.hackney@linklaters.com



Sumit Indwar
Partner
Tel: +852 2901 5626
sumit.indwar@linklaters.com

Indonesia



Randy Irawan (Widyawan & Partners)
Managing Associate
Tel: +62 21 2995 1512
randy.irawan@linklaters.com



Aria Priadhi (Widyawan & Partners)
Managing Professional Support
Lawyer
Tel: +62 21 2995 1551
arie.priadhi@linklaters.com



Ricky Purba (Widyawan & Partners)
Associate
Tel: +62 21 2995 1511
Email: ricky.purba@linklaters.com

Italy



Anna Ferrarresso
Managing Associate
Tel: +39 028 8393 5257
anna.ferrarresso@linklaters.com



Ugo Orsini
Partner
Tel: +39 028 8393 5244
ugo.orsini@linklaters.com



Alessandro Tanno
Managing Associate
Tel: +39 028 8393 5264
alessandro.tanno@linklaters.com

Japan



Hiroto Nakayama
Managing Associate
Tel: +81 36 212 1240
hiroto.nakayama@linklaters.com



Eriko Sakata
Partner
Tel: +81 36 212 1243
eriko.sakata@linklaters.com

Luxembourg



Harry Ghillemyn
Managing Associate
Tel: +352 2608 8353
harry.ghillemyn@linklaters.com



Nicolas Gauzes
Partner
Tel: +352 2608 8284
nicolas.gauzes@linklaters.com



Raoul Heinen
Managing Associate
Tel: +352 2608 8331
raoul.heinen@linklaters.com



Nicki Kayser
Partner
Tel: +352 2608 8235
nicki.kayser@linklaters.com

Key Contacts

PRC



Colette Pan
Senior Consultant
Tel: +86 21 2891 1868
colette.pan@linklaterszs.com



Alex Roberts
Counsel
Tel: +86 21 2891 1842
alex.roberts@linklaters.com

Singapore



Niranjan Arasaratnam
Partner
Tel: +65 6692 5858
niranjan.arasaratnam@linklaters.com



Peiying Chua
Partner
Tel: +65 6692 5869
peiying.chua@linklaters.com



Adrian Fisher
Partner
Tel: +65 6692 5856
adrian.fisher@linklaters.com



Jonathan Horan
Partner
Tel: +65 6692 5702
jonathan.horan@linklaters.com



Daniel Yeo
Managing Associate
Tel: +65 6692 5719
daniel.yeo@linklaters.com

Spain



Carmen Burgos
Partner
Tel: +34 91 399 6088
carmen.burgos@linklaters.com



Paloma Fierro
Partner
Tel: +34 91 399 6054
paloma.fierro@linklaters.com



Yiannis Kyriakides
Managing Associate
Tel: +34 91 399 6055
yiannis.kyriakides@linklaters.com



Ceyhun Pehlivan
Managing Associate
Tel: +34 91 399 6182
ceyhun.pehlivan@linklaters.com

Sweden



Patrik Björklund
Partner
Tel: +46 8665 4130
patrik.bjorklund@linklaters.com



Hedvig Helmersson
Managing Associate
Tel: +46 8665 6630
hedvig.helmerson@linklaters.com



Elisabet Lundgren
Partner
Tel: +46 8665 6777
elisabet.lundgren@linklaters.com

UAE



Reem Alsayegh
Counsel
Tel: +971 4369 5852
reem.alsayegh@linklaters.com



Nicholas Edwards
Partner
Tel: +971 2659 2124
nicholas.edwards@linklaters.com



Andrew Jennens
Partner
Tel: +971 2659 2115
andrew.jennens@linklaters.com

UK



Jennifer Calver
Global Tech and Fintech
Professional Support Lawyer
Tel: +44 207 456 2417
jennifer.calver@linklaters.com



Lisa Chang
Managing Associate
Tel: +44 207 4562 838
lisa.chang@linklaters.com



Julian Cunningham Day
Global Co-head of Fintech
Tel: +44 207 456 4048
julian.cunningham-day@linklaters.com



Harry Eddis
Global Co-head of Fintech
Tel: +44 207 456 3724
harry.eddis@linklaters.com



Richard Hay
UK Head of Fintech
Tel: +44 207 456 2684
richard.hay@linklaters.com



Michael Voisin
Partner
Tel: +44 207 456 4606
michael.voisin@linklaters.com

US



Jonathan Ching
Partner
Tel: +1 212 903 9170
jonathan.ching@linklaters.com



Jeffrey Cohen
Partner
Tel: +1 212 903 9014
jeffrey.cohen@linklaters.com



Douglas Donahue
Partner
Tel: +1 212 903 9222
douglas.donahue@linklaters.com



Joshua Ashley Klayman
U.S. Head of FinTech and Head of
Blockchain and Digital Assets
Tel: +1 212 903 9047
joshua.klayman@linklaters.com



Scott Sonnenblick
Partner
Tel: +1 212 903 9292
scott.sonnenblick@linklaters.com

linklaters.com

© Linklaters LLP. All Rights reserved 2019

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of Linklaters LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP and of the non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, One Silk Street, London EC2Y 8HQ, England or on www.linklaters.com and such persons are either solicitors, registered foreign lawyers or European lawyers.

Please refer to www.linklaters.com/regulation for important information on our regulatory position.