COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

United Kingdom
FINTECH

Contributor

Fox Williams LLP

Jonathan Segal

Partner | jsegal@foxwilliams.com

Chris Hill

Partner and Fintech Lawyer | chill@foxwilliams.com

Mardi MacGregor

Partner | mmacgregor@foxwilliams.com

Peter Finch

Partner | pfinch@foxwilliams.com

Kolvin Stone

Partner | kstone@foxwilliams.com

Sacha Schoenfeld

Partner | sschoenfeld@foxwilliams.com

The authors would like to thank Stewart Cook, Richard Aitchison, Bryan Shaw, Scott Steinberg, Emma Bailey and Chris Finney for their contributions.

|

This country-specific Q&A provides an overview of fintech laws and regulations applicable in United Kingdom.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

UNITED KINGDOM
FINTECH

1. What are the sources of payments law in your jurisdiction?

The most significant pieces of law governing payments in the UK are:

- The Payment Services Regulations 2017 ("**PSRs**").
- The Electronic Money Regulations 2011 ("**EMRs**").

The PSRs are the UK implementation of the Second Payment Services Directive (commonly known as PSD2) which aimed to open up the payments market and govern various payment-related activities that had previously been unregulated. These included money remittance (i.e. sending money from one place to another), operating a payment account, the execution of payment transactions and the issuing or acquiring of payment instruments. Under PSD2 and the PSRs, this scope was increased to include third party providers ("**TPPs**"), the so-called "open banking" account information service providers (or "**AISPs**" – who are enabled to pull digitised transaction data out of a payment account that is operated by another payment service provider), and payment initiation service providers (or "**PISPs**" – who are enabled to initiate a push payment, such as a bank transfer, from an account operated by another payment service provider). Further detail is given on open banking in answer to questions 4 and 5 below.

The EMRs, however, govern the particular payment service of issuing and distributing "e-money", which is an electronic representation of cash. The typical example of e-money is a prepaid card, but these days e-money structures underlie anything from gift cards to mobile banks.

Lastly, whilst it is not strictly speaking legislation, the document "Payment Services and Electronic Money – Our Approach" published by the Financial Conduct Authority (available here) is an excellent guide on how the FCA views the application of the various pieces of legislation.

However, the regulatory payments landscape in the UK is undergoing a potentially seismic change with a number of regulatory initiatives either on the horizon or being actively undertaken. By way of example, earlier in the year, the UK government published its statutory review of the PSRs, alongside a call for evidence on the wider payments landscape, including on the EMRs (available here). Both regimes are likely to be impacted as the Government considers the repeal and replacement of retained EU law as part of its work on the Future Regulatory Framework Review. Alongside this, the Government is in the process of conducting a full review of the payments landscape in the UK, and in November 2023 published a report on the "Future of Payments" (available here) in which it set out its recommendations on the next steps for the UK to successfully deliver a world-leading retail payments ecosystem. The report concludes the UK payments landscape is in a good position, with a long track record of security, reliability and resilience, and a leader on innovation in areas such as real time payments and Open Banking.

However, multiple ongoing major initiatives, including Open Banking, New Payments Architecture and Central Bank Digital Currency, mean the UK's payment landscape is lacking 'a North Star', with no clear or agreed vision of what they aim to achieve in aggregate. Therefore, the strongest recommendation is that the UK Government develops a National Payments Vision and Strategy, with the primary aim of simplifying the landscape and high-level guidance on key priorities so regulators and industry can align on their delivery.

2. Can payment services be provided by non-banks, and if so, on what conditions?

Under the PSRs, non-banks can become authorised to provide payment services. There are a number of ways that they can do this. The first is to become an authorised payment institution ("**API**"). In order to do so they must go through the authorisation process with the FCA, for which purpose they must meet a number of

 © 2024 Legalease Ltd

requirements including the holding of capital, safeguarding funds, record keeping, accounting and audit, conditions around material outsourcings, and provision of information to customers of the payment services. The second is to become authorised as a small payment institution. The compliance burden is significantly less than for an API, but with restrictions such as that a small payments institution cannot have an average monthly transaction volume over the previous year (or projected volume) of more than €3 million.

In addition, the FCA provides for a simplified application process for entities providing account information services only. The application is shorter and the compliance burden is lower, reflecting the fact that AISPs transact in data only and do not move or hold funds. The FCA decides when an application is complete, and has up to 3 months from receipt of the completed application to make a decision on whether or not the application is successful.

Any firm who wants to issue e-money alongside providing payment services will need to become an authorised electronic money institution ("**AEMI**") under the EMRs. Firms wishing to become an AEMI will need to go through a similar authorisation process as described above for APIs. For smaller firms, there is also the ability to get authorised as a small electronic money institution. Whilst the compliance burden is reduced, similar restrictions to those imposed on small payments institutions will apply.

3. What are the most popular payment methods and payment instruments in your jurisdiction?

In its latest Payment Markets Report published in September 2023 (available here), UK Finance confirmed:

- The most popular payment method by far continues to be the debit card. For the first time ever, half of all payments in the UK in 2022 (22.9 billion) were made using debit cards.
- Payments made using credit cards increased by 19 per cent from 3.4 billion in 2021 to 4.1 billion in 2022.
- Across both debit and credit cards, there were 17 billion contactless payments, a 30 per cent increase on the 13.1 billion made in 2021. Contactless payments were used extensively throughout the UK in 2022, with 87 per cent of people making contactless payments at least once a month or more frequently.
- The long-running trend in cash has been one of continued decline, although it remains the second most frequently used payment method. However, the total number of cash payments made in the UK during 2022 increased to 6.4 billion, (2021: 6 billion). Growing fears about inflation and the rising cost of living have meant some people are making greater use of cash as a way of managing budgets.
- Around one in eight people in the UK (12 per cent) reported using BNPL services to purchase something during 2022, the same proportion as in 2021.
- 30 per cent of the adult population reported being registered for at least one mobile payment service in 2022, with younger people more likely to be making use of mobile wallets.

4. What is the status of open banking in your jurisdiction (i.e. access to banks' transaction data and push-payment functionality by third party service providers)? Is it mandated by law, if so, to which entities, and what is state of implementation in practice?

In the UK, open banking is facilitated by the PSRs, implementing PSD2, (see answer to question 1 above for more detail), and the work done by the Open Banking Implementation Entity (the "**OBIE**") and other private entities and financial institutions seeking to implement its effect. The PSRs provide that an account servicing payment service provider – that is, the payment service provider maintaining a payer's payment account – must allow access to AISPs and PISPs (together referred to as "**third party providers**" or "**TPPs**"). AISPs – account information service providers (AISPs) are given access to a payment service user's account and transaction data, under certain conditions. This requirement applies to all account servicing payment service providers who make payment accounts accessible online, and can therefore include not only traditional banks but also e-money institutions and credit card providers. PISPs are given similar access, but practically speaking access will be limited to those payment accounts from which a credit transfer payment can be initiated.

The PSRs impose requirements on both the account servicing payment service provider and the AISP. The PSRs require that the account servicing payment provider: must communicate securely with the AISP in accordance with the EBA RTS on SCA; treat any request for data access from an AISP exactly it would a data access request from the payment account owner; and

 © 2024 Legalease Ltd

not require the AISP to enter into a contract with it. The PSRs require that AISPs: act only with the explicit consent of the payment service user (account owner); ensure the confidentiality of the payment service user's personalised security credential; communicate securely with the account servicing payment service provider in accordance with the EBA RTS on SCA; restrict its access to designated payment accounts and transactions only; not request "sensitive payment data"; and not use, access or store any information for any purpose other than the provision of the account information service that the payment service user has explicitly requested. In this, the PSRs implement the requirements set out in PSD2; however, the PSRs definition of account information services is slightly narrower than that set out in PSD2. While PSD2 takes a broad view of account information service as the provision of consolidated information on one or more payment accounts, the PSRs narrow this by including in the definition the provision that account information thus obtained be provided "only to the payment service user" or "the payment service user and to another person in accordance with the payment service user's instructions". In other words, any AISP registered with the FCA in the UK will need to be able to provide the account information back to the payment service user and not simply route the information to a third party.

In relation to PISPs – payment initiation service providers – similarly, account servicing payment service providers must execute payments initiated by PISPs. The PSRs impose requirements on both the account servicing payment service provider and the PISP. The PSRs require that the account servicing payment provider:

- must communicate securely with the PISP in accordance with the EBA RTS on SCA;
- make available to the PISP all information about the initiation of the payment transaction as well as all information the account servicing payment service provider has regarding the execution of the payment transaction;
- treat any payment order exactly as it would a payment order requested directly by the payment account owner;
- not require the PISP to enter into a contract with it. The PSRs require that PISPs do not hold the payer's funds at any time;
- ensure the confidentiality of the payment service user's personalised security credential;
- do not provide any information about the payer to anyone other than the payee, and then only with the payer's explicit consent;
- identify themselves to the relevant account servicing payment service provider upon initiating a payment order and communicate securely with the account servicing payment service provider in accordance with the EBA RTS on SCA (see answer to question 1 above);
- not store "sensitive payment data";
- not request information from the payer except as necessary for the payment initiation;
- not use, access or store any information for any purpose other than the provision of the account information service that the payment service user has explicitly requested; and
- not modify any feature of the initiated transaction.

OBIE – the Open Banking Implementation Entity

The EU-based PSD2 and PSRs were preceded by and are now in force concurrently with the UK-specific OBIE provisions. The OBIE was initially set up by the UK's Competition and Markets Authority ("**CMA**") in 2016 to deliver open banking to the UK, in response to a CMA report on the UK retail banking that found that established banks do not need to compete hard enough for customers, and that new entrants to the market encountered difficulty in obtaining access. The OBIE required nine major retail banks (known as the CMA 9) to develop application programming interface ("**API**") standards to facilitate the payment service users' access to their current account data. Standard implementation requirements for firms using these API standards have been published by the OBIE, with a view to aligning the firms' APIs with the requirements and goals for establishing TPP access to accounts set out in PSD2. Additional information on the OBIE, including its Customer Experience Guidelines and Technical Specifications, can be found here.

In January 2023, the Competition and Market Authority announced that the six largest banking providers (of the CMA 9) have implemented the requirements of the Open Banking Roadmap and therefore the implementation phase of Roadmap is substantially complete (with the remaining 3 bank providers to complete the remainder of the Roadmap requirements as soon as possible).

In March 2022, the FCA, PSR, CMA and HMT announced the creation of a Joint Regulatory Oversight Committee (JROC) with the remit to oversee the planning and preparation for the future open banking entity and the transition to the future regulatory framework. In June 2023, the JROC published a programme of work to take forward recommendations for the next phase of open banking in the UK and includes a working group on variable recurring payments and another working group on the future open banking entity. Further information

 © 2024 Legalease Ltd

on the programme of work can be found here.

Implementation in practice

According to the most recent Open Banking Impact Report in October 2023 (available here), there were 151 regulated firms with open banking enabled products and services with the majority of those providers offering products and services to help financial decision-making, increased payments solutions and credit solutions. In addition, the Report highlights that over 1 in 9 (11%) of consumers and 17% of small businesses are active users of open banking and the value of open banking payments has reached a record high.

5. How does the regulation of data in your jurisdiction impact on the provision of financial services to consumers and businesses?

The main piece of legislation around data is the General Data Protection Regulation ("**GDPR**"), which has been incorporated into UK law and tailored by the Data Protection Act 2018 ("**DPA**"). As in other jurisdictions within the European Union, the GDPR is an evolution of the previous legislation around data protection and in many ways codifies and puts on a mandatory footing what was already best practice in relation to the treatment of personal data. The scope of data covered by the GDPR is broader than under the previous legislation, in ways that are likely to be relevant for a number of fintech business models. For instance, GDPR explicitly includes biometric data within the scope of the "personal data" it governs, which is likely to be of relevance to those providing identity verification or authentication services. It also includes location data, which may well be relevant to fintech providers that are operating mobile-based services.

Privacy by design and by default

Among the many other obligations emanating from GDPR around the treatment of personal data, some of the most important for early-stage fintechs to consider are the obligations in Article 25 around data protection by design and by default. These entail the building of systems and processes in a way that integrates data protection principles as a matter of technical architecture and process management. One aspect of this is ensuring that personal data is stored in such a way that it is only seen by people who really need to see it, using techniques such as data minimisation and pseudonymisation, meaning that having one single repository of all customer data is unlikely to be acceptable. Existing large organisations, both within and outside the financial services arena, have had to put a large amount of effort into complying with these requirements; new fintechs have an opportunity to get this right from the outset.

Transparency and accountability

Another key focus of GDPR is transparency and accountability. This means that organisations handling personal data have to be very explicit and clear with their customers and their employees about the personal data they are collecting and how they are using it, and have to keep clear records of the same. There are also obligations to include in contracts with data processors (for instance subcontractors for IT services) specific obligations that are designed to draw out the detail around the treatment of personal data in the contractual arrangement, in a way that will help to ensure compliance with data protection principles. Organisations which carry out certain types of processing activities are also obliged to appoint a data protection officer who is responsible for monitoring the organisation's compliance with data protection principles.

International data transfers

Fintechs planning to transfer or store personal data outside the European Economic Area (EEA) should be aware of the strict requirements in doing so. As the GDPR is EU-focused legislation, any entity transferring personal data outside the EEA will need to apply additional protections to that data. This can take the form of, for example, mutual contractual obligations between the transferring and receiving parties. The use of cloud providers, third-party hosting platforms and data centres are just some examples of where personal data is commonly transferred and stored outside the EU. Following the UK's departure from the EU, on 28 June 2021 the EU adopted an "adequacy decision" under which it is viewed as having protections which are equivalent to those in the EU, meaning that most data can still flow from the UK to the EU and the EEA without additional safeguards having to be put in place.

Profiling

The GDPR also places restrictions and obligations on entities using personal data for the purpose of profiling data subjects or making solely automated decisions about them. Profiling and automated decision making can only be carried out in certain circumstances, and data subjects have additional rights in relation to this type of processing, such as the right to object and the right to have any such decision manually reviewed. Technology involving big data, artificial intelligence and machine learning frequently involve profiling and/or

 © 2024 Legalease Ltd

automated decision making.

Data subjects' rights

One other area of GDPR which is potentially a great advantage in fintech is the new set of obligations which empower individuals whose data you are holding ("data subjects") to transfer the personal data you hold about them electronically to another service provider. These "data portability rights" can be very useful for a data-driven fintech company, as they may enable it to some extent to get hold of data collected in the context of other services that might otherwise not be obtainable – in many ways this is a broad data access right that is similar in principle to open banking (see answers to question 4 above).

Regulatory fines

The data protection and privacy regulator in the UK, responsible for enforcing GDPR and the DPA, is the Information Commissioner's Office ("**ICO**" – not to be confused with "initial coin offerings"). As with all European privacy regulators, the ICO is empowered to conduct investigations into the application of GDPR, and impose fines or restrictions on processing. The fines for the most serious breaches can be up to €20m or 4% of worldwide turnover; however, most fines are likely to be significantly less than this.

Marketing

The other major pillar of data regulation in the UK likely to affect fintech is around marketing. This is often confused with being part of GDPR, but is a separate regime that sits alongside it. The UK regulations governing marketing communications are the Privacy and Electronic Communications Regulations 2003, commonly referred to as "**PECR**" or the "**PEC Regs**". These govern the way that organisations deal with marketing calls and messages, including as to how consent for such communications is to be obtained and maintained; they also cover the use of cookies and similar tracking technologies. The PEC Regs are again a UK implementation of a European Directive, known as the e-privacy Directive, which is currently in the process of being amended in the EU.

Scope of privacy regulation – non-personal data

It is worth noting that the above areas of data regulation apply to individuals' personal data, and while this will cover many of the types of data relevant to fintech, it does not cover everything. For instance, while the laws around open banking refer across to GDPR, the payment account data that they govern will in many cases fall outside the personal data regime, as is the case with much of the payments and finance data of small businesses. There are also other areas of financial services where non-personal data is regulated by different regimes, such as the EU Benchmarks Regulation, but these are more niche in their application.

6. What are regulators in your jurisdiction doing to encourage innovation in the financial sector? Are there any initiatives such as sandboxes, or special regulatory conditions for fintechs?

At the regulator level, the FCA has established a number of initiatives to support innovation in the interests of consumers.

Regulatory Sandbox – allows a wide range of firms to test innovative business models, delivery mechanisms, products and services in the real market, with real consumers in a controlled environment. Firms also have direct access to the FCA's dedicated teams, providing a level of advice and support around the regulatory regime and onward authorisation if this is required.

Innovation Pathways – firms with an innovative proposition can ask the FCA about regulation and how it applies to their business.

Digital Sandbox – a permanent facility allowing fintechs access to synthetic data assets to enable testing and validation of solutions, including an API marketplace;.

Green FinTech Challenge – to support development and live market testing of new products and services that will aid the transition to a net zero economy. Successful applicants will benefit from a package of the FCA's support services (Regulatory Sandbox and Innovation Pathways). The firms will also be offered bespoke support and engagement as part of this 'green cohort', for example, by taking part in showcasing and networking events.

At a broader level, Government is also looking at ways to ensure the UK remains at the forefront of innovation. The Financial Services and Markets Act 2023 ("**FSMA 2023**"), marked a pivotal step to improve the UK's financial market competitiveness post-Brexit. The FSMB 2023 is one of a number of measures the Government is undertaking as part of its work on the UK's Future Regulatory Framework and allows for a number of steps to be made towards regulatory innovation. Some of its aims include:

- Enhancing the scrutiny of financial services

 © 2024 Legalease Ltd

regulators.
- Removing unnecessary restrictions on wholesale markets.
- Protecting free access to cash.
- Enabling regulation of digital assets.
- Introducing fraud protections, particularly for APP scams.
- Establishing regulatory sandboxes that facilitate the use of new technologies such as blockchain.

7. Do you foresee any imminent risks to the growth of the fintech market in your jurisdiction?

The most obvious risk is the continuing effect of Brexit. This is for three main reasons. The first and most frequently cited is the loss of the passporting regime, under which firms that are authorised to carry out a regulated activity in one Member State of the EU are permitted to carry out that activity in other Member States on the basis of a registration in that Member State, rather than having to go through a full authorisation process, and without having to have an establishment in that jurisdiction. However, this will of course affect only those fintechs that operate in multiple jurisdictions, and which are carrying out regulated activities – so its effect may be limited in practice, not least because the threat of the loss of passporting has forced affected companies to prepare by setting up a continental base of operations.

The second and more real risk continues to be around immigration and access to talent. Fintech businesses need a wide range of skills that are sometimes quoted as not being available from within the UK in large enough numbers to support the UK's thriving fintech ecosystem, particularly around experienced software engineers. As such, the immigration controls on talent of this type are likely to be key to the success of the UK fintech ecosystem as we navigate the post-Brexit system, and many are watching this particular issue with keen interest.

The third is the potential for regulatory divergence. In many respects, divergence from the rest of European law could of course be a disadvantage, but as with passporting this is likely to affect mainly those aspects of financial services that inherently operate on a cross-border basis, such as international payments. However, for non-international fintechs, there is every possibility that the divergence could be beneficial, allowing UK legislators to create laws that track innovations in financial services more quickly than has been possible at a European level, and perhaps providing templates for other legislators in the process.

However, as set out in several of the answers to these questions, there are a great many reasons why the fintech ecosystem should continue to thrive in the UK, and none of the above issues are likely in our view to damage this materially in practice.

The other obvious risk is the current investment landscape which impacts all start-up and scale up businesses and to which the FinTech sector is by no means immune (as we set out below). With reduced access to funding through a depression in VC activity following the post-Covid boom years, the fall off from the sky-high valuations in that period leading to many businesses avoiding a raise for fear of a down valuation, and high interest rates following decade high inflation levels making debt financing a less attractive proposal, growth in certain FinTechs could be stifled by a lack of access to funding. This is not all bad news however, as those FinTechs with healthy balance sheets might well consider consolidation of their sector through mergers or acquisitions. Market trends also appear to signal that VC activity is increasing and with inflation falling closer to central bank targets, debt finance may start to become more attractive once again in the coming years.

8. What tax incentives exist in your jurisdiction to encourage fintech investment?

The UK has a number of tax incentives available to encourage fintech investment. In particular, the UK's three tax-based financing incentives – the Venture Capital Trust ("**VCT**") scheme, the Enterprise Incentive Scheme ("**EIS**") and the Seed Enterprise Incentive Scheme ("**SEIS**") – promote seed and growth funding. Both the SEIS and EIS encourage equity investment in start up and/or small to medium sized trading companies by providing tax relief to individuals who purchase shares in these companies. The VCT scheme provides tax relief for investors in VCTs, who themselves subscribe for shares in, or lend money to, small unquoted companies. The relevant tax incentives are increased for investment in "knowledge intensive" companies. Certain financial services activities (such as banking, insurance, money-lending, debt factoring and hire purchase financing) are outside the scope of these schemes, but many fintech activities can qualify.

In addition, entrepreneurs may be eligible for Business Asset Disposal Relief (previously known as Entrepreneurs' Relief) which provides for reduced capital gains tax rates if individuals sell a business or business assets, including certain shares or securities in a trading

 © 2024 Legalease Ltd

company or the holding company of a trading group.

Individuals are also encouraged to make tax advantaged investments into smaller and more risky businesses, including fintech businesses, through Innovative Finance Individual Savings Accounts ("**IFISAs**"). IFISAs allow investors to use their tax-free ISA allowance by investing in peer-to-peer lending and crowd funding, instead of simply investing in cash or stocks and shares. Income tax relief is also available more generally for irrecoverable loans that occur on Peer to Peer ("**P2P**") investments, with the amount of any P2P loans that become irrecoverable being able to be offset against interest received on other P2P loans.

The UK also has various schemes which provide tax relief for companies undertaking Research and Development expenditure, both of a revenue and capital nature.

9. Which areas of fintech are attracting investment in your jurisdiction, and at what level (Series A, Series B etc)?

Investment in SaaS platforms and payment solution software providers slowed significantly in the previous 12 months in the UK. However there was a rise in investment in Insurtech businesses and other fintechs that utilise AI technology. Much of the investment has been at the Seed+ or Series A level. Due to the inflated valuations of 2021/22, many fintech businesses decided not to raise Series B or larger rounds in fear of undertaking a downround, rather many undertook bridging rounds to ensure cashflow viability for the short-term in preparation for a larger round when macroeconomic factors stabilise.

10. If a fintech entrepreneur was looking for a jurisdiction in which to begin operations, why would it choose yours?

The early-stage UK fintech market is still very vibrant and still attracts early investment. It is relatively straightforward to incorporate your company in the UK and English incorporated companies allow for a smooth and efficient investment process. There are various tax incentives open to UK investors to invest in UK incorporated businesses and the FCA and UK government are fully supportive to grow this sector.

11. Access to talent is often cited as a key issue for fintechs – are there any immigration rules in your jurisdiction which would help or hinder that access, whether in force now or imminently? For instance, are quotas systems/immigration caps in place in your jurisdiction and how are they determined?

Access to talent is indeed a key issue for fintechs and is often cited as the number one issue for those in the sector. The Government have committed to supporting the sector and has acknowledged that it is crucial that the UK remains an attractive destination for this talent. That includes creating an immigration system that the authorities are determined is quick, efficient and welcoming. There are currently no quota systems or caps in place to restrict or limit numbers as the Government's focus is firmly on encouraging tech entrepreneurs to come to the UK – the restrictions only exist within the Immigration Rules themselves, requiring applicants to meet stringent rules and pay substantial costs to work or set up in business in the UK.

The immigration system, as recently adapted and amended, includes many aspects of the sector's successful campaign to engage with Government and emphasises their support and engagement. There have been a number of changes aimed at helping the sector which have come into force since the UK left the EU, notably:

- A two-year post-study work visa, launched as a Graduate route, introduced in summer 2021. This allows UK based graduates to work for 2 years following graduation in an unsponsored capacity – their permission to work based on their student status. However, in light of the high net migration figures released at the end of 2023 the Government have recently confirmed that this route will be reviewed in line with a recently unveiled package of measures designed to bring down net migration. One of those measures is that the Migration Advisory Committee, an independent, non-departmental public body sponsored by the Home Office that advises the government on migration issues, will review the Graduate Route "to ensure it works in the best interests of the UK and to ensure steps are being taken to prevent abuse. This announcement follows on from a ban on students bringing dependants to the UK except for those on postgraduate research routes, effective from 1 January 2024.
- Post Brexit, the authorities removed the cap on talent on Tier 2 general visa routes and removed of the Resident Labour Market Test

 © 2024 Legalease Ltd

which significantly hampered the ability of the tech sector to recruit talent in the past.

Another recently unveiled change is that which allows migrants to switch visas from within the UK. Under the Points-Based System, the Home Office will allow most migrants to apply to switch from one immigration route to another without having to leave the UK. This will support employers in retaining the talented staff that they have invested in and includes the Graduate route.

12. If there are gaps in access to talent, are regulators looking to fill these and, if so, how? How much impact does the fintech industry have on influencing immigration policy in your jurisdiction?

It's worth asking what the most common immigration routes are for tech professionals looking to work in the UK – these are:

Skilled Worker sponsorship

Following Brexit, the Skilled Worker route has become the most commonly used immigration route with over 1,000 sponsor licence applications for skilled staff received by the Home Office weekly. The numbers of employees sponsored under this route has increased greatly. It is a popular choice for tech companies as it is a relatively straightforward way to source a range of skilled staff across different disciplines. Skilled workers can bring dependent family and settle after five years. There are no caps on numbers but there are skills and salary thresholds and vacancies do have to be genuine, among other requirements.

There are also specialised routes and visa categories for tech entrepreneurs or start up founders looking to work in the UK, including:

Global Talent visas

The Global Talent visa is a route which offers a path to citizenship without any need of a job offer for those at the top of their game in certain sectors, including digital technology. It is the most flexible route in terms of employment as it allows successful applicants the ability to be employed, self-employed or both.

However, there is a high threshold to qualify: applicants need to satisfy the UK Government's appointed endorser, Tech Nation, that they are internationally recognised as a leading talent in the digital technology sector. Nonetheless, thousands of tech talents and their families have used this immigration route to settle in the UK and found or work for some of the biggest UK tech brands.

Innovator Founder visas

Another option for tech founders is the new Innovator Founder category, which replaces the Innovator and Start Up routes, removing the old routes' more onerous requirements (e.g. a £50,000 minimum investment for Innovators). Endorsement that a business plan is innovative, viable and scalable is required by a government-appointed endorsing body.

This route is more attractive than its predecessor routes, but the initial endorsement does require more administrative hurdles and transparency than many entrepreneurs may want. In addition, in order to ensure a right to settlement after three years, various business targets must be met too.

UK Expansion Worker

While in most cases firms will need an established, operating business in the UK to sponsor staff to come to work here, under this UK immigration route, an overseas business can send a small team to establish a branch or subsidiary in the UK. Companies established and trading overseas for three years or more can now send up to five employees to set up UK operations. The Home Office will require particular documents regarding the business's UK footprint, overseas trading and business plans to expand in the UK.

Scale-up visa

Tech professionals could also avail themselves of the Scale Up route, which requires sponsorship by an eligible scale-up company. However, the main advantages to this route are a lighter-touch sponsor licence process, no Immigration Skills Charge and, most controversially, after being sponsored for six months, the tech professional can then choose to work for different employers in the UK. Although this may not appeal to sponsors who have gone through the time and cost of sponsoring an individual only to then lose them to another employer, it might be more appealing for tech professionals seeking a greater degree of flexibility.

It's also worth considering what the potential challenges or obstacles tech companies may face when hiring talent in the UK, and how they should look to overcome them? As Britain aims to be a tech superpower, with the UK tech sector continuing to grow in comparison to other European tech hubs, the industry continues to require the best talent from around the world to fuel its growth. The challenges and obstacles facing tech companies hiring foreign talent in the UK include:

 © 2024 Legalease Ltd

Shortage of talent

The tech industry is one of the UK sectors where clients have been constantly facing a skills shortage, and Brexit has only exacerbated the issue. Britain is competing with tech hubs across the world for the best talent and post-pandemic, most of the developing world is experiencing similar skills shortages. In the UK, the US and the EU, vacancies have increased to match or outstrip the availability of people.

Cost

Despite the government's stated ambition of making the UK one of the top global innovation hubs, it has hiked up visa application fees to unprecedented levels and has substantially increased fees payable by all visa applicants: the Immigration Health Surcharge for migrants – from £624 per applicant per year to £1035 per applicant per year. Like all sectors, tech companies looking to hire foreign talent are now facing significantly higher costs of onboarding migrant talent.

The Immigration Skills Charge is paid by employers sponsoring migrant workers coming to the UK for over six months. Where is this money spent? Current figures show that, for the year ended 31 March 2023, the total raised was £586 million. If the money is used for the purpose intended – to upskill the local workforce – the tech industry should really start to see a larger pool of locally trained talent available to hire.

Illegal work

There are significant perils potentially facing tech start-ups who need to move fast. Moving too quickly and hiring individuals to work in the UK without the appropriate immigration permission can result in fines and even criminal penalties for the applicant and their employer; business visitors cannot travel to the UK and start work, and then apply for their visa. This would also certainly impair a tech company's ability to gain permission for employees in the future.

Individuals who do not currently have the appropriate immigration permission allowing them to undertake the specific role in the UK already will have to travel outside the UK and submit their application from their country of nationality (or a country where they hold permission to live and work), and unfortunately, they cannot move to somewhere close to the UK and apply from there. With timing often crucial to fill a tech role, this requirement may further delay a candidate starting work.

13. What protections can a fintech use in your jurisdiction to protect its intellectual property?

The main intellectual property (IP) rights for a fintech company in the UK are patents, confidential information, copyright, database rights and trade marks:

Patents – An invention is capable of being patented in the UK if it is new (compared to earlier matter), involves an inventive step (compared to earlier matter), is capable of industrial application and does not fall within one of the exclusions. These exclusions include a discovery, a scientific theory, a mathematical method, or a program for a computer *"as such"*. However, it is possible to protect a computer program or software as a patent if it involves a technical contribution. The requirement that the invention is new means that inventors should be very careful not to disclose the invention before applying for a patent. A granted patent provides a very powerful monopoly (generally up to 20 years) for the functional claims in the patent.

Confidential Information– In the absence of a non-disclosure agreement (NDA), it is possible to rely on common law protection if the information has the necessary quality of confidence and is not public, is imparted in circumstances importing an obligation of confidence (e.g. due to the relationship of the parties or the circumstances in which the information was disclosed) and there is unauthorised use of that information to the person's detriment. There is also the Trade Secrets (Enforcement, etc.) Regulations (derived from EU law) which includes a definition of a trade secret and makes it the acquisition, use or disclosure of a trade secret unlawful if it constitutes a breach of confidence in confidential information. Confidentiality agreements, provisions and NDAs would be preferable than relying on these rights as it can be more certain what information is to be kept confidential and it can be easier to prove that the information is confidential. Such protections may be preferred to patent protection in circumstances where the fintech company wants to keep the information confidential forever (as a patent will explain exactly how the invention works and will be available to use after the 20 year protection).

Copyright – Copyright does not protect ideas themselves but rather certain types of works in which an idea is expressed, such as literary works (e.g. a computer program, source code, object code, preparatory design material for a computer program, a table or compilation, the selection/arrangement of a database) or artistic works (e.g. a graphic work, photograph, drawing, diagram, chart, screen displays). Therefore, numerous different types of copyright can subsist in one work. There is no registration system for

 © 2024 Legalease Ltd

copyright in the UK and instead copyright is granted automatically if certain requirements are met. For example, a literary or artistic work must be original, recorded in writing or otherwise (this is not a requirement for a literary work but such a work would be recorded anyway) and the qualification requirements must be met (e.g. by reference to the author or country in which the work was first published). Copyright lasts for a very long time (70 years plus the life of the author for literary and artistic works). Copyright in a literary or artistic work is owned by the author/creator of the work unless it was made by an employee in the course of that person's employment (in which case the employer will be the owner). Therefore, it is important that fintech companies have IP agreements with third parties (e.g. contractors). In general terms, it is an infringement to copy the whole or a substantial part of a copyright work without the owner's permission.

Database (sui generis) rights – This right can protect the contents of a database (copyright instead can protect the selection/arrangement of a database) if there has been a substantial investment in obtaining, verifying or presenting the contents of the database and if the maker of the database meets the qualification requirements. The owner of the database is the person who takes the initiative in obtaining, verifying or presenting the contents of a database and assumes the risk of investing in that obtaining, verification or presentation (unless it was by an employee in the course of employment). This right lasts for 15 years from making the database or making the database available to the public unless there are substantial changes to the contents (as this grants that investment its own term of protection). It is an infringement to extract or re-utilise all or a substantial part of the contents of the database without permission.

Trade Marks– The name or logo of the fintech company may be the first thing that customers see as they look for the relevant company. Therefore, it is important that (where possible) they are protected as trade marks in the relevant territories for the relevant goods/services (terms that are descriptive for the goods/services will be difficult to protect). Trade marks last for 10 years but can be renewed indefinitely. Once registered, they can protect against later identical or similar marks which are used for (or trade mark applications that include) identical or confusingly similar goods/services. If a trade mark is not registered then it may be possible to rely on the unregistered right of passing off, although this can be more difficult. For example, rather than relying on a trade mark certificate, the elements of goodwill, misrepresentation and damage need to be proved to establish passing off.

Registered Designs – A logo or, for example, a unique design of a graphical user interface may be protectable via a UK registered design if it is a design, it is new (there is no earlier identical design or design differing in immaterial details), it has individual character (it produces on the informed user a different overall impression from any earlier design) and it does not fall within one of the exclusions. UK registered designs can last for up to 25 years and grant the owner the right to prevent a design that produces on the informed user the same overall impression.

The two main courts for IP disputes are the High Court and the Intellectual Property Enterprise Court (IPEC) and the general rule is that the 'loser' of the litigation pays (the majority of) the 'winner' of the litigation's costs. The IPEC has a cost cap of up to £500,000 in compensation and £60,000 in legal costs and its relatively quicker process means it can be an attractive court for claims of lower value that are seeking a quicker resolution. Oppositions, cancellations or challenges to trade marks and designs are dealt with via the UK Intellectual Property Office.

14. How are cryptocurrencies treated under the regulatory framework in your jurisdiction?

The way in which cryptocurrencies are treated under the UK's regulatory framework is rapidly evolving. Cryptoasset businesses offering services both *from* and *into* the UK are potentially caught by the framework.

Firms engaging in crypto-related activities should be aware of the current (and pending) changes to the current regulatory landscape, including, for example, that:

(a) activities that use, reference, exchange or deal in cryptocurrencies, can require regulatory authorisation (for example, under the existing non-crypto-specific regime), or even be prohibited;

(b) firms providing certain cryptoasset services (including exchange and wallet services) by way of business in the UK must register with the FCA under the anti-money laundering rules;

(c) to lawfully communicate the promotion of "*qualifying cryptoassets*" to UK consumers, firms in the UK or overseas must comply with the new cryptoasset financial promotions rules;

(d) the Financial Services and Markets Act 2023 ("**FSMA 2023**"):

 © 2024 Legalease Ltd

- introduces a new designated activities regime ("**DAR**") that can be applied to cryptoassets;
- creates a legislative framework to bring cryptoassets within the scope of the existing financial services regulatory regime (the government have indicated that certain activities could be in scope from 2024); and
- enables the UK government to introduce regulation in relation to recognised payment systems that include arrangements using digital settlement assets ("**DSA**") (including stablecoin), recognised DSA service providers, and service providers connected with, or providing services in relation to, these payment systems and DSA service providers.

A. The general (non-crypto-specific) UK regulated activities regime

Under the general, non-crypto-specific, regulated activities regime, certain activities (for example, advising or managing) cannot be carried on in the UK in relation to certain investments (for example, shares or bonds – otherwise known as "*specified investments*") without appropriate authorisation or exemption. The principal provisions regarding the regulated activities regime are contained in:

- the Financial Services and Markets Act 2000 ("**FSMA**"), which is the key statute governing financial regulation in the UK and contains, in section 19, the "*general prohibition*" on unauthorised persons carrying on regulated activity in the UK unless they are an exempt person (by virtue of being an appointed representative of another authorised firm) or an exclusion is available; and
- the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 ("**RAO"**), which contains definitions of the regulated activities and exclusions. Under FSMA it is an offence for a (legal or natural) person to carry on regulated activities in the UK unless it is authorised, or an exemption applies.

Non-compliance with the regulated activities regime may lead to criminal, civil or regulatory penalties. This may include criminal prosecution, contracts being deemed void, voidable or unenforceable, fines being issued against firms and individuals, and/or the FCA using its wide-ranging enforcement powers to prescribe, restrict or suspend the activities of firms.

The extent to which the general, non-crypto-specific, regulated activities regime applies to cryptocurrencies depends on whether cryptocurrencies fall within the definition of a specified investment. This is generally determined on a case-by-case basis and depends heavily on the defining characteristics of the cryptocurrency and the nature of the proposed activity. For example, certain cryptocurrencies may have the characteristics of securities or other financial instruments; or the structure of a specific arrangement may mean that a cryptoasset business is operating a collective investment scheme or providing some other kind of regulated investment service. Cryptocurrency derivatives are a common example of a cryptocurrency which would be deemed a specified investment, meaning that firms carrying on activities in respect of cryptocurrency derivatives need to be appropriately authorised to do so (see also *Expansion of the general regime* below).

Activities relating to cryptocurrencies may also be caught under other regulatory frameworks, not strictly designed with cryptoassets in mind. For example, certain cryptoassets may have the characteristics of electronic money, and therefore be caught within the scope of the Electronic Money Regulations 2011 (the "**EMRs**").

B. Regulatory regimes specifically applicable to cryptocurrencies

Expansion of the general regime

FSMA 2023 has extended the definition of "*specified investment*" under FSMA to include "*any asset, right or interest that is, or comprises or represents, a cryptoasset*". Whilst cryptoassets are not yet included in the list of "*specified investments*" in the RAO, the UK government announced its intention to move forward with the expansion of this list to cryptoassets in a response to its consultation released in October 2023 (see *Future regulation of cryptocurrencies* below).

Regulation of digital settlement assets

FSMA 2023 has also introduced provisions that enable increased regulatory control of DSAs, including stablecoins, as well as wider forms of digital assets used for payment and settlement. FSMA 2023 enables the UK government to introduce regulation in relation to: (i) recognised payment systems that include arrangements using DSAs; (ii) recognised DSA service providers, and (iii) service providers connected with, or providing services in relation to, these payment systems and DSA service providers (again see *Future regulation of cryptocurrencies* below).

Ban on offering of cryptoasset derivatives to retail customers

Since 6 January 2021, there has been a ban on the offering of cryptoasset derivatives and cryptoasset

 © 2024 Legalease Ltd

exchange traded notes to retail clients. This ban was implemented to protect consumers from harm, calm volatility, and reduce the risk of financial crime, and reflects a sometimes inadequate understanding of cryptoassets by retail consumers.

Anti-money laundering ("AML") and counter-terrorism financing ("CTF") regime.

Firms providing certain cryptoasset services by way of business in the UK must register with the FCA under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the "**Money Laundering Regulations**").

The cryptoasset services that the registration requirement will apply to include:

- Cryptoasset exchange providers – including firms that exchange, arrange, or make arrangements with a view to the exchange of (i) cryptoassets for money or money for cryptoassets; and/or (ii) one cryptoasset for another. It also includes firms operating cryptoasset ATMs.
- Custodian wallet providers – this includes firms that safeguard (and/or administer) cryptoassets on behalf of customers (or private cryptographic keys on behalf of customers in order to hold, store and transfer cryptoassets).

The registration process is onerous and requires a firm to provide detailed information about its operations, compliance procedures, and AML risk assessments. Registered firms must comply with ongoing regulatory obligations, for example, in relation to customer due diligence, reporting and record keeping.

The FCA have shown a willingness to take enforcement action against firms that fail to register or to otherwise meet their AML/CTF obligations (criminal sanctions are also possible).

In addition, a person or firm wishing to acquire or increase (direct or indirect) control of a cryptoasset firm registered with the FCA under the MLRs must now submit a change in control notification to the FCA and await their approval before completing the transaction. Failure to obtain this approval is a criminal offence.

The expansion of this regime gives the FCA the power to assess the "*fitness and propriety*" of persons (in the UK or abroad) that control FCA-registered cryptoasset firm. It also gives the FCA the ability to object to the transaction going ahead, and if an objection is made, to make its reasons for objecting public.

Financial Promotions regime

As of 8 October 2023, the UK's financial promotion rules were extended to "*qualifying cryptoassets*" (which notably would include cryptocurrencies). In order to lawfully communicate a cryptoasset promotion, firms must either:

- be registered with the FCA under the Money Laundering Regulations;
- be authorised by the FCA;
- have the promotion approved by a person authorised by the UK; or
- fall within specific exemptions.

Additionally, cryptoasset promotions made to UK consumers will now need to meet requirements under the UK financial promotion regime (including the requirement to be fair, clear, and not misleading), and must include risk warnings in order to ensure that consumers are informed about the potential risks of investing in cryptoassets. These new rules also impose a ban on cryptoasset promotions that include monetary or non-monetary benefits that incentivise investment.

Notably, these financial promotion rules will apply to all firms (in the UK, EU and elsewhere overseas) marketing cryptoassets *in or to the UK*.

All firms marketing cryptoassets to UK customers must understand (and comply with) the new rules. The FCA have said it will be taking robust action against anyone who falls foul of these new rules, and issued 146 alerts about cryptoasset promotions on the first day of the new regime.

Designated Activities Regime ("DAR")

FSMA 2023 introduced the DAR for the regulation of certain "*designated*" financial markets activities. This new regime applies to "*investments*", which, under FSMA 2023, now includes cryptoassets.

Persons carrying out designated activities will not need to be FCA-authorised or meet threshold conditions, but they will be required to follow the regulators' rules in relation to the specific designated activity itself. This may include, for example, requirements relating to reporting, trade-related restrictions, or public disclosures.

At present, no activities have been designated in relation to cryptocurrencies. However, in a consultation released in February 2023, the UK government expressed its intention to create new designated activities tailored to

 © 2024 Legalease Ltd

the cryptoasset market. Cryptocurrency firms should stay up to date with developments in relation to this regime.

C. Future regulation of cryptocurrencies

As noted above, the UK government announced its intention to move forward with its proposals to bring cryptoassets within the scope of the existing financial services regulatory regime in a response to its consultation released in October 2023.

In this response, the UK government sets out its plans to regulate activities relating to cryptoassets in the following 2 phases:

Phase 1 – Activities relating to fiat-backed stablecoins

The UK government intends to bring activities relating to fiat-backed stablecoins within the scope of the UK's existing regulatory regimes by: (a) bringing the activities of issuance and custody of fiat-backed stablecoins (where the coin is issued in or from the UK) within the existing regulatory perimeter of the RAO; and (b) bringing the use of fiat-backed stablecoins in payment chains into the Payment Services Regulations 2017.

The UK government stated that, "*subject to parliamentary time*", it intends to effect these changes as soon as possible, and by early 2024.

Phase 2 – Activities relating to other types of cryptoassets

Similarly, to phase 1 above, the UK government intends to effect the inclusion of other cryptoassets within the list of "specified investments" in the RAO in 2024 (again, "*subject to parliamentary time*").

If the UK government continue to regulate phase 1 and/or phase 2 activities as proposed, firms carrying on activities involving cryptoassets will need to ensure that they have the appropriate authorisation and are following the relevant rules and requirements. The UK government has stated that FCA authorisation will not be automatically granted to firms that are registered with the FCA under the AML and CTF regime.

Other guidance and policy statements

In May 2022, the UK government released a consultation setting out proposals to adapt the Financial Market Infrastructure Special Administration Regime ("**FMI SAR**") to apply to DSA firms. In its response to this consultation, the UK government confirmed that overall, respondents were broadly supportive of the proposals in its consultations, and that next steps will include: (i) the Bank of England considering whether further guidance on the operation of the FMI SAR is necessary; and (ii) updating stakeholders. Firms dealing with stablecoins or other forms of DSAs should keep a watchful eye on developments in this area.

15. How are initial coin offerings treated in your jurisdiction? Do you foresee any change in this over the next 12-24 months?

Initial coin offerings ("**ICOs**") – i.e., the initial release of a new cryptoasset, coin or token to the retail market – saw a surge in popularity in the autumn and winter of 2017 as a method of fundraising akin to crowdfunding, typically for the pre-purchase of cryptoassets on platforms that typically have not been built yet, at a discounted price. There were a huge number of ICOs carried out in many different jurisdictions, that raised vast amounts, and not infrequently on the back of vague or even entirely unfounded promises of technical development. Amongst those were a number of genuinely good offerings, but a relatively small proportion of those ICOs launched products with the cryptoasset as a core, and widely adopted means of value storage or transfer.

Through spring and summer of 2021, a different type of ICO has seen a similar surge in popularity and allocation of capital seeking returns: non-fungible tokens ("**NFTs**") representing ownership or licences over images, songs or other digital assets. There are similar themes: a large number of projects, but only a small portion gaining traction or widespread adoption. A major difference between the 2021 NFT popularity, compared to the 2017 ICO popularity, is a larger number of traditional businesses launching "NFT coins", using it as a new way to interacting with customers and fans.

The vast majority of ICOs are not currently financial regulated offerings, since most cryptoassets do not quite fall within the current list of "specified investment" under the RAO (which has not yet been expanded to reflect FSMA 2023 – see Question 14 *Expansion of the general regime* above). However:

- ICOs which offer tokens that constitute securities would be caught within the UK's existing regulatory regime, and therefore require that a firm complies the UK's Prospectus Regime as with normal share offerings; and
- the launch of a new coin may make result in a firm being deemed a cryptoasset exchange for the purposes of the Money Laundering

 © 2024 Legalease Ltd

Regulations, triggering registration requirements for the firm.

Over the next 12-24 months, we would expect there to be significant developments in respect of how ICOs are treated in the UK. This is largely due to the UK government's response to its consultation released in October 2023 (as referenced above) in which it sets out plans to regulate the making of a public offer of cryptoassets.

Broadly, the UK government intends to establish an issuance and disclosure regime for cryptoassets grounded in the intended reform of the UK Prospectus Regime: the Public Offers and Admissions to Trading Regime ("**POATR**") and tailored to the specific attributes of cryptoassets. For tokens made available through an ICO, disclosure requirements and exemptions will likely be similar to those proposed in the new draft POATR. Such exemptions would therefore be expected to include offers of free cryptoassets (e.g., via an airdrop or similar distribution mechanism) or offers made only to professional / sophisticated investors.

In its response, the UK government made clear that firms will still need to consider obligations around cryptoasset financial promotions for tokens which are exempted from, or out of scope of, the proposed cryptoasset issuance and disclosure regime.

16. Are you aware of any live blockchain projects (beyond proof of concept) in your jurisdiction and if so in what areas?

There are many live operating blockchain projects within England and Wales. Blockchain technologies have been used in respect of equity issuance (Globacap), venture capital (Outlier Ventures), custodial wallet services (Argent), digital asset trading (Archax), central depository services (SETL), AML (Elliptic), regulated customer communications (docStribute), and more.

17. To what extent are you aware of artificial intelligence already being used in the financial sector in your jurisdiction, and do you think regulation will impede or encourage its further use?

Artificial intelligence ("**AI**") has been used in the financial sector for decades, with some of the most high-profile early use cases being the use of AI in data analysis, stock algorithms, and scenario modelling in connection with trading in financial markets.

Like almost every other sector that interacts with or relies upon technology, use of AI in the financial sector in the UK has spread ever wider with adoption rates continuing to rise. A Bank of England and Financial Conduct Authority report on a survey into the state of machine learning in UK financial services (published 11th October 2022 and available here) found that 72% of firms who responded to the survey were using or developing machine learning applications.

The survey suggested that banking was the most influenced financial sector, followed by insurance with the leading use cases being in customer engagement, risk management and compliance, and miscellaneous business areas (e.g. HR, legal). Prominent use cases of machine learning amongst respondents were in insurance pricing and underwriting, credit underwriting, marketing, fraud prevention, and anti-money laundering.

Predictive rather than generative AI has been the dominant force in the take up of AI in the UK financial sector. This is no surprise given that a strong suit of predictive AI is in pattern recognition and identifying the divergence from recognised patterns. AI providers supporting the financial sector therefore offer systems such as those aligned to payment authentication, reducing the threat from inbound emails with active threat detection, or spotting anomalies and suspicious activity in trading patterns.

Take up of generative AI has been slower, despite the explosion of interest prompted by the developments of chatbots such as ChatGPT. Generative AI is generally seen as a new horizon with interest for its use mostly focused on process automation, sales and customer service functions (including customer support chatbots). However, with the well published risks that generative AI brings with it, firms are generally taking a risk based approach to take up to attempt to offset or mitigate risks such as imbedded model bias and hallucination of patterns and features in relation to data sets.

Governing bodies and legislators around the world are becoming increasingly aware of the potential harms that could be caused by AI (mostly thanks to the tsunami of generative AI systems) with the consequence of AI or technologies incorporating AI attracting regulatory attention.

In the UK, the UK Government held a high profile AI Summit on 2 November 2023 to consider the future of AI technologies; many leading technology companies attended. The Prime Minister, Rishi Sunak, used the Summit as a platform to demonstrate the UK's approach to AI which was said to be fourfold:

i. developing a shared international

 © 2024 Legalease Ltd

understanding of the risks presented by AI and agreeing the first ever international statement about the nature of those risks (which was signed by each nation who attended, including the US and China);

ii. the formation of a global expert panel to produce a State of AI Science report, production of the inaugural report will be chaired by Yoshua Bengio, a Canadian computer scientist noted for his work on artificial neural networks and deep learning;

iii. international collaboration on testing the safety of new AI models before they are released through the creation of an AI Safety Institute which will leverage public sector capability to test the most advanced frontier AI models in order to evaluate future generations of AI models before they are widely deployed; and

iv. establishing a series of future international AI safety summits to continue the collaboration achieved during the Summit, Korea and France have agreed to host further summits in 2024.

The message from London is that there is no immediate appetite to regulate AI technologies (other than an Autonomous Vehicle Bill raised in the Kings' inaugural Speech on 7 November 2023), with Downing Street opting to assess the risks presented by emerging technologies first.

However, whilst there is no immediate indication that the UK Government will be rushing to put legislation in place around AI technologies (other than autonomous vehicles), businesses providing or using AI technologies or the outputs of those technologies in both the UK and the EU (including to EU users from the UK) will need to be aware of the impending EU AI Act with the EU Council and Parliament reaching provisional agreement on the draft Act in December 2023, which will have extra-jurisdictional effect meaning that providers or developers who place AI technologies or the output of those technologies on the market or put them into service in the EU will be caught by the Act (in relation to their EU business) even if they are established elsewhere.

The draft AI Act aims to set a global standard for AI regulation, placing obligations on providers, classifying AI technologies by perceived risk, and prohibiting certain technologies altogether. Amongst the interim list of high-risk technologies (which attract the most onerous requirements on the developer/provider under the Act) are AI systems which use biometric identification and categorisation of natural persons and AI systems which are intended to be used to evaluate the creditworthiness of natural persons or to establish their credit score, each of which could be incorporated in fintech technologies.

Given the hefty fines that may be levied for breaches of the EU AI Act, firms should assess which of their AI systems are likely to be high-risk and conduct a gap analysis against their forthcoming requirements under the Act. This will help firms understand the scale of the effort (including any technological changes required) in order for firms to ensure compliance with the Act once in force.

Other than the impending EU AI Act, providers, developers, and users of AI technologies should also be aware of their data protection obligations under the EU GDPR (where data sets include personal data of EU citizens) and the UK GDPR when processing personal data, particularly any such personal data being used to train models for the benefit of the provider/developer.

18. Insurtech is generally thought to be developing but some way behind other areas of fintech such as payments. Is there much insurtech business in your jurisdiction and if so what form does it generally take?

There is a well-established Insurtech business sector in the UK.

So far, the focus has tended to be on the distribution of life and general insurance contracts to consumers, and SMEs. Insurtechs in this part of the market are still developing new ways to make more bespoke insurance products available to a wider range of customers. This often means that it is quicker, easier, and more fun to buy a bespoke policy from an Insurtech than to buy a standard policy from a traditional insurer. The premiums can also be much lower too. This is partly about product innovation. It is also about automation, the stripping out of distribution costs, and using technology to more accurately price and adjust individual risks and premiums, something that often relies on data analytics and gamification to encourage policyholders to proactively reduce their individual insurance risks, in ways that also reduce their premiums.

Insurtechs are also working with insurers and reinsurers on the development, and to improve the take up, of parametric polices. Where they are available, these policies can materially reduce the insurer's claims processing costs, and give policyholders the fastest possible access to their claims money, so they can more quickly and easily recover if disaster strikes. This has

 © 2024 Legalease Ltd

been especially useful for policyholders facing natural disaster risks, but Insurtechs are looking for other opportunities besides.

We are still seeing developments in back-office Insurtech products that make it quicker and easier for insurers to (for example) (a) receive, process and settle valid claims; (b) identify and reject fraudulent and exaggerated claims; or (c) meet their PRA / FCA regulatory obligations as and when they arise.

New insurers are still rare in the UK, but the regulators are looking for ways to make it quicker, easier, and less expensive, to establish new insurers than it used to be. In the meantime, entrepreneurs are using alternative distribution models to bridge the gap.

19. Are there any areas of fintech that are particularly strong in your jurisdiction?

It would be difficult to point to any area of fintech that is particularly stronger than another within the UK, given the strong presence of fintech businesses across the board. Fintechs are active within the business and consumer credit space, payments (including account information services and the services built on this), e-money (including e-money as a means to authorisation by challenger banks), robo-advice, crypto and insurtech. The UK's financial regulatory system is effective in enabling products and service offerings across a wide range of regulated services, facilitating innovation across the financial sector.

20. What is the status of collaboration vs disruption in your jurisdiction as between fintechs and incumbent financial institutions?

The beginnings of fintech in the UK were largely hyped as being about disruption, and at the time this was largely true: challenger banks and international money transfer businesses dominated the headlines. However, the market has now matured into three main sections. First are the genuine disruptors: those who take something that the incumbent financial institutions already do, and do it faster, cheaper or in some way better – and steal market share by doing so. These include international money remittance providers and challenger banks. Second are probably the largest group overall, the suppliers: these are the companies supplying services to other financial institutions in order to help those institutions do something that they do already, but do it better. There are obviously a great many options here, but by way of example only this could include data gathering and analytics, onboarding / ID verification technology, or regtechs that help institutions to maintain compliance with their regulatory obligations. Third are arguably the most significant group in terms of the overall effect on the financial system, the niche-fillers. These are the companies that are doing something that no one else was doing before. This covers a broad range of services, from funding platforms that service loans that the incumbent banks would not normally take on, to companies that produce digital receipts for store purchases to companies that choose to offer traditional banking services in a way that makes them more accessible to people who normally find it difficult to get a bank account. In relation to the first category, collaboration is naturally less likely. However, the second and to a large extent the third categories lend themselves to collaboration. An incumbent financial institution can benefit from new innovations of suppliers without having to create them itself, and can partner with niche-fillers to participate in markets that were previously closed to them. It is in this context that we have seen the most activity and change over the past few years, as incumbents become more skilled at adapting their contracting and procurement processes to the start-up world.

In our experience there is still quite some way to go with many of the banks, but it is now far easier for a start-up to partner with a UK bank than it was even a few years ago. A significant recent step in the field of collaboration is the release by the British Standards Institute of a guide on "Supporting fintechs in engaging with financial institutions". This document was created by five of the UK's biggest banks and a number of leading fintechs, led by Tech Nation and the Fintech Delivery Panel, to act as a guide for fintechs who may be unfamiliar with the procurement processes and concerns of financial institutions on how best to approach the various issues that typically come up in a "partnering process". It is an excellent guide that any fintech should read, it is to our knowledge the first of its kind in the world where a number of major banks have come together to try to facilitate better collaboration with fintechs. There is an argument that similar guidance is needed for institutions to further improve their processes and strategy in order to partner with fintechs effectively, as unnecessarily burdensome documentation, policies and sign-off processes often stand in the way effective partnering – efforts are being made by some institutions in this direction but there are significant further improvements that could be made. The institutions that get the partnering process right stand to gain significant competitive advantage over their peers in the acquisition of new functionality for their customers.

 © 2024 Legalease Ltd

21. To what extent are the banks and other incumbent financial institutions in your jurisdiction carrying out their own fintech development / innovation programmes?

A number of incumbent financial institutions (including both banks and insurance companies) are actively involved in running fintech programmes and accelerators. Most of the major retail banks run an innovation or accelerator programme of some kind, often teaming up with tech consultancies. In addition, many of the banks and insurance companies now have their own specific innovation function which is tasked with finding and partnering with fintechs that will be useful for their business.

As this guide goes to press, HSBC will have launched its own fintech app, Zing, which aims to compete in the lucrative money transfer market with the likes of Revolut and Wise. We understand that HSBC have white-labelled the technology from another fintech, rather than build the technology in-house. It remains to be seen whether this 'fintech launched by an incumbent' is successful in challenging the 'incumbent' fintechs!

22. Are there any strong examples of disruption through fintech in your jurisdiction?

The UK boasts many examples of fintechs disrupting the traditional financial, payments and insurance systems. The UK has seen more challenger bank activity than other regions, hosting Atom Bank, Tandem Bank, Monzo (the first online-only challenger bank to obtain a full banking licence) Monese, Pockit, Starling, Tide and Revolut, among others. A number of these have already obtained a full banking licence whilst others have followed the path of first obtaining an e-money licence. The implementation of the second Payment Services Directive ((EU) 2015/2366) paved the way for a host of providers of account information services ("**AISPs**") and, to a lesser extent, payment initiation services providers ("**PISPs**"). Notably, UK AISPs have taken the initial regulatory description of provision of account and transaction data from multiple accounts to a consumer and elaborated on this, developing innovative uses for this data to bring new fintech products to market, whether by improving on existing processes or creating new offerings. For example, AISPs are currently using account and transaction data to speed up the process of evaluating SME and consumer credit eligibility, thus streamlining the process of obtaining loans. Providers of accounting services use access to account data to provide faster and more accurate accounting services to their users. Other uses of AIS include innovative applications such as automated loyalty point and cashback provision. This space has also seen the growth of intermediary providers of account data, such as TrueLayer, Plaid and Yapily, who are registered as AISPs and provide AIS as a service to third parties in the fintech space who then use the data to provide services to end-users. Other areas in which UK fintechs lead run the gamut from robo-advising and app-based investing (Nutmeg (now acquired by JP Morgan) and Wealthify), peer-to-peer money remittance (Wise), business-to-business lending (Funding Circle), providers of SME small- and micro-loans (iwoca), identity-verification (Onfido, Yoti), peer-to-peer lending (Zopa), invoice factoring (Kriya), and open banking (Fractal Labs, Fluidly).

 © 2024 Legalease Ltd

Contributors

Jonathan Segal
Partner
jsegal@foxwilliams.com



Chris Hill
Partner and Fintech Lawyer
chill@foxwilliams.com



Mardi MacGregor
Partner
mmacgregor@foxwilliams.com



Peter Finch
Partner
pfinch@foxwilliams.com



Kolvin Stone
Partner
kstone@foxwilliams.com



Sacha Schoenfeld
Partner
sschoenfeld@foxwilliams.com



The authors would like to thank Stewart Cook, Richard Aitchison, Bryan Shaw, Scott Steinberg, Emma Bailey and Chris Finney for their contributions.

 © 2024 Legalease Ltd