International Comparative Legal Guides

Fintech 2026

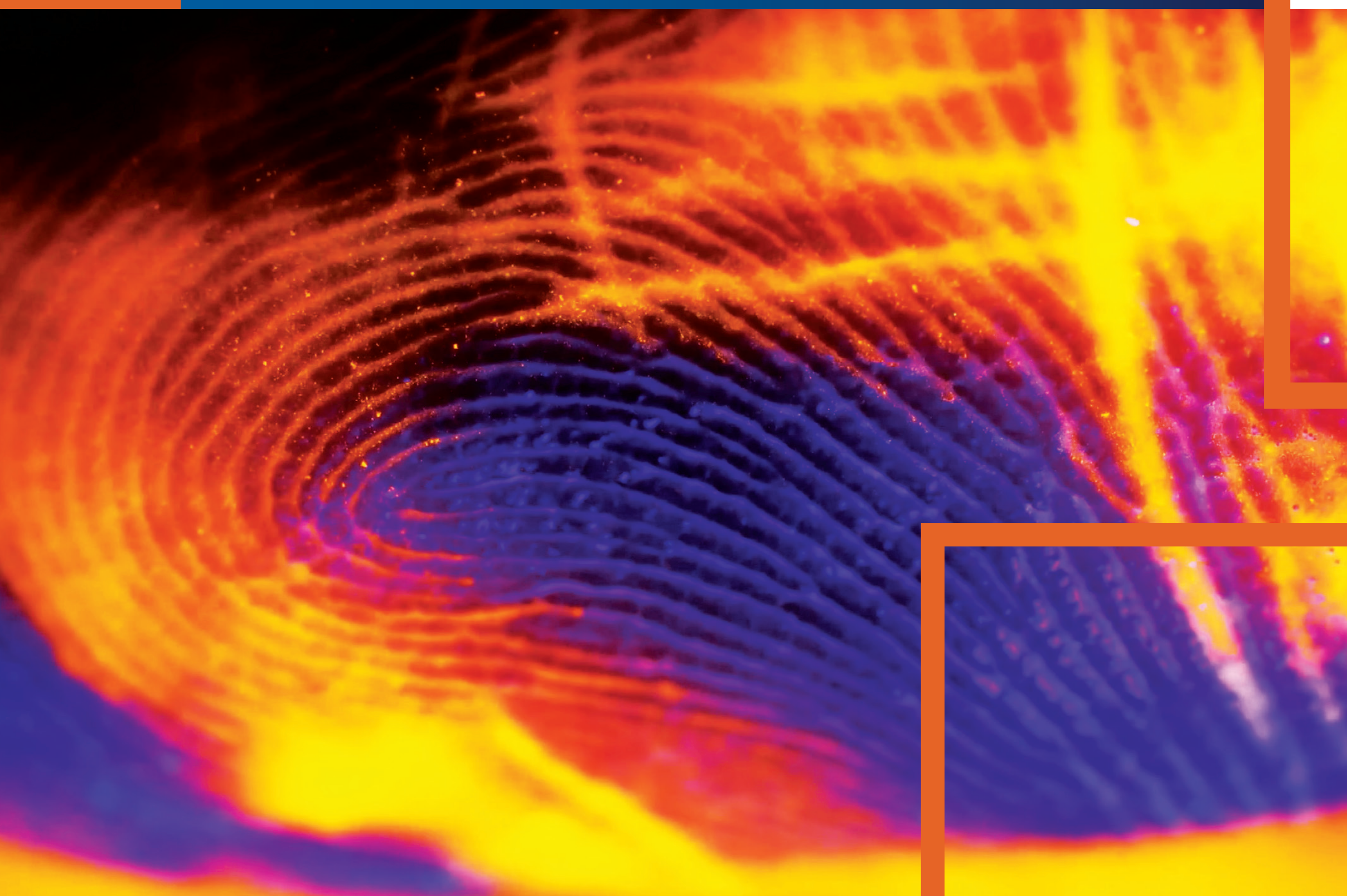
A practical cross-border resource to inform legal minds

10th Edition

Contributing Editors:

David Ives, David Shone & James Cook

Slaughter and May



iclg

glg Global Legal Group

Expert Analysis Chapter

Q&A Chapters

United Kingdom

David Ives

Slaughter and May

David Shone

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and the state of the development of the market. Are there any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, and insurance) including those relating to cryptoassets, tokenisation and artificial intelligence?

The UK remains a leading fintech hub, ranking first in Europe for fintech investment and only second globally to the United States. A broad spectrum of fintech businesses at various stages of growth and development are represented in the UK, and fintech and innovation are at the heart of the UK government's financial services growth strategy.

The UK was an early adopter of innovative payments technology. Open Banking has been celebrated as a UK success story and continues to expand; the latest industry figures published in December 2025 show that more than 16 million users now benefit from Open Banking products and services. Next, Open Finance is set to build on this success and extend Open Banking-like data sharing to a wider range of financial products, including mortgages, investments and insurance. While in the early stages of development, Open Finance is expected to support greater product and service personalisation as well as a more dynamic market, as consumer and businesses are able to compare and switch financial products more easily.

Adoption of artificial intelligence (AI) by the financial services sector continues at pace; in a survey in November 2024, the Bank of England and the Financial Conduct Authority (FCA) reported that 75% of regulated firms were already using AI. Retail use cases will come under scrutiny in 2026 following the launch of an FCA review into how AI may reshape retail financial services by 2030 and beyond. The outcome of this review (called the "Mills Review") will be reported to the FCA Board in summer 2026, and it will consider the development of more powerful, autonomous and agentic systems. We discuss the regulatory approach to AI at question 4.6 below.

Distributed ledger technologies continue to emerge in diverse sectors across the UK, with a concentration in financial services. The FCA's latest research on consumer attitudes to cryptoassets, published in December 2025, found that 8% of UK adults own cryptoassets. This represents a decline compared to 2024, where cryptoasset ownership was at 12%, although 25% of cryptoasset users say they would be more likely to invest if cryptocurrencies were more regulated in the UK. This suggests that uptake may increase when a greater number of cryptoasset activities are brought within the financial services regulatory perimeter in October 2027 (see further question 3.1 below). Noteworthy too is industry focus on tokenisation projects – in particular, deposit and fund tokenisation – alongside heightened interest in stablecoins, where the FCA has announced that stablecoin payments are a priority for 2026.

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

There are currently no prohibitions or restrictions that are specific to fintech businesses in the UK. Depending on the nature of the business, fintechs (and/or the promotion of their activity) may need to be regulated in the same way as other traditional financial services firms.

That being said, there are restrictions related to the use and trading of certain cryptoasset products in the UK. While the FCA recently lifted its ban on the retail sale, marketing and distribution of cryptoasset exchange-traded notes (where admitted to a UK recognised investment exchange), its ban on retail participation in cryptoasset derivatives remains in force.

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) require all cryptoasset exchanges and custodian cryptowallet providers to comply with anti-money laundering (AML) requirements, including registering with the FCA, and implementing identity and other AML checks. This has presented a challenge for certain cryptoasset firms, and the FCA confirmed in September 2025 that only 15% of cryptoasset business applicants have successfully achieved MLR registration with the FCA since January 2020.

See question 3.1 below for further details of the UK regulatory approach to cryptoassets, which is evolving at pace.

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. Although the UK IPO market has been relatively quiet in recent years, investor confidence showed signs of improvement in the second half of 2025 and Q4 saw the first wave of significant UK IPOs in several years (including a landmark listing by Shawbrook, a digitally-enabled specialist bank, which was the UK's largest

IPO by market capitalisation since 2021). Despite current geopolitical headwinds, optimism remains that this will continue, and fintechs are viewed by many as offering the key to unlocking London's public markets. A number of fintechs, most notably neobanks, have weathered the storm and are likely to consider public offerings (in the UK or elsewhere) in the coming years. The regulatory landscape is adapting to create a more hospitable environment for such businesses to float. Fortunately for growth-stage or less mature fintech businesses without access to public markets, there is also a number of other funding sources (both equity and debt) available in the UK.

The Kalifa Review, centred on UK fintech, led to the introduction of new rules for listing companies in December 2021. In particular, companies were permitted to join the premium segment of the Main Market with certain types of dual-class share structures (DCSS), which can be particularly appealing to innovative, founder-led companies but problematic for banks and other firms subject to regulatory capital requirements. The "free float" requirement (the amount of shares an issuer is required to have in public hands) was also reduced from 25% to 10%, as was the minimum market capitalisation threshold (which traditionally favoured more mature, scaled businesses). Even more significantly, in July 2024, major reforms to the listing regime in the UK were introduced. The reforms included merging the "Premium" and "Standard" listing segments into a new, consolidated category, removing the requirement to obtain shareholder approval for a significant transaction or a transaction with a related party, and permitting a wider range of dual-share class structures. The main goal of the reforms, which were the most far-reaching for two decades, was to encourage a broader pool of companies to list on the London Stock Exchange, by relaxing certain eligibility criteria and continuing obligations (see further question 2.3 below).

More recently, a new public offers and admissions to trading regime came into force on 19 January 2026 which, together with the aforementioned listing regime updates, represent a major modernising step in the ongoing revitalisation of UK capital markets by, amongst other things, relaxing certain prospectus requirements to make it easier, quicker and cheaper for UK-listed companies to raise further funding in secondary raises and/or offer their own shares as consideration in a takeover. This also includes a new public offer platforms (POP) regime, which enables firms to raise in excess of £5 million outside of public markets without having to publish a full prospectus, making the process significantly faster, simpler and more affordable.

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 (CLN). The CLN becomes convertible into equity on the occurrence of certain events, such as a material funding round, an exit or an IPO, usually at a discount to the value per share implied by such event. An alternative to the CLN, structured so as to qualify for certain tax reliefs, is the advanced subscription agreement, whereby the investor subscribes for future equity determined by reference to the relevant trigger event.

As a fintech matures, similarly to other start-ups, it will typically undergo a series of equity fundraisings (seed funding, Series A, Series B and so on).

Many start-ups saw a reset in valuations after 2021, caused primarily by high inflation, the increased cost of living and geopolitical turbulence. This resulted in a number of "down rounds" (an equity raise undertaken at a discount compared to the company's prior raise), particularly among technology firms.

Notwithstanding the valuation reset, there have been several high-profile fintech equity raises in recent years. Most notably, Revolut announced in November 2025 that it had completed a fundraising round which valued the company at $75 billion (a sharp rise from the $45 billion valuation set the previous year) following a period of major global expansion and earnings growth. That transaction reportedly raised $3 billion in total and was led by Coatue, Greenoaks, Dragoneer and Fidelity. Other recent raises include FNZ (London-headquartered international wealth management platform) securing $650 million in new equity funding from its existing institutional shareholders and payment services provider Rapyd raising $500 million in a Series F round primarily to fund its acquisition of PayU (a major European payments company).

Crowdfunding continues to grow 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, through platforms such as Crowdcube and Republic Europe. 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.

The London Stock Exchange recently launched the Private Securities Market (PSM) as the first platform established under the UK's new Private Intermittent Securities and Capital Exchange System (PISCES) regime, with PSM's opening auction scheduled for 25 March 2026. A PISCES platform represents a new type of regulated trading platform designed to facilitate the intermittent trading of existing shares in private companies within a multilateral system. The idea is loosely modelled on Nasdaq Private Markets, where blocks of shares in private US companies are frequently traded. PISCES platforms will offer a route to liquidity for existing investors in private companies without having to wait for an IPO or M&A deal. Although a PISCES platform cannot be used for a primary fundraising, the increased prospect of liquidity should also help attract primary investors. Among other things, private companies may use a PISCES platform to help rationalise or broaden their shareholder base or enable employees to sell shares.

The new POP regime (which, as noted above, is expected to make fundraising outside of public markets significantly easier) is also gaining traction, with Crowdcube having recently become one of the first retail investment platforms in the UK to be authorised as a POP.

Debt

Small fintechs often do not have recourse to "traditional" bank loans and have therefore relied on a number of more tech-focused banks. The market has seen an increase in competition and a bifurcation between early-stage and late- or growth-stage lending, including a rise in specialist private credit lenders. Other tech-focused banks continue to provide debt finance to technology 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 various tax incentives for investment in start-ups. Generally speaking, these incentives are not specific to the tech or fintech sectors and are available to qualifying companies and investors in all sectors.

These include the Seed Enterprise Investment Scheme (SEIS), which offers a 50% income tax relief for UK taxpayers investing up to £200,000 in qualifying start-ups. Gains made on a disposal of shares are exempt from capital gains tax. For both purposes, the shares must have been held for at least three years. To qualify for the SEIS, following reforms introduced in 2023, a company must (among other qualifying criteria) be no more than three years old, have less than £350,000 in gross assets and have fewer than 25 employees.

This complements the Enterprise Investment Scheme (EIS), which offers tax relief for investment in more mature companies (though the tax relief available under the EIS is 30%). Equivalent relief is also applicable if an investment is made through a venture capital trust.

In addition, R&D tax credits are available in the UK. Following changes introduced in April 2024, loss-making R&D "intensive" SMEs are entitled to claim a tax deduction and payable credit in respect of expenditure on qualifying R&D (known as enhanced R&D intensive support), and companies of all sizes can claim tax relief on such expenditure through an "above-the-line" R&D expenditure credit.

To assist companies in attracting and retaining top talent, the Enterprise Management Incentives Scheme (EMIS) is also available. Companies with gross assets of £30 million or less and fewer than 250 employees (or, with effect from 6 April 2026, gross assets of £120 million or less and fewer than 500 employees) may be eligible, and as a result are able to grant share options over shares worth up to £3 million (or, with effect from 6 April 2026, up to £6 million). An employee is entitled to certain tax breaks on up to £250,000 worth of EMI options granted to them in any three-year period.

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. The main conditions that must be satisfied in order to list shares in the Equity Shares in Commercial Companies category of the Main Market are:

- The company must be duly incorporated, validly existing and operating in conformity with its constitution, and its shares must comply with the laws of the company's place of incorporation, be duly authorised, and have all necessary statutory and other consents.
- The company's shares must be freely transferable and free from any restrictions on the right of transfer.
- The company must have an expected aggregate market value of at least £30 million.
- The company must publish an approved prospectus containing specified information, including three years (or such shorter period as the company has been in operation) of historical financial information and a statement that the company has sufficient working capital for the next 12 months.
- At least 10% of the shares must be in "public hands" at the time of admission.
- If the company has a controlling shareholder (broadly, a person who controls 30% or more of the voting rights), it must: (i) demonstrate that it is able to carry on its main business activity independently from the controlling shareholder at all times; and (ii) require the election and re-election of independent directors to be subject to approval by a majority of independent shareholders as well as a majority of all shareholders (a dual vote).
- As a general rule, shareholder voting must be conducted on the basis of one vote per ordinary share. However, provided certain conditions are met, a company can adopt a DCSS in which unlisted shares issued to certain pre-IPO shareholders (such as employees, directors, founders and other qualifying pre-IPO investors) can exercise multiple votes on most types of resolution.

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

According to data from Dealroom, the UK start-up ecosystem is now worth over $1.3 trillion, making it the most valuable ecosystem in Europe and third most valuable globally. It is home to over 200 "unicorns" (a start-up company valued at over $1 billion), over 200 "futurecorns" (high-growth tech companies that are predicted to reach the $1 billion mark in the future) and more than 25,000 funded start-ups.

IPO activity over the last couple of years had been muted but we are beginning to see signs of improvement (see question 2.1 above). In any case, investment in fintech has continued strongly. According to Dealroom, fintech was the UK's leading industry for venture capital investment in 2025 (calculated by reference to total venture capital investment raised in 2025). Revolut remains Europe's most highly valued start-up with a $75 billion price tag after completing its latest fundraising round in late 2025. Similarly, Monzo secured a £4 billion valuation in a fresh round of funding in 2024.

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 the provision of banking, consumer credit and insurance services, as well as certain areas more typically associated with fintech start-ups, such as crowdfunding.

A firm that wishes to undertake regulated activities in the UK will need to apply for authorisation from one of the UK's financial regulators, the 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.

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. Indeed, the provision, or operation, of technology and financial regulation is becoming increasingly enmeshed in certain contexts, as traditional financial services are now delivered via digital platforms and apps, and technology firms offer payment wallets and credit options. An example of how this trend translates to regulation can be found in a recently established regime created to regulate certain services provided by "critical" third parties, such as cloud, AI and other ICT service providers, to financial services and financial market infrastructure firms. The FCA is also keeping an eye on the activities of big tech firms operating at the boundary or outside the regulatory perimeter, and monitoring the increasing participation of big tech firms in retail financial services (with a recent focus on digital wallets, alongside the Competition and Markets Authority (CMA)).

Looking to the future, work is underway to introduce a number of new regulated activities tailored to the cryptoasset market, where these cryptoasset activities mirror, or closely resemble, regulated activities performed in traditional financial services. These new activities – which include cryptoasset safeguarding, cryptoasset intermediary activities and stablecoin issuance – are expected to go live on 25 October 2027, and the application period for firms for authorisation in respect of these new activities will open in September 2026.

Additional regulatory initiatives that may impact the regulatory framework for fintech businesses include plans to modernise payment services regulation (and the approach to stablecoins), the development of Open Finance and the outcome of the Mills Review into how AI will shape retail financial services (see question 1.1 above).

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? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

UK financial regulators and policy-makers continue to be receptive to fintech, particularly as the UK seeks to maintain its position as a competitive, innovative and pre-eminent financial centre that is supportive of growth. This is evidenced by a number of tech-focused initiatives, including:

- the FCA's "AI Lab", where key features include a "Supercharged Sandbox", giving firms access to high-performance computing, enriched datasets and advanced AI tools, and "AI Live Testing", which provides firms with a safe place to test AI systems in real-world conditions, with appropriate regulatory support and oversight;
- the FCA's "Smart Data Accelerator", which aims to advance Open Finance and smart data for UK businesses by enabling organisations to use synthetic data to develop proofs of concept while supporting dynamic policy making;
- the Bank of England and FCA's "Digital Securities Sandbox", a regulated live environment that has been created to explore how developing technologies could be used by firms to undertake the activities of notary, maintenance and settlement for financial securities either alone, or together with the operation of a trading venue; and
- the Bank of England's "AI Consortium", which acts as a platform for public-private engagement on the capabilities, development, deployment and use of AI in financial services.

The UK's Information Commissioner's Office (ICO), the main data privacy regulator in the UK, also hosts a sandbox to support organisations in developing innovative products and services, using personal data in different ways.

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 that 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) or rely on an exemption to the authorisation regime.

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 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).

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.

3.4 How is your regulator approaching the challenge of regulating the traditional financial sector alongside the regulation of big tech players entering the fintech space?

To date, big tech players have made only modest inroads to the UK financial services sector, with the notable exception of payment services and mobile wallets in particular. We have not, however, seen technology platforms operating outside the financial services sector make any significant plays within the retail financial services sector beyond this.

Given the nature of the services offered by big tech players who are active in the fintech space, the FCA and the CMA have emerged as the most significant regulators in this area.

The FCA's existing competition objective and new secondary objective of economic growth and competitiveness may affect the regulator's approach to balancing the benefits and risks of technological innovation and market entry by large technology businesses. At the same time, its consumer protection mandate has to date guided it towards a relatively cautious approach to disruptive providers in the sectors that it regulates.

Looking ahead, Open Banking and Open Finance offer new opportunities in financial services, and could ultimately also require data sharing by tech as well as financial services providers. This is something that the FCA has recently explored to address the data asymmetry that currently exists between certain tech and financial services providers, and it is currently monitoring big tech firms' activities to assess whether further policy changes may be needed. Meanwhile, the CMA plans to consult on potential interventions in relation to digital wallets in the second half of 2026.

Finally, feedback to the Mills Review, referred to in question 1.1 above, is also of interest here; it asks respondents whether big tech will come to control the primary retail customer relationship by 2030, and whether AI systems could provide services functionally equivalent to regulated activities such as advice or intermediation while remaining outside the regulatory perimeter.

In the meantime, tech firms looking to offer regulated services in the UK will continue to be subject to the same requirements, rules and supervisory scrutiny as their traditional counterparts.

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 General Data Protection Regulation (GDPR), supplemented by the Data Protection Act 2018 (DPA 2018), regulates the processing of personal data and special category data and applies to fintech organisations established in the UK. However, the UK GDPR has extra-territorial reach and may also apply to some fintech organisations established outside the UK (see question 4.2 below). While the UK GDPR remains closely aligned to the EU's equivalent GDPR regime from which it originated, the two regimes are increasingly diverging, particularly in light of changes introduced in the UK's Data (Use and Access) Act 2025 (DUA Act). The DUA Act has made modest amendments to the UK's data protection regime, introducing a number of relaxations (including to facilitate the use of AI and decision automation), as well as a new requirement for organisations to have a data protection complaints process.

In the UK GDPR, processing is defined widely to cover any operation performed on personal data, including collecting, storing or destroying that data. Fintech organisations caught by the UK GDPR can be controllers, joint controllers or processors, with differing levels of liability and obligations applying according to this designation. Under the UK GDPR:

- "controllers" are organisations that process personal data and determine the purpose and means of such processing;
- "joint controllers" are two or more controllers that jointly determine the purposes and means of processing; and
- "processors" include service providers and other persons that process personal data on behalf of a controller.

The UK GDPR follows a principles-based 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 need a "lawful basis" for the processing (for example, consent). The UK GDPR requires high standards of privacy compliance, including mandatory breach notification, the implementation of data protection by design and default, and for organisations to comply with overarching accountability requirements.

The DPA 2018 supplements the UK GDPR, requiring both pieces of legislation to be considered together. For example, it includes a number of exemptions, provisions relating to international transfers and detail on the enforcement powers of the UK data protection regulator, the ICO. In addition, the Data Protection (Charges and Information) Regulations 2018 (as amended) impose a data protection fee of between £52 and £3,763 on data controllers (depending on the size and type of organisation, unless they are exempt).

The sending of direct marketing (e.g. via email or social media direct message) and the placing of cookies or similar tracking technologies is covered by both the UK data protection regime and the Privacy and Electronic Communications Regulations 2003 (PECR). The DUA Act raises the potential penalties for cookies and marketing infringements under the PECR to UK GDPR levels (see question 4.3 below).

Sector-specific regulators, including those in the finance sector, also 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?

The UK GDPR has a wide extra-territorial reach, applying to any controllers and processors established outside the UK that offer goods or services to individuals in the UK, or that monitor their behaviour in the UK.

The UK GDPR (as amended by the DUA Act) also restricts the transfer of personal data outside the UK unless the standard of protection for the personal data is "not materially lower" after the transfer. The UK government has approved a number of countries (and some territories and sectors within countries) as providing "not materially lower" protection, through adequacy regulations. Personal data can flow freely from the UK to such countries. If there are no adequacy regulations in place for a country, other "appropriate safeguards" set out in the UK GDPR and the DPA 2018 may be relied on to transfer personal data out of the UK. These include, among other things, standard data protection clauses issued by the ICO.

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 the following:

- Large fines – the ICO can impose fines on controllers and/or processors of up to 4% of their annual worldwide turnover, or £17.5 million (whichever is greater).
- Criminal liability – the DPA 2018 includes a number of criminal offences; for example, knowingly or recklessly obtaining or disclosing personal data without the controller's consent.
- Damages claims – individuals who have suffered as a result of infringement of the UK GDPR can claim compensation. There is also the potential for representative and group actions in certain circumstances.

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 that could apply following a cyber breach in the UK, some of which were originally derived from EU legislation – for example:

- data protection rules (for example, around security and breach notification), which will apply where personal data is involved (see question 4.1 above);
- the Computer Misuse Act 1990, which creates a number of cyber-crime offences relating to actions such as unauthorised access or interference with a computer and distributed denial-of-service attacks;
- the Product Security and Telecommunications Infrastructure Act 2022, which creates, among other things, a new regulatory regime to make consumer connectable devices and products more secure;
- the UK's Network and Information Systems regime, which is designed to increase the resilience of suppliers of critical services in the UK (energy, health, transport, etc.) and is being updated. The Cyber Security and Resilience Bill is currently working its way through parliament and will, among other changes, bring certain IT providers and data centres in scope; and
- new ransomware rules, which have been proposed by the UK government. These would ban ransomware payments by certain critical national infrastructure organisations, some of whom could be in the finance sector, and require victims of a ransomware attack to report the attack and any intention to pay.

Sector-specific rules may also apply. For example: (i) fintech businesses that are telecoms operators or internet service providers may face action from the ICO for breach of the PECR and Ofcom for breaches of the Telecommunications (Security Act) 2021; and (ii) PRA and/or FCA rules may apply in the financial services sector (see below). 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.

Cyber continues to be a regulatory priority for both the FCA, which has responsibility to take regulatory action to counter financial crime, and the PRA. Both regulators impose rules seeking to bolster firms' operational resilience (which encompasses cyber resilience), and expect firms to report material cyber incidents. Looking forwards, the Bank of England and PRA are expected to consult on expectations around the management of ICT and cyber resilience risks in Q2 2026.

The UK's National Cyber Security Centre also provides cyber support for organisations, produces guidance (including on specific risks such as the Ukraine crisis, ransomware and supply chain risk) and offers various certification schemes.

Please note that the UK Network and Information Systems Regulations 2018 do not apply to most UK fintech organisations.

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

Financial crime is governed in the UK by a range of legislation.

The key piece of AML legislation is the Proceeds of Crime Act 2002 (POCA), which sets out the principal money-laundering offences, including concealing, disguising, converting or transferring the proceeds of crime. There are also various "secondary" offences, which include the tipping off of persons engaged in money laundering to any investigation.

Firms operating in the regulated sector, including fintech firms, must comply with the MLRs, which back up the provisions in POCA. These set out detailed requirements in respect of customer due diligence and AML policies and procedures, aligning the UK regime with the Financial Action Task Force's international standards, and designating the FCA as the AML and counter-terrorist financing supervisor in relation to certain cryptoasset businesses.

The FCA specifies additional rules and guidance in respect of anti-financial crime systems and controls in its Handbook, which applies 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 AML offences in POCA, the BA applies generally to any entity doing business in the UK.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction (for example, AI)?

Please refer to our comments above on the UK data protection regime and cyber-security laws or regulations. There is no legislation in the UK that is aimed specifically at the fintech sector.

In relation to AI, the UK government set out its AI Action Plan in January 2025, confirming that it will increase public compute capacity, invest in AI infrastructure, look to open access to data and drive AI adoption in government. On the regulatory side, the UK sees its current pro-innovation approach to AI regulation as a source of strength. It has discussed introducing a new AI law covering the most powerful AI models, although the details around this are currently unclear. Otherwise, the UK will continue with its sector-specific approach to AI regulation, ensuring risks are managed in a proportionate manner and encouraging regulators to support AI innovation. Regulators such as the data (ICO) and financial (FCA) regulators are already actively managing AI risks (for example, the ICO is due to introduce statutory AI guidance in 2026). They are also looking to co-operate where appropriate. For example, the Digital Regulatory Cooperation Forum brings together four key regulators responsible for digital regulation – the ICO, FCA, CMA (the competition regulator) and Ofcom (the communication regulator).

Any additional regulatory regimes would likely be specific to the sector in which a particular fintech firm operates. In April 2024, the Bank of England, PRA and FCA confirmed their view that the existing regulatory framework is well equipped to capture regulated firms' use of AI and machine learning, for now. The House of Commons Treasury Committee has, however, challenged this view in a report published in January 2026 which found that the three authorities *"are not doing enough to manage the risks presented by AI…[and] are exposing consumers and the financial system to potentially serious harm"*. The regulatory position may further be influenced by the outcome of the Mills Review (see question 1.1 above).

Future areas of focus for the financial regulators will likely include AI governance and third-party providers of AI, and possibly whether requirements may need to be applied to model providers directly. Meanwhile, the FCA and the ICO are working together to support firms in navigating the challenges to AI innovation that stem from the interaction of financial regulation and data protection requirements.

5 Technology

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

Innovations and inventions can be protected in the UK by various different IP rights. Copyright and patents are of particular relevance to the fintech sector, but other IP rights such as database rights, as well as the law of confidentiality, can also play a part.

- **Patents**: Patents are the most common way to protect inventions in the UK and provide the owner with a 20-year monopoly right. They are registered rights and therefore need to be registered before they become effective. In order to be patentable, an invention must be new, involve an inventive step, be capable of industrial application and not be excluded from protection under the Patents Act 1977. Of particular relevance to the fintech sector, computer programs, business methods and mathematical methods "as such" are excluded from patentability in the UK. Applying these exclusions has not been straightforward, historically, but the UK Supreme Court has recently changed the English courts' approach, bringing the UK more into line with the European Patent Office. It remains to be seen, however, how the English courts will apply the new approach in practice and whether the changes made will ultimately lead to different outcomes on patentability.
- **Copyright**: Copyright is an unregistered right that protects various different categories of "work" in the UK. These include literary, dramatic, musical and artistic works, as well as other types of work such as films, sound recordings, broadcasts and typographical arrangements. Of particular importance to the fintech sector, computer programs (both object code and source code) are protected as literary works. Other elements that are produced when a computer program is running, such as screen displays, graphics and sound effects are also protectable by copyright.
- **Database right**: There are two different types of protection available for databases in the UK: (i) copyright, which protects the structure of the database; and (ii) *sui generis* database right, which protects the data or content stored in the database. A database will be protected by copyright if, by reason of the selection or arrangement of the contents of the database, the database constitutes the author's own intellectual creation. A database will be protected by the *sui generis* right if there has been a substantial investment in obtaining, verifying or presenting the contents of the database.
- **Confidentiality**: The laws of confidentiality and trade secrets can also be used to protect inventions and innovations in appropriate cases. Almost any type of information can be protected by the law of confidentiality, provided that it remains confidential. This includes details of inventions that may not be patentable, as well as things like software source code. Where a fintech business is unable to obtain a patent for an innovation or invention (e.g. for a particular computer program), confidentiality or trade secrets can be a good way of seeking to prevent third parties from copying that invention or innovation.
- **Trade marks**: The branding of fintech companies, as well as individual products and services, may be protected by registered and unregistered trade marks. Registered trade marks can be applied for and registered in the UK at the UK Intellectual Property Office (UK IPO). Unregistered trade mark rights may be enforceable through the English courts under the law of passing off.

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

The rules on ownership of IP vary and depend upon the context in which they are created. A high-level summary of the position for each type of IP right mentioned above is set out below.

- **Copyright**: The basic position is that the author of the work will be the first owner of any copyright in it. In most cases, the author is the person who creates the work. However, for computer-generated works, the author will be the person who undertakes the arrangements necessary for the creation of the work. If a copyright work is created by an employee during the course of their employment, copyright will generally belong to the employer. Where, however, a business commissions a third party to develop works on its behalf, then the third-party contractor will own the resulting copyright unless the copyright has been assigned by written agreement to the commissioning business. There are many ongoing debates at national and international level in relation to how copyright is impacted by the use of AI technologies.
- **Patents**: As registered rights, patents need to be applied for and registered before they become effective. Any person can apply for a patent, but only certain people are entitled to be granted one. Entitlement primarily rests with the inventor (which cannot be AI), however, similar to copyright, if the invention is made by an employee during the course of their employment, then the rights to the patent will generally belong to the employer. There are also statutory provisions for compensation to employees for patents that are of outstanding benefit to the employer.
- **Trade marks**: Generally, the person who applied for and registered the trade mark is the first owner of that trade mark.
- ***Sui generis* database rights**: The first owner of *sui generis* database rights will be the "maker" of the database, that is, the person who took the initiative in obtaining, verifying or presenting the contents of the database and who assumed the risk of investing in the same. As with patents and copyright, in an employment scenario, the rights will generally belong to the employer (absent an agreement to the contrary).

5.3 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)?

As IP rights are territorial rights, in the majority of cases, local rights will be needed to ensure protection in the UK. The main exception is for copyright, where international copyright conventions (such as the Berne Convention) provide automatic reciprocal protection in the UK and overseas for qualifying works. The WIPO Copyright Treaty, which is a special agreement under the Berne Convention, particularly deals with protection of copyright for software and databases.

Patent protection in the UK may be obtained by (1) the national UK route, (2) the European patent system (EPC), or (3) the international patent system (PCT). The UK is not participating in the Unitary Patent and the centralised enforcement system of the Unified Patent Court. UK patents (including UK designations of European patents or international patents) will be needed in order to enforce patent rights in the UK.

Trade mark protection in the UK may be obtained by (1) the national UK route, or (2) the international Madrid System (designating the UK). EU trade marks no longer have effect in the UK. As a result, UK trade marks (including UK designations of international trade marks) will be needed in order to enforce trade mark rights in the UK.

Prior to Brexit, *sui generis* database right protection (see question 5.2 above) could be obtained at the EU level and enforced in the UK. However, EU-wide database rights no longer provide protection in the UK for databases created after 1 January 2021. Instead, UK entities can now obtain an equivalent UK-specific database right that offers equivalent protection. Owners of EU-wide database rights that came into effect before 1 January 2021 were automatically granted an equivalent UK right.

5.4 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 assignment (transfer), licensing and granting security interests.

- **Assignment**: Generally, the assignment of an IP right must be in writing and signed. However, if the whole of a business is transferred, then its registered trade marks are also automatically transferred, except where there is an agreement to the contrary, or circumstances clearly dictate otherwise. Assignments of UK patents and registered trade marks must be registered as soon as practicable with the UK IPO so as to maintain priority against later third-party interests, and within six months of the date of the transaction to maintain a right to costs for infringement proceedings relating to conduct before registration. Copyright assignments do not need to be registered in the UK.
- **Licences**: Exclusive copyright licences must be in writing and signed by, or on behalf of, the copyright owner if the licensee wishes to maintain standing to sue for infringement (non-exclusive copyright licences can be oral or in writing). Patent licences are not required to be in writing or to be signed, but it is advisable in order to clarify terms and assist with registration with the UK IPO. Trade mark licences must be in writing and signed by the licensor, and should ideally be registered with the UK IPO. It should also be noted that the licensing of IP rights (particularly patents) can give rise to competition issues, so care must be taken.
- **Security interests**: IP rights can be used as security for finance. Details of a security interest (such as mortgage or charge) over IP held by a UK company must be registered with UK Companies House within 21 days of its creation otherwise it will be void against a liquidator, administrator and any creditors of the business. Mortgages (which usually take effect as an assignment and licence back) and charges of UK patents and registered trade marks should also be registered with the UK IPO as soon as possible after the transaction.

David Ives is co-head of our Fintech group, having advised numerous emerging fintech businesses and financial institutions investing in, or partnering with, disruptive fintech companies. His work in this sector covers a wide range of technology and commercial matters and issues, and recently included advising a leading international payment processing company on the long-term provision of tech-based outsourced services underpinning the operation of a critical part of the UK's payments infrastructure.

Slaughter and May
One Bunhill Row
London, EC1Y 8YY
United Kingdom

Tel: +44 20 7090 4266
Email: david.ives@slaughterandmay.com
LinkedIn: www.linkedin.com/in/david-ives-2bbab88

David Shone is co-head of our Fintech group, and advises fintechs, traditional financial institutions and investors on commercial and regulatory issues of strategic importance to their businesses, including fundraising, governance, capital structuring, outsourcing arrangements and product development. His clients include Monzo, Tencent, Teya, Credit Karma and TreasurySpring alongside traditional financial institutions such as Barclays, Nationwide, Santander, Aviva and Standard Chartered.

Slaughter and May
One Bunhill Row
London, EC1Y 8YY
United Kingdom

Tel: +44 20 7600 1200
Email: david.shone@slaughterandmay.com
LinkedIn: www.linkedin.com/in/david-shone-a21b43121

Slaughter and May is a global law firm headquartered in London. Our tier one-ranked fintech and emerging technology practice supports clients from across the digital financial services spectrum, ranging from established financial institutions and global technology and telecoms providers, to investors, entrepreneurs and high-growth start-ups. We advise our clients on the legal implications of developments, innovation and growth in digital financial services.

www.slaughterandmay.com

SLAUGHTER AND MAY