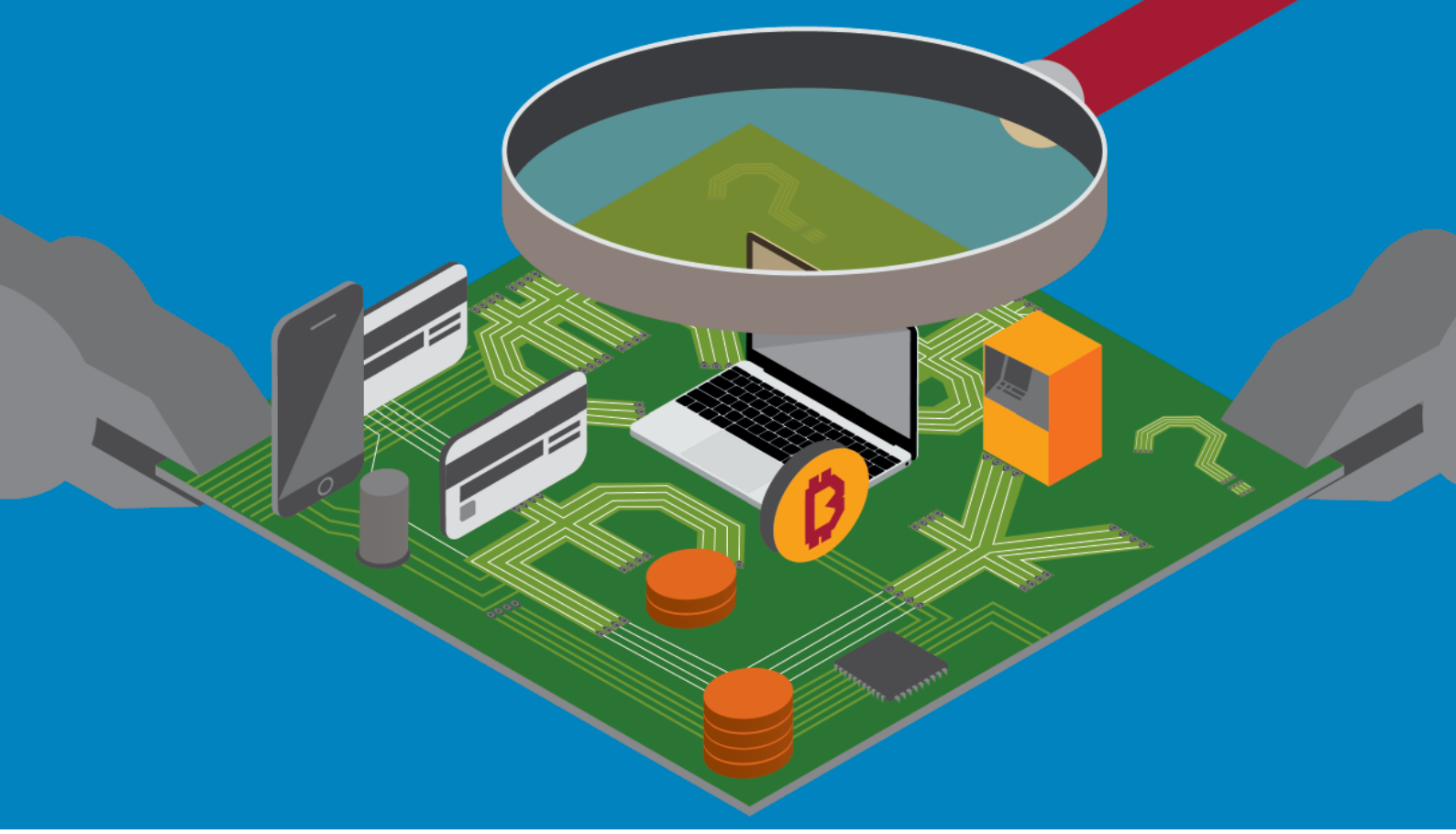


FINTECH
KEY ISSUES FOR OPERATING FINTECH BUSINESSES

Guy Potel, Gavin Weir, James Greig, Philip Trillmich, Carsten Lösing, Tim Hickman, Hyder Jumabhoy and Klementyna Zastawniak of White & Case LLP consider some of the key areas of risk involving fintech businesses of which potential investors should be aware.

If you ask three financial services business people what financial technology, or "fintech" means to them, you will probably receive three, or even more, answers. The term fintech means different things to different people depending on where in the financial services ecosystem they operate.

Fintech covers a broad range of new and developing technologies as well as alternative financial products and service distribution models, from so-called challenger banks and specialist finance providers at one end of the spectrum, to distributed ledger technology (DLT) innovators at the other end. Fintech can be consumer-facing, internal business-facing or even embedded in financial services market infrastructure.

Irrespective of whether fintech is perceived as an enabler or disruptor of business models, the reality is that change is inevitable as financial institutions jostle to remain competitive in the rapidly changing markets of today. It is no surprise that fintech mergers and acquisitions are on the rise. It seems clear that fintech will continue to drive the evolution of financial services, disrupting some sub-sectors, enabling new developments in others, and providing new and improving infrastructure for the digital age.

Change can be very healthy in the lifecycle of any business, but investment in largely unchartered waters, especially in a heavily regulated financial environment, raises a variety of complex legal concerns (*see box "Checklist of issues in fintech transactions"*).

This article examines some of the key legal risks associated with businesses from across the fintech spectrum. The article focuses, in particular, on regulatory and payments services, intellectual property (IP), and data protection risks.

OVERVIEW OF REGULATORY RISKS

The landscape within which fintech businesses must operate is clearly complex and a wide range of risks and regulatory requirements must be considered. The innovative nature of fintech businesses means that the regulatory framework within which they sit is not always easy to navigate.

In a world of increasing financial regulatory complexity, fintech businesses that currently operate outside the regulatory perimeter may soon find themselves needing to comply with a spider web of legislation. Operating within the regulatory perimeter poses challenges for innovation; the time, manpower and

infrastructure costs associated with understanding, implementing and complying with applicable regulation can be prohibitive for many start-up businesses.

Helpfully, regulators across the EU appreciate the importance of adapting their regulatory and supervisory approaches to balance promotion of sustainable market-based service provision on the one hand, with the need to avoid entry barriers for innovators which are too high on the other hand. One example is the UK Financial Conduct Authority's (the FCA) establishment of Project Innovate and the Innovation Hub and, more specifically, the so-called "regulatory sandbox". In 2016, the FCA selected 24 businesses to test their products, services and delivery mechanisms in a live environment using a specially tailored registration process. Through its regulatory sandbox programme, the FCA seeks to achieve "right touch" supervision by waiving or modifying regulation that, in the context of a particular fintech business, may be unduly burdensome or which is not achieving its purpose. The regulatory sandbox is part of the wider Project Innovate that aims to support the commercial imperatives of start-up businesses, provide flexibility, lower costs and enable access to support and speed to market.

However, regardless of whether a fintech business benefits from the temporary sanctity of the FCA's regulatory sandbox or other similar programmes across the EU, understanding the current and potential regulatory risks associated with a business model is critical. Fintech businesses need to develop and maintain strategies in order to deal with the multifaceted nature of operating and innovating within the financial services sector and for anyone seeking to invest in, acquire, dispose of or partner with a fintech business, navigating the legal complexity involved will be essential. While many participants in the fintech sector say that they do not believe fintech businesses should be subject to tighter regulation, the most commonly cited barrier to deal-making is the lack of regulatory clarity (*see box "Survey responses"*).

Regulatory framework

In considering regulatory challenges, one of the key points for those interested in fintech to remember is that regulation always trails innovation and only rarely will regulation be specifically designed to address particular technological advances while those advances are in their early stages of development. This means that technological innovators need to think about how their novel ideas will fit into existing regulatory frameworks if their nexus with the real economy or market place involves them in producing products for marketplaces which are otherwise tightly regulated.

This is particularly true in the financial services sector, where regulation bites on virtually every aspect of the business and operations of financial services firms, whether they are at the consumer facing front-end, interacting with the public as buyers of financial services or they are at the other end of the spectrum, involved in providing financial market infrastructure services, keeping the plumbing and wiring of the financial markets open and functioning. Regulation will bite in different ways at different points in the supply chain, with focuses varying between consumer and conduct facing rules through to regulatory

Checklist of issues in fintech transactions

In-house lawyers and practitioners should consider the following questions when advising potential investors in, or buyers of, fintech businesses:

Regulatory

- Does the business currently conduct any regulated activities, either in the UK or elsewhere? Does the business have the relevant regulatory permissions to operate?
- If not currently required to be authorised, is it reasonably likely that the business may need to become authorised in the future? Which regulatory framework(s) could apply to the business? How prepared is the business to navigate the regulatory approval processes, including evidencing sufficiency of internal systems and controls?
- Is regulation that is currently in the pipeline an opportunity or a threat for the business? How does the business's business plan fit within the upcoming regulatory framework? Is the business correctly positioned to respond to that regulation?

Intellectual property and information technology

- Which intellectual property assets are material for the operation and success of the business? Does the business own or at least have the exclusive right to use all of the assets? If a brand identity is integral to the success of the business, does the business own registered trade marks to protect that identity?
- What are the risks relating to the business' intellectual property, such as third party infringement or patent troll attacks? Does the business have the right infrastructure and governance to develop, exploit and protect its intellectual property?
- What IT systems does the business use? Is this IT scalable to meet demand? Are these IT systems compatible with the buyer's existing systems? Has enough time and budget been reserved for data migration and testing?

Data protection and cyber security

- Does the business rely on the collection, analysis or transfer of personal data?
- Does the business have a programme in place which will enable it to comply with the General Data Protection Regulation (*2016/679/EU*) by 25 May 2018?
- Are the business's protocols and systems sufficiently malleable to enable the business to comply with data processing requirements even if the ways in which the business processes data change?
- Are the business's technical measures, monitoring and training policies and practices sufficiently robust to withstand cyber attacks? Does the business have appropriate protocols for responding in event of a cyber security breach?

requirements that systems be robust, stable and protected from operational risks that could result in systemically significant failure (*see box "Examples of the regulation of fintech").* Also, regulation can affect a particular innovation in a number of different ways, which can be different depending on the jurisdiction where the innovation is being launched.

All of these factors produce a regulatory environment where regulators will be keen to:

- Understand what a particular innovation will do, how it will work and what the risks and rewards will be not only to consumers but also for them as regulators.
- See how the particular innovation fits into the existing legal, regulatory and prudential landscape, so that they can understand what sections of the rule book apply.
- Understand what particular conduct, operational or stability issues or risks the innovation may give rise to.

Recent commentary on fintech regulation

These various strands can be discerned from a number of recent speeches and papers from leading regulators on their attitudes to various fintech areas of innovation. The most notable among these was a report from the European Securities and Markets Authority (ESMA), in which ESMA set out its views on how DLT might affect securities markets and how it saw potential for risks, including as yet unidentified risks, arising (*www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf*).

The second was a major speech by Mark Carney, Governor of the Bank of England, in January 2017 in which he discussed the potentially significant effect of fintech, but balanced potentially benign effects with some equally worrying points about possible systemic and societal risks and the need for both real regulatory engagement, but also for regulatory caution (*www.bankofengland.co.uk/publications/Documents/speeches/2017/speech956.pdf*).

Finally, the Bank for International Settlements Committee on Payments and Market Infrastructures issued a paper in February 2017 on DLT in payment, clearing and settlement which usefully summarises DLT technically and then poses some useful but difficult questions for regulators and innovators to consider (*www.bis.org/cpmi/publ/d157.pdf*).

The effect is that innovators in fintech need to be aware that, while regulators are interested in what they are doing, this interest is coloured by a significant level of caution. In turn, this means that technological innovators need to think at an early stage where in the financial services supply chain their new idea will sit, in order to work out what part of the current regulatory regime will be relevant.

Cross-border implications

Innovators also need to bear in mind that, given there is no harmonised or overarching regulatory framework within which fintech innovations can slot. At the moment, regulators in each jurisdiction are looking at fintech developments against their own rule books. Some regulators are keen to understand and work with innovators; the FCA, the Bank of England, the German Federal Financial Supervisory Authority (BaFin) and the Singaporean Monetary Authority are good examples. Others have not been quite so welcoming.

However, this means that, at the moment, cross-border application of fintech which implicates a regulated area of activity means getting the innovation past regulators in both locations, or as many locations as the technology will be used. That is not necessarily straightforward and slows down the network benefit reward that fintech should deliver.

PAYMENT SERVICES

In terms of general legal requirements, the Directive on payment services in the internal market (*2015/2366/EU*) (2015 Directive), also known as the second Payment Services Directive or PSD2, is of particular importance to fintech businesses, in particular those fintech companies that provide services in the payment space and focus on payments. The deadline for implementation of the 2015 Directive by each EU member state is 13 January 2018, well ahead of the likely timing of Brexit and the implementation of the UK's departure from the EU.

The 2015 Directive extends the scope of the Payment Services Directive (*2007/64/EC*) (2007 Directive) and supplements existing regulatory provisions in the payment services sector, such as the Regulation on interchange fees for card-based payment transactions (*2015/751/EU*) (MIF Regulation), the second Electronic Money Directive (*2009/110/EC*) (Second E-Money Directive), the Payment Accounts Directive (*2014/92/EU*) and the Single Euro Payments Area Regulation (*260/2012/EU*) (SEPA Regulation) (*see feature article "New payment services regime: preparing for a revised landscape", www.practicallaw.com/8-630-5425*).

Fintech and the 2015 Directive

The rationale behind the 2015 Directive is to establish a framework to respond to the significant innovation within the payment services sector, which has left certain regulatory gaps and legal uncertainties. The 2015 Directive will be the basis for innovative processes and products in the payment service sector, such as mobile payment wallets, while ensuring that payment service providers are able to launch safe, secure and easy-to-use digital payment services with sufficient legal clarity, a high level of security and adequate protection of consumer rights in terms of payment data protection and unauthorised bank transfers. Therefore, subject to certain specific exemptions, the 2015 Directive will be relevant to any fintech company in the payment area, from payment or e-money institutions to businesses which deal with electronic vouchers or gift cards.

The business activities which the 2015 Directive expressly regulates are set out in Annex I to the 2015 Directive. The list includes several business activities which also came within the scope of the 2007 Directive, such as execution of payment transactions through a payment card or similar device and services enabling cash withdrawals from a payment account, but it has also been extended to include two new services and the respective new payment service providers (*see "New regulated services" below*).

Consequences of non-compliance

The consequences of a business failing to comply with the 2015 Directive are very severe. Under the 2015 Directive, the competent authorities are entitled to take various actions as part of their supervisory role in order to ensure continued compliance with the 2015 Directive, from issuing recommendations or guidelines to suspending or withdrawing authorisation issued to a payment institution.

Member states are also required to provide that their respective competent authorities may adopt or impose any penalties or

Examples of the regulation of fintech

To illustrate the variety of regulations that can apply to a fintech business, three possible areas where a fintech innovation may be being developed are considered below to see what particular regulatory areas will be pertinent.

A crowdfunding website	The business will need to think about conduct rules (consumer credit, disclosure, enforcement, interest rate rules) and client suitability rules and whether its underwriting algorithms are potentially discriminatory. It will need to consider anti-money laundering and "know your client" processes. It will need to consider data protection issues and, in due course, will need to consider cyber security and, possibly, payments issues. However, any requirements relating to operational stability and systemic issues are likely to be less stringent for this type of business.
A payment tech innovator	The business will need to think about the complicated web of regulation around payment services, about data protection and cyber security. It will also need to be able to assure its counterparties that it is a secure and safe platform for others to use to intermediate regulated activity. It will need to be very clear about its own business model and consider whether it will have the effect of removing intermediaries from the process. It should consider whether it will actually develop to carrying on regulated activity in its own right, such as the direct provision of banking services.
A distributed ledger technology (DLT) innovator in the clearance and settlement sector	The business will need to think about stability, interoperability and cyber security in equal measure. Central banks will be examining any DLT innovation very closely to see how it will affect the financial services supply chain.

measures required to end any breaches of the 2015 Directive. These enforcement powers may be extensive; for example, the FCA and BaFin both have the power to impose fines on firms and individuals, and to name and shame them publicly. Other FCA powers include applications to the courts for injunctions and to initiate criminal prosecutions where unauthorised business is undertaken.

Extension of geographical and material scope

The 2015 Directive significantly amends the existing regulatory framework for payments within the EEA. It seeks to strengthen the regulatory framework for the single market in the EEA for wire transfers, direct debits and other non-cash payment methods and to respond to the latest technical innovations. It does so by extending the scope of the 2007 Directive (which already covers all EEA-currency payments, where the payment service providers (PSPs) of both the payer and payee are located within the EEA) to all currencies between EEA-domiciled PSPs and to so-called one-leg payment transactions (where one PSP is located outside of the EEA and the other within the EEA) in any currency.

Certain specific exclusions that previously allowed particular business activities to remain outside the scope of the 2007 Directive have been restricted. This includes the limited network exemption that was available for specific purpose instruments such as store cards or public transport cards. These are no longer permitted to develop into more general purpose instruments on an unauthorised basis.

Furthermore, the exemption available to telecoms operators for digital goods has been limited under the 2015 Directive and only covers payments made through telecom operators for the purchase of digital content up to a value of €50 per transaction, or where the cumulative value does not exceed €300 per month for an individual subscriber or for a pre-funded account. Payments transmitted by a telecoms operator for the purchase of physical goods and services will be considered a regulated activity under the 2015 Directive.

In practice, this means that the scope of regulated activities is significantly expanded. PSPs falling under the 2015 Directive and operating in the EU will, for example, need to provide information and transparency on the charges and conditions relating to national and international payments, and similarly, be held liable in the event of a problem attributable to them.

New regulated services

As mentioned above, the list of business activities expressly regulated by the 2015 Directive has been extended to include two new services and the respective new PSPs. These are:

- Payment initiation services, with the respective provider being called the payment initiation service provider, for example, Apple Pay or PayPal in the UK, Sofort in Germany, IDeal in the Netherlands or Trustly in Sweden.
- Account information services, with the respective provider being called the account information service provider, for example, Mint in the UK, which provides consolidated information on multiple credit cards and bank accounts.

A payment initiation service is defined as a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another PSP. The provider, where the customer's account is held, is called the account servicing PSP. Payment initiation service providers are considered payment institutions and are required to go through the complete licensing process that would prove that they are able to fulfil the various requirements to become authorised to offer payment services, including capital and organisational requirements, risk management capabilities, personal reliability of its officers and shareholders and anti-money-laundering capabilities to name just a few.

An account information service is defined as an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another PSP or with more than one PSP. An account information service provider does

not require a license to perform account information services, but simply needs to register and prove that it holds the required professional indemnity insurance. The European Banking Authority (the EBA) will develop a publicly available electronic central register, identifying the payment services for which each payment institution is authorised or for which an account information service provider is registered.

Consumer rights

The 2015 Directive will also strengthen consumers' rights in several ways. Firstly, the 2015 Directive provides for an unconditional refund right for a period of eight weeks from the date when the funds were debited. While this already applies under the SEPA Regulation core direct debit scheme as a contractual right between the scheme's participating members through an adherence agreement, the 2015 Directive will provide a legislative basis for this right.

Secondly, except in cases of fraud or gross negligence by the payer, the amount of the payer's maximum liability for payments that have not authorised by him has been reduced from €150 to €50. Thirdly, the 2015 Directive provides that the payee may not request charges for the use of payment instruments for which interchange fees are regulated under Chapter II of the MIF Regulation and payment services to which the SEPA Regulation applies. This means that where card charges imposed on merchants are capped in accordance with the MIF Regulation, merchants cannot impose any surcharge on customers for card-based transactions both online and in shops, for example, by charging additional fees for using a credit card when booking a holiday online.

Fourthly, where the final amount of the transaction is not known in advance, for example, when booking a hotel, renting a car or when pre-authorising petrol purchases at petrol stations, the payee will only be able to ring-fence funds on the payer's card account where the cardholder has approved the exact amount that can be blocked. The payer's PSP is required to unblock those funds without undue delay once information about the exact final amount is received and, at the latest, after having received the payment order. Finally, PSPs must put in place dispute resolution procedures and will generally be required to respond to payment complaints within 15 business days of receipt.

Practical implications of the 2015 Directive

Fintech businesses will need to be proactive in responding to the changes to the scope of regulated activities, which reflect recent technological developments and a trend towards customers that have multiple relationships with PSPs and an increased need for interaction. Third-party PSPs frequently use application programming interfaces which make it easier for software developers to access different databases or applications. This represents a major paradigm shift in the EU payments area. It will now be mandatory for traditional banks to grant third parties access to customer data, both under the 2015 Directive and also, in the UK, under the Competition and Markets Authority's Open Banking Initiative, which requires banks to enable customers and small businesses to share their data with other banks and third-party PSPs to enable customers to manage their accounts with multiple providers through a single digital application.

This will have a major impact on systems and operations as account servicing PSPs will need to enable third-party providers to access their online payment accounts. They need to ensure that they can respond to requests for payment initiation and account information where the customer has given their explicit consent. Account servicing PSPs need to process payment orders received from licensed payment initiation service providers and data requests from registered account information service providers and grant access to these services in an objective, proportionate and non-discriminatory manner. The rules on access of authorised or registered PSPs need to be objective, non-discriminatory and proportionate and they must not inhibit access more than is necessary to safeguard against specific risks, such as settlement risk, operational risk and business risk and to protect the financial and operational stability of the payment system. Any rejection of the requesting payment service needs to be justified by the account servicing PSP by providing the full reasoning behind it.

In turn, third-party PSPs will need to comply with certain security requirements. In order to be authorised as a payment institution, third-party PSPs will need to provide extensive documents to the competent authority, including evidence that it holds sufficient initial capital, which ranges from €20,000 to €125,000 depending on the type of payment service being provided. Certain security requirements will also need to be complied with, for example, account information service providers will need to hold professional indemnity insurance or a comparable guarantee covering the territories in which they offer services. PSPs will also ensure that they have the necessary organisational and technical infrastructure in order to carry out their regulated business activities in compliance with the 2015 Directive.

Further practical considerations which should be taken by PSPs are in relation to strong customer authentication requirements where the payer accesses its payment account online, initiates an electronic payment transaction or carries out any actions through a remote channel which may imply a risk of payment fraud or other abuses. Strong customer authentication is a procedure based on the use of two or all of the following elements:

- Knowledge; that is, something only the customer knows, for example, a pin code.
- Ownership; that is, something they own, for example, a mobile phone.
- Inherence; this is, an individual characteristic of the customer, for example, a fingerprint.

These elements must be mutually independent. As provided under the 2015 Directive, regulatory technical standards (RTS) on strong customer authentication and common and secure communication have been developed by the EBA in order to specify the exact requirements and application of strong customer authentication (the standards). The EBA published its final draft RTS on 23 February 2017 (*www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2*).

The standards will have practical consequences for many fintech businesses in the payment services sector so will need to be considered by these businesses. For example, PSPs are exempted from the application of strong customer authentication where the payment is initiated from an unattended

payment terminal in relation to payment of a transport or parking fare. The final draft of the standards has also increased the threshold for remote payment transactions from €10 to €30, which means that many payments may not require strong customer authentication.

Outlook for fintech

Advance planning and preparation for the changes brought in by the 2015 Directive is critical. Traditional banks have been considering the extent of the requirements that they can impose on third-party PSPs in order to grant access to their accounts while ensuring that the rules remain objective, non-discriminatory and proportionate. On the regulatory side, certain non-bank PSPs are considering whether they are now required to fulfil the licensing requirements under the 2015 Directive due to the reduction in scope of exemptions granted under the 2007 Directive.

The 2015 Directive has also prompted some companies to consider restructuring their business models or to scan the market for new business opportunities in the market. In particular, traditional banks will need to decide how far their strategy needs to change to comply with the 2015 Directive. This could range from making only the necessary changes to ensure basic compliance with the 2015 Directive, to teaming up with third parties (including fintech businesses) to provide compliant services (for example, authentication services), to restructuring entirely to go beyond the requirements of the 2015 Directive and create in-house capabilities to develop new products and services to stay on top of innovation in this area.

Fintech businesses will also need to be aware of any further ongoing changes alongside the 2015 Directive. In particular, the standards to be adopted by the European Commission in spring 2017 and to be implemented by member states 18 months thereafter (presumably from November 2018) and the alignment of the Second E-Money Directive to the 2015 Directive might bring further changes to the regulatory landscape. As such, market participants should remain vigilant and monitor the regulatory developments.

INTELLECTUAL PROPERTY

Fintech businesses rely heavily on software, databases, other technology, data and trade secrets. These assets often provide an important advantage over competitors. For fintech businesses that offer consumer-facing services or products, branding is another important asset, in particular in an industry where the ability to grow a brand identity and keep a loyal customer base is often one of the most important factors for success. Most of these assets are or can be protected through intellectual property rights (IPRs) or, in the case of trade secrets, through other legal mechanisms, such as the law of confidential information under English law.

IP for fintech businesses

Each fintech business is well advised to develop and implement an IP and trade secrets strategy, ideally from the early stages of the business. This type of strategy should cover the creation, acquisition, protection, use, exploitation and enforcement of IP and trade secrets, and procedures to avoid infringement of third-party IPRs or the unlawful use or disclosure of third-party trade secrets.

Copyright is the most relevant type of IPR for many fintech businesses because it is the IPR that generally protects software, which is often the most valuable IP asset in a fintech business. Under certain circumstances, copyright can also protect databases, which are another important type of fintech assets. Copyright subsists immediately on creation of the relevant work, without the requirement for any additional act, such as a grant or a registration.

However, a corresponding disadvantage is that establishing ownership of copyright is often complicated, in particular in relation to software, because it requires establishing precisely which individual created which part of the software. Also, software and databases will often be developed through collaboration of a number of individuals. This can create particular problems resulting from joint ownership. One of the most important operational and strategic tasks for a fintech business in the area of IP will therefore be keeping a record of all software and databases created for the business and the contributions of each relevant individual. Another important task is to put in place, from the beginning, the necessary contractual arrangements to ensure that all copyrights in relevant software and databases, along with all other IPRs in relevant materials, vest in, or are assigned to, the business on creation or development. Trade secrets should be protected through contractual confidentiality provisions, and ideally also by restricting access to trade secrets to individuals who need that access in order to fulfil their respective tasks for the business (*see feature article "Trade secret protection: guarding against a global threat", www.practicallaw.com/5-637-7032*).

Beyond copyright and trade secrets, fintech businesses should determine on a case-by-case basis whether other IPRs, in particular registered rights such as patents, registered designs or registered trade marks, are available to protect their intangible assets. Filing applications to be granted or to register these rights requires the investment of time and money, in particular, application fees, other official fees, and counsel fees for preparing and prosecuting the applications. Fintech businesses should therefore decide whether it makes strategic and economic sense to apply for registered rights.

IP for buyers or investors

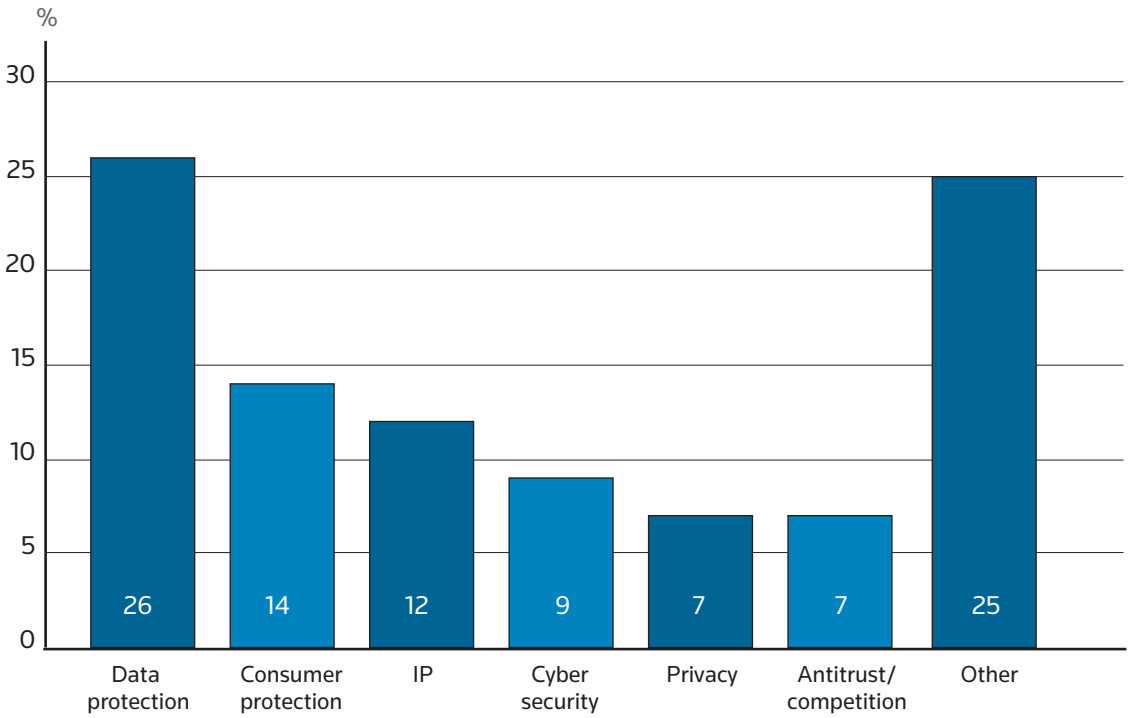
Anyone interested in acquiring or investing in a fintech business should certainly include IP and trade secrets in the due diligence exercise, in order to identify and assess any related risks and, where possible, remedy them, and to assess the value of IP or trade secrets owned or used in the business. A large number of players in the fintech industry feel that doing due diligence on intangible assets is one of the top three biggest challenges to fintech deals (*see box "Survey responses"*).

Working out who owns the IPRs in assets is often complex and requires rather extensive fact-finding exercises, in particular with respect to software and databases. Any fintech business that has documented the creation of all software and databases as well as the contributions of each relevant individual, and that has procured ownership of all IPRs in the software and databases and all other IP created or acquired for the business, will be a more attractive target for an acquirer or investor.

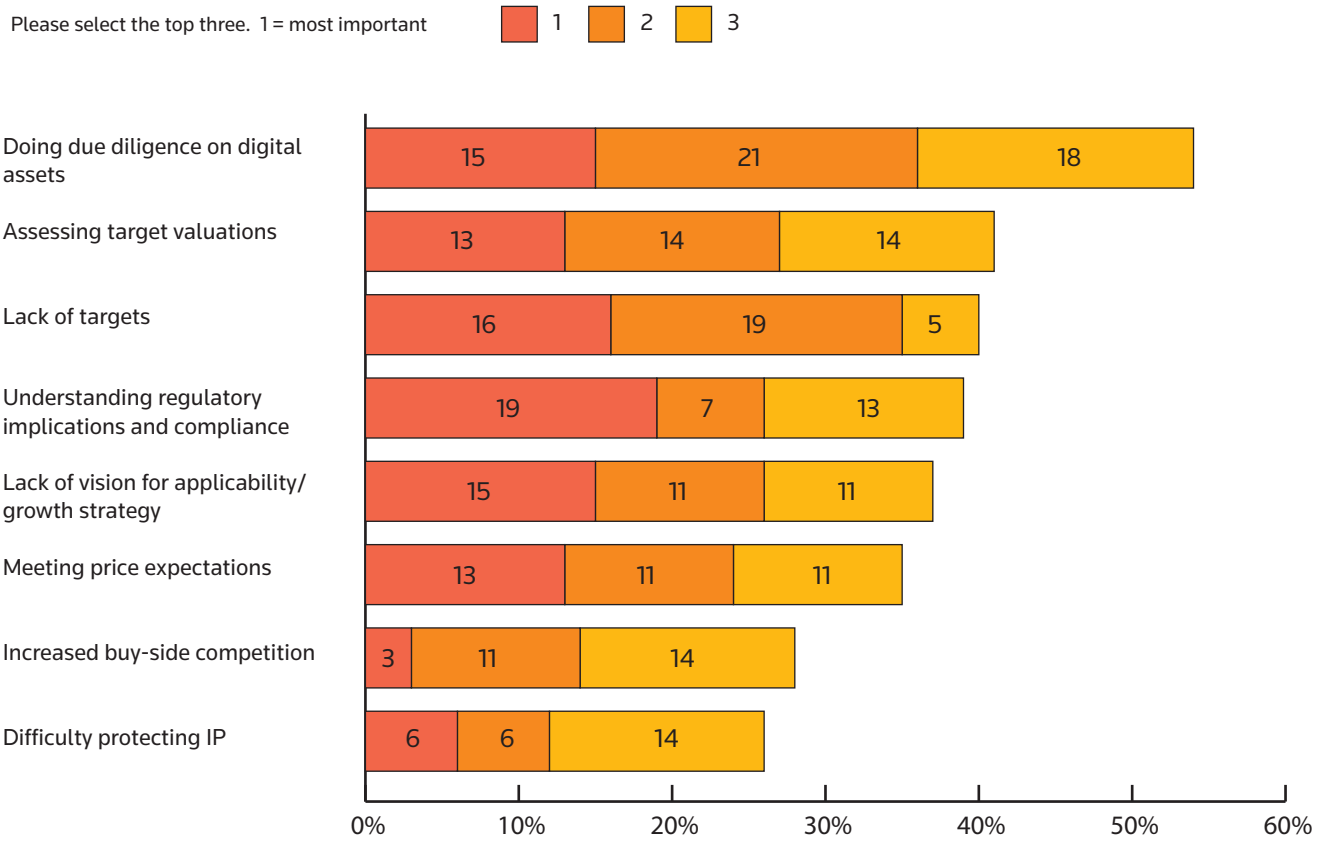
It can also be difficult for potential acquirers or investors to assess the risks related to IP assets, including the risks that the rights in those assets will be infringed by third parties, or that the use of those assets by the target business infringes third party rights. Further risks in connection with software-focused fintech businesses may result from the use of open source software (OSS). Some OSS licences require, as a condition for the use of the OSS, that the source code of any software derived from OSS products must be made available, or that the derivative software must be provided for free. These requirements

Survey responses

Are there any specific regulatory or compliance issues you find challenging?



What do you perceive as the biggest challenge for fintech deals?



Source: Fintech M&A: From threat to opportunity, White & Case LLP.

significantly limit the possibility to exploit the derivative software commercially.

A further risk comes from patent trolls, which are increasingly targeting fintech businesses, in particular those using distributed ledger technology, with the aim of extracting money through forced licensing arrangements by threatening to enforce patents primarily obtained for that aim.

Another big challenge for potential acquirers of, or investors in, fintech businesses is establishing the value of IP assets, which typically represent a large portion of the overall value of a fintech business. Even though a number of valuation methods are available, accurately vetting the value and growth potential of fintech start-ups that may not even be profitable at the time of acquisition can seem like a shot in the dark.

IP in collaborations

Businesses looking to collaborate in fintech will have to conduct due diligence on the IP assets of their envisaged partners and to reach agreement on issues such as the contribution of existing IP and sometimes IP developed outside the collaboration, the ownership of IP developed within the collaboration, rights to use that IP, the management, protection, exploitation and enforcement of that IP, as well as the rights of each collaborator on leaving the collaboration or termination of the collaboration.

DATA PROTECTION AND CYBER SECURITY

The ability to collect, analyse, manipulate, and transfer data is crucial to almost every fintech business. Without the free flow of data, much of the fintech industry would grind to a halt. However, in many parts of the world, and especially in the EU, the desire to use and share data conflicts with data protection laws. Those laws restrict the ability of fintech businesses to use data for certain purposes, place limits on the duration for which data can be retained, and grant broad rights to individuals with respect to their data.

Historically, data protection compliance has not been viewed as a major problem in fintech, because the cost of non-compliance under the current regime is so low. At present the maximum fine for a serious breach of EU data protection law is typically less than €1 million in any given member state, and average fines for first offences are well below that level. In addition, many of the national data protection authorities in the EU have limited budgets, and have therefore tended to focus their efforts on the worst offenders, meaning that many businesses could get away with a certain level of non-compliance. However, the data protection regulatory landscape is undergoing a drastic shift.

The GDPR

On 25 May 2018, enforcement of the General Data Protection Regulation (*2016/679/EU*) (GDPR) will begin, bringing with it stricter limits on how businesses can use data. There are two key reasons why the GDPR poses dangers to fintech businesses:

- It dramatically escalates the maximum fines for data protection non-compliance, up to the greater of €20 million, or 4% of worldwide turnover. Consequently, the risks associated with non-compliance become much more serious.
- It contains aggressive extraterritoriality provisions, meaning that non-EU fintech businesses may become subject to the GDPR as a result of doing business in the EU, even if they have no physical presence in the EU.

In light of these risks, it is not surprising that many fintech businesses identify data protection as their greatest regulatory challenge (*see box "Survey responses"*).

Fintech businesses and the GDPR

One of the reasons why GDPR compliance presents such a significant challenge to fintech businesses is that the scope of the

Related information

This article is at practicallaw.com/9-639-9305

Other links from uk.practicallaw.com/

Topics

Securities, markets and investments	topic2-541-9505
Conduct of business	topic2-201-5206
Information technology	topic5-103-2074
Data security	topic8-616-6189
Data sharing	topic2-616-6187
Technology: data protection	topic8-616-6207
E-commerce	topic2-103-1274
Payment services	topic9-103-2034
Regulated activities	topic2-201-5211
Banking	topic7-385-1287

Practice notes

Data protection and new technologies	5-204-0488
Service providers, security and data breach notification	5-549-7832
Payment Services Regulations 2009: background, scope and key terms	8-519-8105
Hot topics: Payment Accounts Directive	9-532-2487
UK implementation of the second Electronic Money Directive	8-506-1503
Regulated activities: issuing electronic money	9-201-9022

Previous articles

New payment services regime: preparing for a revised landscape (2016)	8-630-5425
General Data Protection Regulation: a game-changer (2016)	2-632-5285
Crowdfunding: an alternative source of financing (2016)	3-633-1200
Blockchain technology: emerging from the shadows (2016)	4-634-8506
Challenger banks: risks and rewards for new entrants (2016)	0-630-1959
Big data: protecting rights and extracting value (2015)	1-595-7246
Cryptocurrencies and mobile payments: all change (2015)	4-616-6092
Data transfers in the cloud: the struggle for compliance (2014)	8-581-9685

For subscription enquiries to Practical Law web materials please call +44 207 202 1200

GDPR is so broad. It applies to anything that a business does with any data that relate directly or indirectly to people (personal data). Personal data are found in a wide range of contexts, such as retail banking data, HR records, IP addresses, online advertising cookies, emails, instant messaging apps, and so on. As a result, the task of working out how best to achieve GDPR compliance in a fintech context can be extremely complex and time-consuming.

Practical implications of the GDPR

Even if a fintech business could achieve complete GDPR compliance today, the ways in which personal data are used in fintech change all the time, as new technologies are developed and new business opportunities created. As a result, it is better to think of GDPR compliance as an ongoing process of improvement, rather than a one-time compliance effort. This process of improvement typically begins by working out how a fintech business is using personal data. For example:

- What kinds of data are collected.
- Which legal entities are responsible for making decisions about the data.
- Where the data are transferred around the world.

The aim here is not to map out everything that happens to data within a fintech business, as that is often unfeasible from an IT perspective. Rather, the aim is to identify the areas in which the business is likely to face GDPR compliance risks. Once a fintech business has identified the range of GDPR compliance risks it faces, it is generally advisable to work out which of those risks are most central to the business; for example, compliance risks relating to key contracts or major business operations are likely to be more urgent to address than risks relating to arrangements with minor service providers. In general, the most central risks should be addressed first, and lower priority compliance risks can be addressed at a later date.

One GDPR compliance risk that is likely to affect all fintech businesses is cyber security. The GDPR requires that businesses must put in place adequate security measures to protect personal data from malicious threats, such as third-party hackers, and also from inadvertent threats, such as accidental loss or destruction of data through oversight or negligence. Adequate cyber security in this context includes both technical measures, such as strong password requirements, firewalls, two-factor authentication, and organisational measures, such as ensuring that employees have access only to data they actually need in order to perform their roles, providing employees with adequate training, protecting against social engineering. However, the GDPR provides technical specifications for the cyber security measures that must be put in place. This means that each fintech business is responsible for reviewing its own data processing activities, identifying the cyber security risks that it faces, and ensuring that adequate technical and organisational measures are implemented.

In addition, whenever a business engages a service provider to process personal data on its behalf, it must by law include in the service contract an obligation on the service provider to implement adequate cyber security measures. This requires fintech businesses to review their existing service agreements to ensure that the correct cyber security provisions are in place. There is a risk that, in some cases, service providers may seek to raise prices before they will agree to GDPR compliant cyber security language being included in their agreements.

Outlook for fintech in data protection

For fintech businesses facing these data protection and cyber security compliance challenges, early planning is essential. Enforcement of the GDPR begins in just over 12 months. Fintech businesses will find it very difficult to bring their operations into compliance with the GDPR by this date unless they take its requirements seriously, and commit sufficient time and resources to satisfying those requirements. Because the GDPR affects almost all of the ways in which fintech businesses process personal data, the scale of this task should not be underestimated.

Guy Potel, Gavin Weir, James Greig and Philip Trillmich are partners, Carsten Lösing is a local partner, Hyder Jumabhoy and Tim Hickman are senior associates, and Klementyna Zastawniak is an associate at, White & Case LLP.

The White & Case report "Fintech M&A: From threat to opportunity" is available at www.whitecase.com/publications/insight/fintech-ma-threat-opportunity.