ICLG

The International Comparative Legal Guide to:

Fintech 2018

2nd Edition

A practical cross-border insight into Fintech law

Published by Global Legal Group, with contributions from:

A&L Goodbody
Advokatfirmaet BAHR AS
Anderson Mōri & Tomotsune
Anjarwalla & Khanna
Appleby
ATZ Law Chambers
Bär & Karrer Ltd.
BBA
BonelliErede
Bonn Steichen & Partners
Bredin Prat
De Brauw Blackstone Westbroek
ENSafrica
Erciyas Law Office
Etah-Nan & Co, Attorneys
Evris Law Firm
Galicia Abogados, S.C.
Gilbert + Tobin
Gleiss Lutz
Goldfarb Seligman & Co.
Gorrissen Federspiel
GVZH Advocates
Haiwen & Partners
ISOLAS LLP
Kim & Chang
Lee and Li, Attorneys-at-Law
Mannheimer Swartling
Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados
McMillan LLP
MinterEllisonRuddWatts
QUORUS GmbH
Rahayu and Partners Law Offices in Association with HFW
Romulo
Roschier, Attorneys Ltd.
Shearman & Sterling LLP
Shearn Delamore & Co.
Shook Lin & Bok LLP
Slaughter and May
Trilegal
Udo Udoma & Belo-Osagie
Uría Menéndez
Uría Menéndez – Proença de Carvalho
Wilmer Cutler Pickering Hale and Dorr LLP
WKB Wierciński, Kwieciński, Baehr
Yale Law School

glg
global legal group

global legal group

Contributing Editors
Rob Sumroy and Ben Kingsley, Slaughter and May

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Jane Simmons

Senior Editors
Suzie Levy
Caroline Collingwood

CEO
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Stephens & George
Print Group
May 2018

ISBN 978-1-912509-08-9
ISSN 2399-9578

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Continued Overleaf →

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

EDITORIAL

Welcome to the second edition of *The International Comparative Legal Guide to: Fintech*.

This guide provides corporate counsel and international practitioners with a comprehensive worldwide legal analysis of the laws and regulations of fintech.

It is divided into two main sections:

Three general chapters. These chapters provide an overview of artificial intelligence in fintech, the regulation of cryptocurrency as a type of financial technology, and fintech and private equity.

Country question and answer chapters. These provide a broad overview of common issues in fintech laws and regulations in 44 jurisdictions.

All chapters are written by leading fintech lawyers and industry specialists and we are extremely grateful for their excellent contributions.

Special thanks are reserved for the contributing editors Rob Sumroy and Ben Kingsley of Slaughter and May for their invaluable assistance.

The *International Comparative Legal Guide* series is also available online at www.iclg.com.

Alan Falach LL.M.

Group Consulting Editor

Global Legal Group

Alan.Falach@glgroup.co.uk

United Kingdom

Rob Sumroy

Ben Kingsley

Slaughter and May

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

London is consistently ranked as one of the most 'fintech-friendly' cities in the world and, as such, a broad spectrum of fintech business is represented both in London and the UK more widely. The UK was an early adopter of payments technology and this market is now reaching a degree of maturity. Likewise, the sharing economy and crowdfunding are well-established in the UK, but we would expect both of these areas to continue to grow.

Open Banking, an initiative led by the UK Competition and Markets Authority, was launched in January 2018, and refers to a secure set of technologies and standards that allow customers to give companies other than their bank or building society permission to access their accounts securely. This is expected to translate into an emerging market of new third-party online service providers.

Big Data continues to be an important area of innovation and research both for start-ups and established financial services firms. We expect that an increasing capacity to analyse and use Big Data will dovetail with the rapidly developing Internet of Things to, for example, provide financial services firms (such as insurers) more complete sources of customer data. One other emergent sub-category of fintech in the UK, is regtech – tools and services to automate compliance tasks, which continues to gain momentum.

In 2017, we continued to see significant growth in the application of fintech to asset management, in particular, the use of robo-advice, which is increasing in both sophistication and prevalence (at least one UK retail bank launched a fully regulated robo-advice proposition in 2017).

The discussion surrounding blockchain technology continues, with much recent dialogue focussed on the use of bitcoin and other cryptocurrencies and the related topic of ICOs, which continues to attract global regulatory scrutiny. Although blockchain technology is yet to make a meaningful practical impact on the UK fintech landscape, the broad range of possible use cases and the high level of disruption expected from the application of the technology is now widely recognised.

Progress of, and investment into, the UK's fintech sector has continued since the UK voted to leave the EU with statistics showing that total capital invested into UK fintech in 2017 comfortably exceeded 2016 levels.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

There are currently no prohibitions or restrictions that are specific to fintech businesses in the UK.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

The UK has mature debt and equity capital markets accessible to businesses above a certain size. For example, raising finance through an IPO has been a popular avenue for certain fintech businesses in recent years (see further our answers to questions 2.3 and 2.4 below). However, even for those fintech businesses which are not yet in a position to raise finance through these 'traditional' routes, there are a number of funding sources available in the UK once the resources of 'family, fools and friends' have been exhausted.

Equity

Early stage, venture capital, funding before it is possible to put a valuation on a company is often done through a form of convertible loan note. The loan becomes convertible into equity on the occurrence of certain events such as a material funding round, exit event or an IPO, usually at a discount to the value per share applied by such event. Investments in loan notes will not qualify for certain tax reliefs, including SEIS and EIS described in question 2.2 below. An alternative to the convertible loan note, structured so as to qualify for such reliefs, is the advanced subscription agreement, whereby the investor subscribes for future equity determined by reference to the relevant trigger event.

As a company matures, it will typically undergo a series of equity fundraisings.

Crowdfunding, where members of the public pool resources through an intermediating platform (typically in exchange for shares), is

growing in popularity in the UK for start-up businesses. In particular, it offers private investors an opportunity to invest in early-stage businesses which would previously have only been accessible to business angels or venture capitalists. The UK crowdfunding sector is well-established and growing in size and, as such, it is sometimes possible to raise substantial sums. The mobile bank Monzo raised £2.5 million in a second crowdfunding campaign in 2017, while challenger bank Revolut raised £3.9 million. Many fintech start-ups have combined crowdfunding finance with finance raised from more traditional sources, such as from venture capital and business angels. Incubators, which generally offer facilities and funding for start-ups in return for an equity stake, are also increasingly prevalent in the UK and may present an attractive option to small and growing fintech businesses.

Debt

Whilst small businesses are unlikely to have recourse to 'traditional' bank loans, there are more niche banks such as Silicon Valley Bank and OakNorth Bank which specifically provide debt finance to tech start-ups. There are also numerous peer-to-peer lending platforms and invoice financing firms operating in the UK, which provide alternative sources of debt finance to small and growing businesses.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

The UK Government offers the following tax incentives for investment in start-ups:

- The Seed Enterprise Investment Scheme (SEIS) offers a 50% income tax relief for UK taxpayers investing up to £100,000 in qualifying start-ups. A company can raise no more than £150,000 in total via SEIS investment. To qualify for SEIS, a company must be no more than two years old, have assets of less than £200,000 and have fewer than 25 employees. This complements the Enterprise Investment Scheme (EIS) which offers tax relief for investment in higher-risk small companies, though the tax relief available under the EIS is less than under the SEIS.
- R&D tax credits of up to 230% for certain companies with fewer than 500 employees.
- The Patent Box Scheme, which allows companies to apply a lower rate of Corporation Tax to profits earned from patented inventions.

It should be noted that these incentives are not specific to the tech or fintech sectors and are generally available to qualifying companies and investors in all sectors.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The precise conditions depend on the type of listing and the market on which the shares will be listed. A premium listing on the main market of the London Stock Exchange will, for example, entail more onerous requirements than a listing on the more junior Alternative Investment Market.

In summary, a standard listing on the main market of the London Stock Exchange would require compliance with the following key requirements:

- The company to be duly incorporated, validly existing and operating in conformity with its constitution and its shares to comply with the laws of the company's place of incorporation, duly authorised and have all necessary statutory and other consents.
- The company's shares to be freely transferable and free from any restrictions on the right of transfer.
- A minimum market capitalisation of £700,000.
- The company to publish an approved prospectus.
- The company to ensure that at least 25% of its shares are in public hands.

In contrast, to list on the Alternative Investment Market, there are no requirements in respect of the percentage of shares to be in public hands or market capitalisation and, in certain cases, no requirement for admission documents (such as the prospectus) to be pre-vetted by the market or UK regulators.

To obtain a premium listing on the London Stock Exchange, a company would need to comply with requirements additional to the standard listing requirements above, such as supplying three years of audited financial accounts and demonstrating a sufficient revenue-earning record and working capital.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

A notable example from the past 12 months is that of Alfa Financial Software, a London-based fintech firm, which listed on the London Stock Exchange in June 2017 and was valued at close to £1 billion. The UK's largest ever fintech IPO is Worldpay, the payments processor, which floated on the London Stock Exchange in 2015 valued at £4.8 billion.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

There is no specific regulatory framework for fintech businesses, which are subject to the existing body of UK financial regulation. Fintech firms will fall within the regulatory perimeter if they carry on certain regulated activities (specified in legislation) by way of business in the UK and do not fall within the scope of an exemption. This regulatory perimeter covers 'traditional' financial services, such as provision of banking, consumer credit and insurance services, as well as certain areas more typically associated with fintech start-ups, such as crowdfunding. It is important to note that just because a firm regards itself as more 'tech' than 'fin', this does not necessarily mean that it will escape regulation; many activities that might be regarded as mere technological services can fall within the scope of the regulatory perimeter. Whether a particular activity constitutes a regulated activity can, therefore, be a complex question and we recommend obtaining specific legal advice.

A firm that wishes to undertake regulated activities in the UK will need to obtain authorisation from one of the UK's financial regulators, the Financial Conduct Authority (FCA) or the Prudential Regulation Authority (PRA). Once authorised, those firms will be subject to a range of additional primary legislation, as well as detailed (and in some cases, activity-specific) rulebooks published by the FCA and the PRA.

The FCA, like other regulators, has recently expressed concern about the regulatory status of coin and token offerings. It published a consumer warning about the risks of ICOs in September 2017, noting that although many ICOs will fall outside the regulated space, some ICOs may involve regulated investments depending on how they are structured.

3.2 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested?

The financial regulators and policy-makers in the UK are very receptive to fintech. The UK Government's publicly stated position is to make the UK the 'global capital of fintech' and it continues to provide political and policy support to the sector. This support has included developing the UK's digital infrastructure (for example, through the provision of high-speed broadband), creating a favourable tax and investment regime for start-ups (for which, see further our replies to questions 2.1 and 2.2 above) and promoting the UK fintech industry globally through its network of embassies and trade delegations.

This favourable political environment naturally has influenced the approach of the PRA and the FCA. In particular, the FCA is generally regarded as one of the most forward-thinking regulators in the world in this area and has established 'Project Innovate' to assist both new and established businesses to introduce innovative financial products and services into the UK. Project Innovate consists of three core elements:

- an 'Innovation Hub', which supports innovative businesses in understanding the regulatory framework and how it applies to them, assists with preparation of authorisation applications for qualifying firms and provides a dedicated contact for up to a year after an innovator business is authorised;
- an 'Advice Unit', which provides regulatory feedback to firms developing automated models that seek to deliver lower cost advice to consumers; and
- a 'Regulatory Sandbox', which the FCA describes as a 'safe space' for businesses to test innovative financial products, services, business models and delivery mechanisms in a live environment without immediately incurring all the normal regulatory consequences of engaging in the activity in question.

3.3 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Where a fintech firm wishes to perform regulated activities in the UK, it will need to consider whether it requires authorisation to do so. It is important to note that a person does not need to be established in the UK in order to carry out regulated activities in the UK – a fintech business based overseas which deals with customers in the UK is likely to be viewed as carrying on activities in the UK.

Where an overseas fintech firm performs regulated activities in the UK, it will need to obtain authorisation from the UK financial regulators (as described further in our answer to question 3.1 above), rely on an exemption to the authorisation regime or, if established in an EU Member State, rely on any passporting rights which may attach to the activities in question.

There are numerous exemptions to the performance of regulated activities, some of general application and others associated with specific activities. Application of these exemptions is, of course, fact dependent, but it is worth noting that one exemption – the 'overseas person exemption' – is specifically targeted at firms established outside of the UK. This exemption is, however, restrictive in scope, applying only to certain activities and where there is direct involvement of an authorised or exempt firm in the performance of the activity or a 'legitimate approach' by an overseas person (e.g., an approach that does not breach the UK's financial promotions regime).

As noted above, another route to undertake regulated activities in the UK without authorisation from a UK financial regulator is to rely on a passport provided for in European legislation, at least until the UK's departure from the EU. This would enable the firm to use an authorisation in another EU country to perform regulated activities in the UK.

Overseas fintech firms should also have regard to the UK financial promotions regime under which firms are not permitted, in the course of business, to communicate (or cause to be communicated) an invitation or inducement to engage in investment activity, unless that person is authorised or the communication falls within the scope of an exemption. As with regulated activities, one such exemption relates to overseas communicators.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The UK data protection regime is currently viewed as one of the more business-friendly European data protection regimes. However, EU (including UK) law is changing. From 25 May 2018, the General Data Protection Regulation will apply. It has direct effect in all EU Member States and applies to Fintech organisations established in the UK which process personal data. Processing is defined widely to cover any operation performed on personal data including collecting, storing or destroying that data. It applies to:

- 'controllers' – defined as those organisations which process personal data and determine the purpose and means of such processing; and
- 'processors' – which includes service providers and other persons which process personal data on behalf of a controller.

The previous regime (based on the Data Protection Act 1998 (DPA) which implemented the European Data Protection Directive) was principles-based. The GDPR retains this approach: those processing personal data must comply with a set of principles (for example, personal data must be processed fairly, lawfully, transparently and securely) and needs a 'lawful basis' for the processing (for example, consent). It also codifies case law and best practice guidance developed under the previous regime. However, the GDPR is more prescriptive and restrictive than the law it replaces. For example, it includes mandatory breach notification provisions and high monetary sanctions, and imposes obligations on both controllers and processors (the DPA focussed on controllers).

While the GDPR aims to harmonise data protection legislation across the EU, it does give Member States limited opportunities to make provisions for how it applies in their country. In the UK, a draft new Data Protection Act (currently in bill form) is passing through the legislative process: it includes these provisions for the UK. It also covers areas (like law enforcement) not covered by the GDPR. There is also a draft UK Regulation which will impose a data protection fee of between £40 and £2900 on data controllers (depending on the size

and type of organisation, unless they are exempt). This will replace the current notification fee.

Note: Unsolicited direct marketing by electronic means is also covered by the Privacy and Electronic Communications Regulations 2003 (PECR), which again are based on an EU Directive. A new Regulation, to replace this Directive, is currently being negotiated at EU level, and it is expected to become law before the UK leaves the EU. In addition, sector-specific regulators, including those in the finance sector, regulate the use of data by organisations that fall within their remit.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Yes to both questions. The GDPR:

- has a wide extra-territorial reach, applying to any controllers and processors established outside the EU who process the personal data of EU individuals and offer goods or services to them, or monitor their behaviour; and
- restricts the transfer of personal data outside the EEA unless adequate protection is in place. There are various ways to obtain adequate protection, including using 'approved form' standard contractual clauses relating to data export or obtaining consent from the individual whose data is being transferred.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

There are a range of sanctions available, including:

- Large fines – the UK's data regulator (the Information Commissioner's Office or 'ICO') could only issue fines of up to £500,000 under the DPA. However, fines under the GDPR can be much higher – up to 4% of annual worldwide turnover or €20 million (whichever is greater).
- Criminal liability – the DPA and the draft Data Protection Bill include a number of criminal offences, for example, knowingly or recklessly obtaining or disclosing personal data without the controller's consent. Directors, managers and officers can (in certain circumstances) be held personally liable for offences by corporations.
- Damages claims – individuals who have suffered as a result of infringement of the GDPR may be entitled to compensation. There is also the potential for group actions.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

There are a variety of laws and regulations which could apply following a cyber breach in the UK, and many of them derive from EU legislation. For example:

- data protection rules (for example, around security and breach notification) will apply where personal data is involved (see above);
- sector-specific regulators may take action, for example: (i) in the financial services sector, the FCA may take action if a cyber breach was caused by a bank or other regulated entity failing to implement effective systems and controls (which is likely to include having robust cybersecurity measures); and (ii) fintech businesses which are telecoms operators or ISPs may face action from the ICO for breach of PECR, and Ofcom for breach of the Communications Act 2003; and
- the Computer Misuse Act 1990 creates a number of cybercrime offences relating to actions such as unauthorised access or interference with a computer and DDoS attacks. It was amended in 2015 to implement the EU's Cybercrime Directive.

The EU's NIS Directive, lays down measures aimed at achieving a high common level of security of networks and information systems within the EU. These include imposing security requirements and incident notification obligations on 'operators of essential services' together with certain digital service providers. Banks are included in the list of sectors relevant to operators of essential services in the Directive. However, the UK Government has chosen to exclude them from the list of relevant sectors when implementing the Directive into UK law. In their view, the finance sector is already sufficiently regulated in this area.

The UK also has laws relating to the interception of communications and the ability of public bodies to carry out surveillance, although they are beyond the scope of this chapter.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The UK's key piece of anti-money laundering legislation is the Proceeds of Crime Act 2002 (POCA). There are essentially three principal money laundering offences: (i) concealing, disguising, converting or transferring the proceeds of crime; (ii) becoming concerned in an arrangement to facilitate the acquisition, retention or control of, or to otherwise make available, the proceeds of crime; and (iii) acquiring, possessing or using property while knowing or suspecting it to be the proceeds of crime. There are also 'secondary' offences of: (i) failure to disclose any of the above offences; and (ii) tipping-off of persons engaged in money laundering as to any investigation.

Firms operating in the regulated sector, including fintech firms, must also comply with the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 which set out detailed requirements in respect of customer due diligence and anti-money laundering policies and procedures, among other things.

In addition, the FCA specifies additional rules in respect of anti-financial crime systems and controls in its Handbook, which will apply to authorised firms. Both the PRA and the FCA regard adoption of rigorous and robust anti-financial crime systems and controls as essential to meeting the ongoing regulatory requirements of being an authorised firm.

The Bribery Act 2010 (BA) is the UK's anti-bribery legislation. The BA is generally regarded as rigorous and onerous by worldwide standards, and specifies offences in respect of bribing another person, being bribed, bribery of foreign public officials and a corporate bribery offence relating to the failure of commercial organisations to prevent bribery. As with the basic anti-money laundering offences in POCA, the BA applies generally to any entity doing business in the UK.

Finally, the Criminal Finances Act 2017 introduced two new UK corporate offences for failing to prevent the facilitation of domestic or overseas tax evasion, which can be committed by any body corporate or partnership.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

Please refer to our comments above on the UK data protection regime and cybersecurity laws or regulations. There is no legislation in the UK which is aimed specifically at the fintech sector. Any additional

relevant regulatory regimes would likely be specific to the sector in which a particular fintech firm operates.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Subject to the mandatory benefits referred to at question 5.2 below, individuals can generally be hired on whatever terms are considered appropriate. When hiring, it is important to bear in mind that the prohibition of discrimination in employment applies to everything from job advertisement, candidate selection and recruitment, to employment terms and reasons for dismissal. Unlike most other employment-related claims, compensation for discrimination is uncapped.

Under UK law, the term 'dismissal' incorporates employer terminations, expiry of fixed-term contracts and constructive dismissals (where the employee resigns and treats himself as dismissed due to a repudiatory breach by the employer).

Broadly, employees with two years' service can claim unfair dismissal if a dismissal: (i) does not fall within one of five fair reasons (such as conduct, capability or redundancy); (ii) does not follow a fair procedure (including compliance with relevant codes of practice); or (iii) is not fair and reasonable considering all the circumstances, including the employer's size and resources. Remedies include compensation (subject to statutory caps), or in limited circumstances reinstatement or re-engagement. Dismissals for certain reasons (such as whistleblowing) are automatically unfair, they do not require a qualifying period of employment, and compensation is uncapped.

Except in cases of gross misconduct or any other repudiatory breach, dismissing an employee without the required notice period (or payment *in lieu*, where permitted under the contract) generally leads to a wrongful dismissal, allowing the employee to claim for loss of earnings which he would have received during the notice period.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Employers must pay all workers at least the specified national minimum/living wage, and must contribute to the state pension and health system on the workers' behalf. In addition, eligible jobholders must be automatically enrolled into a personal or occupational pension scheme meeting certain minimum requirements (unless they opt out).

All workers are entitled to at least 28 paid days of annual leave (which includes public holidays and is pro-rated for part-time workers), as well as specified minimum daily and weekly rest periods. Shifts longer than six hours must usually also include breaks. Workers may not work more than 48 hours per week averaged over 17 weeks, unless they opt out of the 48-hour limit (which is very common in practice).

Employees who are unfit for work may be entitled to statutory sick pay after the third day of absence, although employment contracts often provide for more generous company sick pay. Special rules apply in respect of the minimum periods of leave and pay for employees taking maternity, paternity, adoption or shared parental leave and certain other family or study-related types of leave.

Bonuses, which are typically linked to performance criteria, are often non-contractual or involve discretion if included in the contract. Many companies also offer share incentives to their employees.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Immigration rules apply to all companies and are not specific to the fintech sector. EEA (excluding Croatia) and Swiss nationals, some Commonwealth citizens and qualifying family members may currently work in the UK without permission. When the UK exits the EU, the free movement rights of EEA and Swiss nationals will be restricted, although the details are yet to be finalised as part of the Withdrawal Agreement.

Most other migrants are subject to a five-tier points-based system and (with some exceptions) must be sponsored by an employer and pass a points assessment. The sub-category covering skilled roles which cannot be filled with a UK/EEA worker is subject to an annual limit divided into monthly quotas. Where applications exceed the quota, those scoring the highest points are given priority. Minimum skill and salary levels apply, and all workers must satisfy minimum English language skills and maintenance requirements. The system also allows for a transfer of overseas employees to UK companies within the same corporate group in some circumstances.

Businesses wishing to employ overseas workers must obtain a sponsor licence for the appropriate tier(s), allowing them to issue certificates of sponsorship to migrants. Sponsors must comply with various requirements, including conducting right-to-work checks, complying with record-keeping duties and reporting certain employee events to authorities. Sponsors are rated based on their compliance; if a sponsor's rating is downgraded below a certain threshold, it is not able to issue new certificates of sponsorship (but can usually still sponsor extensions for its existing workers).

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Fintech products will typically be based on computer programs or software which in the UK is primarily protected by copyright as a type of literary work. Copyright will arise automatically in the computer code and may also subsist in other elements of the software, such as screen displays, or graphics, such as on-screen icons and designs.

In terms of monopoly rights offered by a patent, there are limits on the protection available. Hardware may benefit from patent protection. However, under UK patent law, computer programs as such are excluded from patentability. Business methods are also generally excluded from patentability in the UK. However, it may be possible to obtain a patent where it can be shown that the application of a computer program possesses a technical character and there is research to show that a significant number of patents are being filed in this sector in the UK. Given these difficulties, the law of confidence is an important means to prevent disclosure of technical information, in particular source code. Database rights may also be relevant where the product comprises a type of information management system.

Registered trade marks will protect the branding applied to a fintech product and registered design protection should also be considered for other types of fintech products, such as portable or wearable devices.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Under UK copyright law, the general rule is that the first owner of copyright will be the author, and in the case of a computer-generated work, the author will be the person who undertakes the arrangements necessary for the creation of the work. An important exception to this rule is that works made by a person in the course of his employment will belong to the employer. However, where a company contracts with a third party to create works (e.g. software) on its behalf, the contractor will own the copyright and the company commissioning the work will need to deal expressly with the ownership of these rights by obtaining an assignment of the rights.

A patent for an invention is owned by the inventor. There are also statutory provisions dealing with the ownership of inventions created by employees.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

IP rights are territorial rights. In addition to national registrations, IP owners seeking UK protection can obtain international and, prior to Brexit, EU-wide registrations for certain IP rights and in some cases can obtain cross-border relief.

International copyright conventions provide automatic reciprocal protection overseas for UK qualifying works. The WIPO Copyright Treaty particularly deals with protection of copyright for software and databases.

Patent protection in the UK may be secured via the national route or under the European (EPC) or international (PCT) patent application systems. Upon grant, these registrations provide a bundle of national rights enforced individually as a national patent in the relevant jurisdictions. In Europe, a new unitary patent right, the Unitary Patent (UP) and a complementary centralised enforcement system, the Unified Patent Court, has been agreed but, owing to delays in ratification, is not yet in force. The new patent right will offer protection in up to 26 countries in Europe with the UPC providing cross-border enforcement for UPs as well as for European Patents.

Trade marks and designs can be registered nationally, as EU-wide unitary rights (EU Trade Mark and Community Registered and Unregistered Designs) and under international registration systems. The EU rights are enforced in national courts which are designated Community courts and can issue pan-European relief, although following the UK's departure from the EU, unitary rights, (principally EU trade marks and designs) will not apply in the UK and enforcement mechanisms such as cross-border relief will no longer cover the UK.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP is usually exploited/monetised by means of assignment (transfer), licensing, and the granting of security interests.

There are slightly different formalities for the various IP rights for assignments and licences. Generally, however, an assignment must be in writing and signed by the assignor. Copyright licences can be oral or in writing (exclusive licences must be in writing). Patent licences do not need to be in writing but it is encouraged for registration (see below). Trade mark licences must be in writing and signed.

It is important to register transactions concerning registered rights (assignments, licences and mortgages) on the relevant public register in order to maintain priority as against third-party interests registered in the interim. Where details of an assignment or licence are not registered for trade marks and patents, the assignee/exclusive licensee cannot claim the costs of infringement proceedings relating to the period before registration of the assignment/licence.

Security interests granted through either legal mortgages or charges (in writing and signed) must be registered at Companies House within 21 days following the date of their creation in order to protect against creditors. This is in addition to the registration requirements at the relevant IP registry.

Rob Sumroy
Slaughter and May
1 Bunhill Row
London EC1Y 8YY
United Kingdom

Tel: *+44 20 7090 4032*
Email: *rob.sumroy@slaughterandmay.com*
URL: *www.slaughterandmay.com*

Rob is Head of Slaughter and May's Technology and Outsourcing practices and co-heads the firm's Fintech Team. He advises on all aspects of IT, outsourcing, e/m-commerce, big data, data protection, cyber security and IP, as well as assisting organisations with their digital strategies. Rob is ranked in the IT and Outsourcing sections of *Chambers UK*, recognised as a leading individual for Commercial Contracts in *The Legal 500* and is listed in *SuperLawyers*.

Ben Kingsley
Slaughter and May
1 Bunhill Row
London EC1Y 8YY
United Kingdom

Tel: *+44 20 7090 3169*
Email: *ben.kingsley@slaughterandmay.com*
URL: *www.slaughterandmay.com*

Ben is a partner in Slaughter and May's Financial Regulation practice and co-heads the firm's Fintech Team. His clients span the full spectrum from established global financial and TMT groups to high growth start-up challengers. He advises on all aspects of UK and EU financial regulation, including in the areas of banking, insurance, asset management, payments, mobile banking, e-money, and digital financial services. Ben is recognised in *The Legal 500* as a leading individual in the area of fintech.

SLAUGHTER AND MAY

Slaughter and May is a full-service international law firm headquartered in London with first class European technology and fintech practices. We are pleased to have been retained as UK and EU legal advisers to a broad range of investors, entrepreneurs, high growth start-ups, established businesses and multi-national corporations. Among our many tech and fintech sector clients we are delighted to have supported Stripe, Euroclear, Equinix, WorldRemit, Aviva, Arm Holdings, Google and Vodafone.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com