SHOOSMITHS

FinTech and the law

10 September 2024

The trend for financial services businesses and others to procure services from FinTech providers – and for providers to offer their services direct to consumers – has increased over the last 15 years. In this article, we outline some of the key areas of law that relate to FinTech.

Similar to technology law more broadly, FinTech law is very much a “discipline of disciplines”.

It encompasses various areas of law relevant to, among other things, contracts, intellectual property, data and privacy, financial services regulation, consumer protection, and more. Lawyers advising FinTech providers, or their customers, on arrangements must understand how various areas of law connect, overlap and sometimes conflict to be able to guide their clients through the issues and to appreciate and address risks.

We explained previously that FinTech involves the use of technology to provide financial services and products. This can include online banking, payments, lending, insurance, personal financial management, cryptocurrency, and more. The trend for financial services businesses and others to procure services from FinTech providers – and for providers to provide their services direct to consumers – has proliferated over the last 15 years. That change has taken place against a legal background which has had to evolve to keep up.

Contracts in FinTech

When two parties do business a legal contract will be formed. These are essential in governing the relationship between the various parties involved in the provision and use of FinTech. Depending on the nature and scope of the service, different types of contracts may apply:

- **B2C contracts**: Where a business provides FinTech products or services directly to its individual end user consumer, we would expect to see: terms and conditions which lay out the rules governing the relationship between them; possible end user licence agreements (EULAs) which define the rights and restrictions associated with using the applicable technology; and, for example, privacy policies which outline how the supplier collects, uses, shares, and protects personal information provided by the consumers.
- **B2B contracts**: In business-to-business arrangements where one or more parties is to provide FinTech solutions or services to the other , we commonly see: agreements for the supply of the FinTech service / platform by one party to the other (including software-as-a-service (SaaS) and software licence agreements), and also collaboration and partnership agreements where two parties might be collaborating to provide a FinTech solution to end-customers.

All contracts should deal with issues that include: the relevant contracting parties and who has what rights and obligations; the duration of the agreement and when either party can terminate; what fees are due; and what level of liability each party will have if something goes wrong. The distinction between B2B and B2C contracts is relevant because in some cases there are more regulatory controls on the terms which can be used in B2C contracts, which are aimed at protecting consumers.

Beyond the basics, FinTech contracts can involve more specific elements depending on the nature of the deal between the parties, the identity of the parties, or the product or service involved. In many cases specific drafting and approaches have evolved to reflect particular industry or business models or wider legal and regulatory considerations. Examples include agreements which involve the provision of payment processing systems, third party software licences, hardware and infrastructure (such as point-of-sale terminals), and collaboration and partnership agreements. The latter are prevalent for financial services business and FinTechs who form partnerships with each other or other businesses (including startups or scaleups) to integrate their products or services with existing platforms, or even competitors, with a view to accessing cutting-edge technologies, expertise, or market insight.

Intellectual property in FinTech

Intellectual property (IP) law is another important area for FinTech. It governs the protection and use of the (often critical) intangible assets and innovations that underpin a product or service. Providers of FinTech need to identify, secure, and protect their IP rights, as well as avoid infringing the IP rights of others. Users of FinTech need to understand the permitted scope of that use, ensure that they do not lose control over important assets which may be generated in the course of use, and ensure protection from third party claims that a product or service is infringing.

Key types of IP and their relevance include:

- **Patents**: Patents may be obtained for FinTech inventions that are new, inventive, and have industrial applicability (such as hardware). They are less likely to relate to software or methods of doing business (though this is possible in some jurisdictions) and are not easy to obtain. Patent applications involve a rigorous examination process and may face challenges from competitors or third parties. However, once they are obtained, they provide a virtual monopoly over the relevant technology for the life of the patent.
- **Trademarks and brands**: Trademarks and brands are the shop window of any business. In 2023, Interbrand found that the top five of the world's 100 most valuable brands were tech businesses, which unsurprisingly included Apple, Microsoft, Amazon, Google, and Samsung. Rankings 28, 37, 40, and 41 were all businesses involved in FinTech and consisted of Amex, VISA, PayPal, and Mastercard. Other FinTech giants ranked were Stripe, Revolut, and Klarna. Trademarks and brands are particularly important in FinTech, as they can represent the identity, reputation, and value of a product or service which, given the complex nature of the industry, might otherwise be difficult for a consumer to understand. Consumer-facing FinTech is a fiercely competitive market born from a desire to disrupt and apply consumer tech-based user experience to often very traditional financial services such as banking and payments. Against that background brand recognition and loyalty can be critical. Registration (where possible), and protection of trademarks and brands, as well as monitoring and enforcement against potential infringements or dilutions are all key.

- **Confidential information and know how**: FinTech platforms and services often deal with or involve sensitive data, know-how, and proprietary technology (software, algorithms, etc.) which may be the main source of competitive advantage or innovation. To that end, protecting confidential information and know how is vital and FinTechs and their customers must employ robust security measures and requirements. It is no coincidence that very often the first step between parties to a potential FinTech collaboration is a non-disclosure agreement (NDA).
- **Copyright**: FinTech relies heavily on software as a way to operate and deliver relevant financial products and services (ranging from customer on-boarding to payment systems). Copyright law protects software code (including source code, object code, and user interfaces). FinTech systems also compile and analyse large datasets containing financial information, market data, and user-generated content. Copyright law may also protect original datasets that meet the requirements of creativity and originality. In the AI – age, the importance of the legal rules which govern ownership of relevant software systems, the data they rely on / create, and possibly the information they consume to "learn" and produce results cannot be overstated. FinTech providers and users need to identify relevant rights, put in place necessary licenses or permissions for use, and, where required assert their own rights and address infringement by third parties.
- **Database**: Database rights are permissions that grant the owner the exclusive right to extract or re-use a substantial part of a database, which is a collection of independent works, data, or other materials arranged in a systematic or methodical way. This can be important and apply to the valuable datasets that are used or generated by a FinTech service (such as financial or transaction data, customer information, or market insights). FinTechs and users need to be aware of their database rights, as well as respect the database rights of others.

Data protection and privacy in FinTech

A significant proportion of FinTech services – especially those that are consumer facing – involve the collection and processing of personal data. This can be of various types and from numerous sources (including customer on-boarding and transactions, financial records, behaviour patterns, preferences, and complaints). Data protection legislation regulates the collection, processing, and transfer of personal data.

Like other businesses, both financial services business and FinTechs need to comply with the data protection laws and regulations that apply to relevant data, and the role they play in relation to it, including the General Data Protection Regulation (GDPR), the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations 2003. In the data economy, data and its use and protection (including restrictions on protection) is an everyday issue.

- **Registration**: Those handling personal data may need to register their data processing activities with the relevant data protection authority, being the Information Commissioner's Office (ICO) in the UK, and pay a fee, depending on the size and nature of their service. This registration process involves providing details about the types of personal data processed, purposes of processing, data sharing practices, and security measures implemented.
- **Authorisation**: Businesses must also obtain or show authorisation or consent from individuals before processing their personal data, especially sensitive data such as financial information.
- **Justification for use**: There should be a valid legal basis for the processing of personal data (such as consent, contract, legitimate interest, or legal obligation) and the data subject must be informed

of the purpose and scope of the processing.

- **Internal governance**: There is a level of internal governance required at any business handling personal data in order to stay legally compliant. Businesses need to provide clear and transparent information to their data subjects about their rights and choices regarding the processing of their personal data. Data Protection Impact Assessments (DPIAs) are needed for those conducting high-risk data processing activities. Where a Data Subject Access Request (DSAR) is received, a business should have dedicated channels and mechanisms for receiving and processing requests, ensuring timely responses and providing individuals with access to their personal data in a transparent and secure manner.
- **End user terms and notices / policies**: Businesses dealing with the public are required to provide clear and transparent information to end users about how their personal data is collected, processed, and used. This information should be communicated via end user terms and policies (including privacy policies and terms of service) which outline the types of personal data collected, the purposes for which it is processed, the legal basis for processing, data retention periods, and any third parties with whom data is shared.
- **B2B provisions regarding sharing / processing**: Where businesses involved with FinTech enter into contractual agreements with other parties that provide them with personal data, or process personal data on their behalf or in collaboration with them they should clearly define their respective roles and responsibilities in a way which addresses relevant legal requirements. For example, data sharing agreements typically include provisions for data ownership, confidentiality, data minimisation, and restrictions on data use; they also specify the responsibilities and obligations of each party regarding data protection and security.
- **Export**: Those looking to transfer personal data outside of the jurisdiction where it was originally collected should establish a legally valid basis for doing so. They must implement appropriate safeguards to protect personal data when exporting it to third countries. It will also be necessary to assess the data protection laws and practices in the destination country to ensure that they provide an adequate level of protection for personal data. If the destination country does not offer an adequate level of protection, additional safeguards may be required to ensure the security and privacy of exported data, for example incorporating Standard Contractual Clauses (SCCs) into contracts with data importers in third countries.
- **Cyber attacks and breach**: Businesses must adopt appropriate technical and organisational measures to protect the personal data they process from unauthorised or unlawful access, use, disclosure, alteration, or destruction and report any data breach to the relevant data protection authority within mandated timescales. Non-compliance with breach notification requirements can result in significant penalties and reputational damage, demonstrating the importance of proactive measures to prevent and mitigate cyber attacks.

Financial services regulation

In the UK, while financial services regulation is primarily the role of the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) (part of the Bank of England), the scope of regulation for FinTech services can vary considerably. This creates a patchwork of laws, regulations and rules which financial services businesses, providers, and other businesses looking to use FinTech (depending on the activities performed by them) may need to comply with.

Financial services businesses should be familiar with the regulatory landscape, but without sophisticated expertise and knowledge, FinTech providers can often feel overwhelmed by the sheer volume and complexity.

Many providers express frustration at the slow pace of change in financial services law. And since financial services law in the UK is not FinTech-centric, many rules which providers and users may find themselves subject to will not have been designed and implemented with their new technologies in mind. This has created a cat-and-mouse scenario between FinTech providers and users and regulators who are trying to keep law and regulation up to the same pace.

Here are some of the key issues:

- **Regulated activities**: “Regulated activities” (and payment services) are key concepts in financial services law. In the UK, anyone performing a regulated activity (for example provision of credit, or promotion of investments) must be authorised by the FCA (or in some cases, the PRA) to do so, or at least fall within the scope of a regulatory exemption. The first consideration many FinTech providers may have to take is whether their product or service will amount to a regulated activity (or a payment service). This can also be a consideration for non-financial businesses who may, for example, be looking to embed a FinTech offering (and related financial service) in their customer journey. Determining whether a particular activity is within the regulatory perimeter can be a difficult exercise. The Financial Services and Markets Act 2000, the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, the Payment Services Regulations 2017 and the E-money Regulations 2011 set out between them the range of activities which may or may not be regulated. However, conducting regulated activities (or a payment service) without the necessary authorisation from the FCA carries serious consequences and is a criminal offence.
- **Authorisation and permissions**: FinTech providers carrying on a regulated activity or a payment service must obtain authorisation from the FCA or PRA (depending on the nature of the activity). A FinTech provider applying for authorisation must obtain permission from the regulators to carry on particular regulated activities or payment services. Authorisation does not grant a provider freedom to carry on all regulated activities and payment services. This reaffirms the importance for FinTech providers to ensure they are confident they understand what regulated activity or payment service they will be carrying on. It is common for businesses (FinTech or otherwise) to inadvertently carry on a regulated activity or payment service for which they do not have permission.
- **Conduct and culture**: In the aftermath of the 2008/9 financial crisis, the UK government and regulators took steps to ensure better oversight of senior management and executive decision-making in financial services firms. This led to the introduction of the Senior Managers and Certification Regime (SMCR) for many financial services firms. SMCR is designed to ensure that those in certain positions within financial services firms are fit and proper, and have the right competencies to perform their jobs. Those performing executive and board level functions will need to be approved to do so by the regulators themselves. There are also more recent requirements such as the UK Consumer Duty to take into account – which represents a major change in the rules applicable to the treatment of end-customers.
- **Processes, policies, systems and controls**: Processes, policies, systems and controls represent some of the most important parts of a financial services firm’s operating and governance model. The FCA has specific rules that state firms must have reasonable and proportionate systems and

controls. There are also recently introduced requirements imposed on financial services firms which require them to have mapped out their organisation and supply chain and worked out their levels of operational resilience and impact tolerance if critical services and arrangements are interrupted.

- **Complaints**: For those FinTech providers who will be dealing with consumers (which is a substantial proportion) complaints invariably play a large role in the day-to-day functioning of a business. The regulators expect financial services firms to take complaints seriously and there are strict rules set out by the FCA on how firms must handle and deal with complaints. The regulators also expect firms to monitor complaints to help inform their own approaches to compliance with the myriad of rules and regulations.
- **Outsourcing**: Outsourcing – especially of critical or important functions – plays a significant role in financial services. This can be the case for start-up or scale-up FinTech providers but also where large organisations may be looking to use the services of a third party to run their operation. Unsurprisingly, the financial services regulators have specific rules in relation to the outsourcing of material functions. That is, functions which relate to a financial services firm's regulated activities or payment services or without which they would struggle to operate. The now ubiquitous use of cloud services and IT outsourcing has also caught the attention of the regulators – likely as a result of high-profile instances of IT failures which have resulted in customers of financial services firms being unable to use and access their products. FinTech providers and financial firms procuring technology-based services to a large enough degree should take particular care to ensure that outsourcing agreements meet the requirements of the regulators – which differ depending on the type of regulated activity or payment service being undertaken.
- **Regulatory sandbox and innovation hub**: FinTechs may benefit from the FCA's initiatives to support innovation and competition in the FinTech sector, such as the regulatory sandbox which allows providers of FinTech to test their products and services in a controlled environment with reduced regulatory requirements, and the innovation hub which provides them with guidance and support on the regulatory framework and the authorisation process.

Regulators and regulation have often been seen to be the follower, rather than the leader, in relation to innovation and developing technologies. As new technologies and business models emerge and gain traction in financial services, an exercise is required to work out where they "fit" in the existing regulatory landscape. At the same time regulators must start to understand the technologies, their application, and whether new regulation is required to govern their use. Some hope can be taken from the emergence of open banking rules – which stemmed from a Competition Law Review into the dominance of leading banks – and which has provided the "rails" along which many FinTech propositions have emerged over the last decade or so.

However, new developments such as artificial intelligence (AI), calls for "Open Finance" (which would allow sharing of financial data from / to non-banking entities), a focus on ESG in finance, and increased automation of fraud, as well as the measures to try and address it, mean that there will be substantial amounts of innovation which regulators will need to continue to understand.

Consumer law

Consumer law will protect the rights and interests of consumers who use FinTech services. Financial services businesses and FinTechs need to comply with the consumer protection laws and regulations that

apply to their FinTech offerings, including the Consumer Rights Act 2015 which applies to all consumer contracts for financial services.

- **End user terms and treatment**: Businesses must ensure that their end user agreements and terms of business are fair, transparent, and compliant with the relevant consumer law provisions (such as the rules on unfair contract terms, unfair commercial practices, distance selling, and cooling-off rights). They also need to treat their consumers fairly and honestly, and provide them with adequate information, advice, and redress mechanisms.
- **Licensing and authorisation**: Businesses may need to obtain a licence or authorisation from the FCA or another competent authority, depending on the type and scope of the FinTech service (such as payment services, electronic money, lending, investment, or insurance).

Other laws and regulation

The above areas of law are arguably the most immediate and relevant to most if not all FinTech products and arrangements, however there may be more areas to consider, depending on the specific proposition or business model. These may include tax, corporate, banking, securities, and competition laws. While well-established financial businesses may be well-versed in these areas, newer FinTechs may lack familiarity. Additionally, all businesses, including FinTechs, should also take into account employment law regardless of their industry focus.

As well as legislation and policy-based laws and regulations, many areas of business relevant to FinTech have their own industry-based rules which much be accounted for when considering a proposition or proposed deal between two parties. A key example is the large body of industry rules applicable to those operating in the payments sector and which participants are expected to comply with and in some cases flow down to others. Payment industry rules regulate everything from settlement times to how payment related data can be stored and/or processed.

Disclaimer