Ireland


Kevin Allen


Peter Walker


Chris Martin

A&L Goodbody

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, including in response to the COVID-19 pandemic. 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, insurance and blockchain applications)?

Fintech in Ireland covers the whole spectrum of financial services and technology industries. At its core, it is centred on the combination of both in order to develop innovative business models which are disrupting the parameters of traditional financial services. Homegrown success stories like TransferMate, Realex Payments, Stripe, CurrencyFair, Fenergo and Fund Recs which operate in Ireland alongside global financial services giants and leading technology companies. These include Google, Microsoft, SAP, First Data, Visa and PayPal in areas such as money transfer and payments, lending, wealth management, crowdfunding, distributed ledger technology and digital currencies.

Ireland continues to build on its long-established record in the financial services and technology sectors. 49% of fintechs surveyed in late 2018 are expecting revenue growth of 100% or greater, with 32% of those anticipating global revenue growth of between 100–500%. According to the Irish Government's "*Ireland for Finance*" Strategy (IFS 2025), there are approximately 430 fintech businesses in Ireland employing approximately 44,000 people, with up to 50,000 people in direct employment in the sector by 2025. Access to a skilled workforce has been a strong contributing factor to the development of the Irish fintech ecosystem. It has established Dublin as a "*booming Fintech hub*" and set its sights on matching the success of top global fintech players such as London, New York, Silicon Valley and Singapore.

One of the most notable trends that emerged over the past year, which has impacted large multinationals and SMEs alike in the fintech sector, has been the establishment of Ireland as a location of choice for fintech businesses looking for a post-Brexit base. Fintechs were forced to consider the impact of Brexit on their business and Ireland has leveraged its relationship with the UK market in this regard. This has contributed to several fintechs, like challenger banks such as Starling and payments companies like Soldo, stating their intention to establish, and having established, operations in Ireland following Brexit.

Ireland has also taken steps to establish itself as a blockchain hub, and the Irish Government signalled its intention to support this area by creating Blockchain Ireland, an initiative to promote innovation and cooperation across companies working with the technology. This has led to ConsenSys and Deloitte developing innovation studios in Dublin, Circle expanding its business internationally and CoinBase having opened an office in Ireland as part of its Brexit plans.

Fintech and associated services have continued to grow throughout 2020 and the pandemic, with an increase in the use of contactless payments, and the ongoing authorisation of new regulated fintech providers.

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

At present, there are no categories of fintech businesses that are prohibited in Ireland. However, depending on the nature of the activities being carried out, certain fintech businesses may be subject to regulatory authorisation and related restrictions.

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)?

Most Irish fintech start-ups are raising funding through traditional funding mechanisms such as venture funding, Government-supported funding and debt. For example, the Irish Department of Finance estimated in 2017 that crowdfunding constitutes only 0.33–0.4% of the SME finance market in Ireland compared with 12% in the UK. Equally, despite the massive global surge in capital raising through initial coin offerings (**ICOs**) and token sales, there have been few ICOs and token sales carried out by Irish companies to date.

We have included further details on the various available funding options below:

Equity
Venture capital firms and private equity investors continue to focus on high potential fintech businesses. The Irish Venture Capital Association recently noted that venture capital had increased during the pandemic, with a 13% increase in investment in Irish tech firms to almost €1 billion, of which approximately 12% went to Irish fintech businesses.

Debt
In addition to traditional lending from financial institutions for small and medium-sized businesses, there are many alternative funding options available for fintech businesses in Ireland. Online financing platforms, crowdfunding and peer-to-peer lending platforms are often used in combination with more traditional sources of funding. Peer-to-peer lending is beginning to gain pace through platforms such as Linked Finance and Flender. The speed at which funds can be raised makes this a particularly attractive option.

Crowdfunding
Ireland does not currently have a bespoke regulatory regime for crowdfunding. However, the EU has published Regulation (EU) 2020/1503 (the **Crowdfunding Regulation**), and the associated MiFID II Amending Directive (Directive (EU) 2020/1504) which will introduce requirements for crowdfunding service providers in terms of both authorisation and conduct of business requirements, as well as a passporting regime for crowdfunding platforms across Europe. The Regulation and associated Directive will apply from 10 November 2021.

ICOs & Token Sales
A small handful of Irish blockchain companies have raised capital through ICOs. As with crowdfunding, Ireland does not currently have a bespoke regulatory regime for token sales and ICOs. However, the CBI has issued warnings to investors (echoing similar warnings from EU regulators) on the risks associated with virtual currencies and ICOs.

However, in March 2018 the Department of Finance published a discussion paper on Virtual Currencies and Blockchain Technology, in which it proposed the creation of an intra-departmental Working Group that would draw on the expertise of multiple State agencies to explore and oversee developments in virtual currencies and blockchain. The Working Group's stated mandate will include "monitoring developments" at EU and global levels in relation to virtual currencies and blockchain, identifying economic opportunities for Ireland in this area, and "considering whether suitable policy recommendations" are required. The tone of the paper is not dissimilar from the approach adopted at EU level by the European Commission in its Fintech Action Plan 2018, in which the Commission committed to "monitoring the developments of cryptoassets and Initial Coin Offerings" together with EU regulators and other international standard setters, with a view to "assessing whether regulatory action at EU level is required". The 2018 Plan was followed by a consultation on digital finance strategy by the European Commission in April 2020, with a summary of responses to the consultation being published in September 2020. These focused on ensuring that the regulatory framework was technology neutral, removing fragmentation in the single market for digital financial services and promoting a well-regulated data-driven financial sector.

On 24 September 2020, the European Commission also adopted a digital finance package, which included details of a digital finance strategy and legislative proposals on cryptoassets and digital resilience, with the aim of developing a competitive EU financial sector that gives consumers access to innovative financial products, while ensuring consumer protection and financial stability.

The OECD also released its Regulatory Approach to Tokenisation of Assets in January 2020 which examined the benefits of asset tokenisation and the challenges to its wider adoption.

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?

Taxation
The attractively low corporate tax rate in Ireland of 12.5% in respect of trading profits is a major incentive for start-ups or companies looking for a location for their business investments. Some other attractive features of Ireland's tax code relevant for IP companies include the R&D tax credit regime, the stamp duty exemption available on the transfer of a wide range of IP, the key employee reward mechanism, Ireland's Double Taxation Agreement network (currently 74 agreements signed and 73 in effect) and the potential effective 6.25% tax rate, under Ireland's Knowledge Development Box, on profits arising from certain IP assets which are created as a result of qualifying R&D activity carried out in Ireland or the European Economic Area (the **EEA**).

Ireland's tax landscape also includes a number of start-up- and entrepreneur-focused tax reliefs including a relief from capital gains tax (**CGT**) for individual entrepreneurs disposing of certain business assets (CGT entrepreneur relief), a tax relief of up to 40% of investments made in certain corporate trades by individual investors (the employment investment incentive) and tax reliefs for entrepreneurs who leave an employment to set up their own company (the start-up relief for entrepreneurs).

Enterprise Ireland
Enterprise Ireland (the State agency responsible for supporting the development of manufacturing and internationally traded services companies) offers a number of support systems:

- **Competitive Start Fund (CSF)**: This fund offers equity investments of up to €50,000 in return for a 10% equity stake. Calls are made throughout the year for specific sectors, and, in June 2018, a specific fintech CSF was announced which was open to companies working in fintech, proptech, artificial intelligence, machine learning, augmented and virtual reality, the internet of things, blockchain and cloud. This resulted in equity investments being made in five fintech businesses. The most recent CSF closed in March 2021, with potential funding of up to €1 billion, which was open to all sectors, including fintech.
- **Innovative High Potential Start-Up (HPSU) Fund**: Enterprise Ireland offers equity investment to HPSU clients on a co-funded basis (similar to a venture capital approach). The funding goes towards the achievement of an overall business plan, rather than funding towards discrete elements of a business plan, such as R&D or employment creation. In 2020, the fund allocated over €48 million (the highest level of funding so far) to early stage companies including fintech businesses.

Industrial Development Authority (IDA)
In addition to providing logistical and practical support to multinational companies (**MNCs**) investing in Ireland, the IDA can in certain circumstances offer grant assistance to MNCs establishing or expanding their Irish activities. For the most part, grant assistance is linked to job creation and is contingent on the company submitting a formal business plan to the IDA. Any potential grant aid is negotiated on a project-by-project basis and is subject to approval of the board of the IDA. Total grants are subject to ceilings as dictated by EU State aid rules.

Ireland Strategic Investment Fund (ISIF)
ISIF is an €8 billion sovereign development fund with a statutory mandate to invest on a commercial basis to support economic activity and investment in Ireland. ISIF has a long-term investment strategy, and therefore can act as a source of "permanent" or "patient" capital that can work to a longer-term horizon than most participants in the market.

ISIF has made a number of high-profile investments in US companies and funds, including Silicon Valley Bank, Polaris Partners, Lightstone Ventures, Sofinnova Ventures, Highland Capital Partners and Arch Venture Partners. In 2020, it invested in Motive Partners Fund II, a specialist private equity firm focused on growth equity and the buyout of investment in fintech business. It has invested across a wide variety of sectors, including various funds targeting financial services and technology.

Other Government-Backed Schemes

- **Disruptive Technologies Innovation Fund**: €500 million has been made available through this fund for projects involving enterprises and research partners by the Department of Business, Enterprise and Innovation. The funding will be available for projects that develop disruptive technologies which transform businesses and have SME participation. The first call for funding has occurred and awards have been made to companies, several of which are relying on artificial intelligence, data analytics and blockchain technology.
- **Startup Refunds for Entrepreneurs (SURE)**: This initiative allows individuals to obtain a refund from the Government of up to 41% of the capital they invest in establishing their own company over a six-year period.
- **Employment and Investment Incentive (EII) Scheme**: This scheme allows individual investors to claim tax relief of up to 40% on investments they make in other companies. The EII scheme is available to unquoted micro, small and medium-sized trading companies, subject to certain exceptions.

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

The first step in an Irish IPO is to decide which market to list in, which essentially depends on the scale of the business and the funding required by the company. The precise listing rules differ in respect of different markets. The Irish stock exchange, Euronext Dublin, offers four markets: Euronext Dublin, which is suited to large companies and requires a minimum of 25% of its shares to be placed in the public and requires a three-year trading record; Euronext Growth, which suits smaller companies (minimum market capitalisation of €5 million) in the early stages as no trading record is required; the Global Exchange Market (**GEM**), which is a specialist debt market; and finally, the Atlantic Securities Market (**ASM**), which is a market dedicated to companies that wish to dual list in both the EU and the US.

General requirements for listing securities on Euronext Dublin (the principal market in Ireland) include the following:

- an issuer must be duly incorporated or otherwise validly established and operating in conformity with its constitutional document;
- securities must conform with applicable laws of the place of incorporation and be duly authorised;
- securities must be freely transferable; however, the ISE may permit securities that are partly paid if there is no restriction;
- expected aggregate market value of all securities must be at least €1 million for shares and €200,000 for debt securities;
- the whole class of securities must be listed; and
- an approved prospectus must be published for the securities.

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

Examples of notable exits include:

- the founder of Realex Payments, an Irish online payment technology, exiting the business in 2015 following a €115 million acquisition by US company Global Payments;
- Irish financial compliance solutions company Kyckr listing on the Australian stock exchange in October 2016; and
- Irish insurance software company Fineos listing on the Australian Securities Exchange in August 2019, raising $211 million.

It is expected that increased M&A activity will continue to be seen within the fintech space. In particular, further consolidation within the emerging payment and regulatory solutions sector is anticipated.

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.

Ireland does not have a specific regulatory framework for fintech businesses. In some cases, fintech businesses will fall outside of the regulatory ambit as they do not involve the provision of services or undertaking of activities which fall within a regulated activity (as defined in legislation).

However, fintech businesses providing regulated activities (as defined in legislation) which cannot avail of an exemption will fall within the existing body of financial regulation and so require prior authorisation from the CBI to conduct business. If authorised, the firms will be subject to Irish legislation and various ongoing CBI requirements, but fintech companies authorised by the CBI can benefit from regulatory passporting across the EU. Payment institutions, electronic money institutions (**EMIs**), investment companies, money transmission businesses and payment initiation and account information service providers are examples of business models which may require authorisation, as will certain crowdfunding platforms when the Crowdfunding Regulation comes into force.

The legislation most likely to apply to fintech businesses are:

- the European Communities (Electronic Money) Regulations 2011, which transpose the E-Money Directive into Irish law and pursuant to which undertakings may seek authorisation to issue e-money;
- the European Union (Payment Services) Regulations 2018, which transpose the Second Payment Services Directive into Irish law and which govern payment institutions and third-party payment services providers (including, for example, payment initiation and account information services);
- the European Union (Markets in Financial Instruments) Regulations 2017, which transpose MiFID II into Irish law and which provide a regulatory framework for businesses who are providing investment services and activities; and
- the Central Bank Act 1971 (as amended), which governs applications for banking licences.

Fintech businesses may also be subject to consumer protection legislation, CBI codes of conduct including the Consumer Protection Code, as well as anti-money laundering and data protection legislation, depending on the services that they are offering.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Cryptocurrencies and cryptoassets are not subject to specific regulation in Ireland, and the CBI confirmed in February 2018 that such virtual currencies do not have legal tender status in Ireland. However, despite the lack of specific regulation, it should be noted that cryptocurrencies or cryptoassets may be subject to the existing regulatory frameworks that are in place.

The Fifth EU Anti-Money Laundering Directive (**5MLD**) imposes obligations on (certain types of) exchanges and wallet providers. Member States were required to transpose 5MLD into national law by January 2010. The Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020, which transposes the remaining provisions of 5MLD, was enacted on 18 March 2021.

In a speech setting out the CBI's Financial Conduct Priorities for 2020, the CBI's Director General of Financial Conduct highlighted that the Central Bank has been developing a supervisory engagement strategy in relation to "virtual asset service providers", in anticipation of the CBI soon becoming responsible for supervising the compliance of such firms with requirements under 5MLD.

As discussed in question 2.1, in September 2020, the European Commission also adopted a digital finance package, which included details of a digital finance strategy and legislative proposals on cryptoassets and digital resilience, with the aim of developing a competitive EU financial sector that gives consumers access to innovative financial products, while ensuring consumer protection and financial stability.

The OECD also released its Regulatory Approach to Tokenisation of Assets in January 2020 which examined the benefits of asset tokenisation and the challenges to its wider adoption.

3.3 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?

Central Bank of Ireland engagement with new entrants

The CBI is mandated as Ireland's financial services regulator. As part of this role, the CBI has encouraged fintech development but also recognises and warns against the potential to blur lines between regulated and unregulated activities and the challenges this may present. The CBI has sought to develop a clearer picture of fintech activity in Ireland with a view to better understanding the implications for regulatory policy and supervisory activity. It has identified a number of areas, including payments, regtech, markets and exchanges, deposits and lending, investment and advice, insurance, analytics, capital raising, crowdfunding virtual currencies, ICOs and the start-up support ecosystem, where they consider fintech to be prevalent. The CBI continues to review the sector and is closely following and actively contributing to the European Supervisory Authority's approach to fintech. However, the CBI's focus is on the risks to consumers from fintech developments and on protecting consumers where activity is not yet regulated.

As part of its fintech engagement, the CBI launched its Innovation Hub in April 2018. This initiative is aimed at providing entities with a point of contact to engage on innovation and fintech. The European Banking Authority has described both innovation hubs and regulatory sandboxes as "innovation facilitators", and the CBI opted to use the former, instead of developing a regulatory sandbox, in its bid to facilitate financial innovation and to better understand new technologies and new ways in which financial services are being designed, developed and delivered. The CBI reported on the Innovation Hub most recently in its 2020 update report.

This reported that the Innovation Hub has had over 250 engagements with firms and individuals, with an approximately 25% year-on-year increase in engagement in 2020 compared to 2019; in total receiving 70 enquiries in 2020. The Central Bank noted two key themes emerging in the 2020 engagements, namely:

i) an increasing shift toward a more data-driven financial sector (with solutions focused on how to enable data transfer by, for example, seeking to register as an Account Information Service Provider, and how to analyse non-financial factors in the digital age); and
ii) the growth and maturity of blockchain in financial services (with more examples of blockchain deployment use cases broadening to be one element in the overall technology stack of a firm's solution, and the increased development of cryptoasset-enabling infrastructure and services).

As part of the CBI's engagement through the Innovation Hub, they have hosted industry events, including information sessions on consumer protection, authorisations and supervision, as well as a "Regtech Sprint Roundtable" to discuss machine-readable rules. The Innovation Hub has, however, proven to be mutually beneficial for both the participants and the CBI, as it has given fintech firms a platform to make presentations to the CBI on their business models and provide them with information on their use of technology. The CBI will continue to use the Innovation Hub as a tool to get better sight of innovation as it occurs in fintech businesses and has highlighted the importance of engaging with innovators early in their development cycle.

The CBI published a discussion paper in 2017 regarding the impact of the digitalisation of financial services on the consumer protection regime. At a speech given by the CBI's Director of Policy & Risk in November 2019, it was indicated that the CBI had the intention of building on that discussion paper in 2020 in the context of a review of the Consumer Protection Code, with a view to updating it so as to ensure its appropriateness for an increasingly digitalised world.

Government engagement with new entrants

In 2015, the Irish Government launched the IFS2020. This aimed to consolidate and grow Ireland's position as the global location of choice for specialist international financial services. A key element of this strategy was the recognition and promotion of fintech as a rapidly expanding area of innovative financial services. To this end, the IDA worked with its clients to determine what role Ireland can play as they plan their future technology requirements.

The successor to IFS2020, IFS2025, was published by the Government in April 2019. The IFS2025 strategy seeks to take account of current and future developments, structured around:

1. Operating environment: ensuring the policy, culture and legislative conditions underpinning international financial services will support growth.
2. Technology and innovation: providing a collaborative approach to addressing emerging challenges and opportunities.
3. Talent: having skilled people to meet the demands of the international financial services sector.
4. Communications and promotion: ensuring that Ireland's international financial services offering is communicated to investors.

The IFF Strategy considers opportunities for Irish financial services actors and of note is the establishment of a Fintech

Foresight Group (**FFG**), which will bring together stakeholders for the purpose of advising legislators on developments in both fintech and general technology for the wider international financial services sector. Chaired by the Banking & Payments Federation Ireland, the first meeting of FFG was held in August 2019, with the most recent being held in August 2020, and brought together public sector representatives, indigenous fintech companies and representatives from domestic and international financial service providers.

The IFF Strategy notes that some of the initial projects for the FFG will include:

- supporting a "virtual digital bridge" from the "Dublin Silicon Docks" to international financial services firms elsewhere in Dublin and other regions;
- enhancing links and collaboration between fintech firms and third-level institutions;
- forging a relationship with the "Grand Canal Innovation District", which seeks to build a sustainable innovation ecosystem in the "Dublin Silicon Docks" area; and
- exploring the potential for formal collaboration agreements with other jurisdictions, and for facilitating a "fintech bridge" from within the EU to other global fintech locations.

Beyond the work of the FFG, some of the other proposals contemplated in the IFF Strategy include the following:

- Enterprise Ireland will launch a promotional campaign about the advantages of Ireland for fintech and paytech firms, and hold a seminar aimed at fintech firms relating to driving operational excellence;
- an assessment of overseas models of fintech accelerators and hubs and their suitability in an Irish context;
- an industry-led "Financial Foundry" to promote the sharing of ideas, testing of concepts, development of prototypes and building of partnerships between fintech and related firms;
- over the life of the IFF Strategy, Enterprise Ireland's "Global/Sector Financial Services Team" will drive the global expansion by Irish-owned financial services and fintech companies by working one-to-one on their business plans;
- Enterprise Ireland will assess the role of smart cities and towns in Ireland; and
- in terms of talent, the IFF Strategy highlights a key requirement for the success of the strategy being the availability of sufficient numbers of people with the skills needed. Skillnet Ireland is an enterprise-led body that provides companies with opportunities to develop relevant training solutions.

3.4 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?

A fintech business wishing to provide regulated services in Ireland, regardless of whether the business is based in Ireland or not, must either obtain authorisation from the CBI, avail of an exemption or "passport" into Ireland from another EU Member State.

Some key points to note in this regard are:

- Firms wishing to establish a regulated fintech business in Ireland must engage in the CBI's authorisation process. The CBI's key principle is that the firm's "heart and mind" must be in Ireland, as shown by the firm having its principal place of business in Ireland, sufficient senior management presence and demonstrating a high level of decision-making. It is expected that key leadership positions will operate from Ireland, including roles such as chief executive, head of finance, head of operations and head of compliance.
- The CBI will require the board to be of a sufficient size and have sufficient expertise to enable it to adequately oversee the company's operations, and have at least one independent non-executive director (such role is often filled by an Irish resident).
- There is no set minimum number of staff. Headcount will be driven by the levels of business activity planned and is to be discussed with the regulator. Outsourcing arrangements are permitted but must be documented in clear legal agreements.
- The CBI also requires firms applying for authorisation to be adequately capitalised. The amount will vary depending on the precise nature and scope of services in respect of which authorisation is required.
- Finally, the CBI will require the applicant to submit a business plan and summary details of all the key policies, processes and procedures which will be put in place in the new business, including detailed anti-money laundering policies.
- Various exemptions apply to the performance of regulated services. These exemptions can be general or apply to a specific area.

Alternatively, a fintech business authorised to provide regulated services in another EU Member State can notify the CBI (via its home stake regulator) that it intends to rely on the EU "passporting" regime to provide those activities in Ireland.

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 Data Protection Act 2018 (**DPA**) and the General Data Protection Regulation 2016/679 (**GDPR**) (together **Data Protection Legislation**) together regulate the processing of personal data and apply to data controllers and data processors in Ireland, in the EU and those outside the EU who offer goods and services to, or monitor, EU residents.

The GDPR, as a regulation, is directly applicable in Ireland and the DPA gives effect to, and provides derogations from, the GDPR under Irish law. A notable derogation is that the DPA has set the digital age of consent in Ireland at 16.

The profile and influence of the Data Protection Commission (**DPC**), the independent authority responsible for dealing with data protection issues in Ireland, has developed an increased status since the implementation of Data Protection Legislation. It has become the lead data protection regulator for many of the world's largest multinational tech companies under the GDPR's one-stop shop mechanism.

In addition, the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, which implement Directive 2002/58/EC (as amended by Directive 2006/24/EC and 2009/136/EC) (the **ePrivacy Regulations**), deal with data protection issues in relation to phone, email, SMS and internet use and will generally apply to data controllers which fall within the scope of the DPA.

In January 2017, the European Commission put forward a new ePrivacy proposal, which was intended to come into force alongside the GDPR on 25 May 2018. The draft ePrivacy Regulation will repeal and replace the current ePrivacy Directive. There have been significant delays in agreeing the text of the Regulation.

However, on 10 February 2021, the European Council agreed its position on the ePrivacy Regulation. This allows the European Council to start talks with the European Parliament on the final text of the ePrivacy Regulation, and marks a significant step forward in the efforts to make the ePrivacy Regulation a reality. Once adopted, the draft text provides for a two-year transition period, starting from 20 days after the publication of the final text of the ePrivacy Regulation in the EU Official Journal.

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

Yes to both questions. Data Protection Legislation applies to organisations not established in the EEA who offer goods and services to, or monitor, EU residents.

The GDPR prohibits transfers of personal data to a "third county", unless that country benefits from an adequacy decision, the transfer is subject to an appropriate safeguard (under Article 46 GDPR), or a derogation (under Article 49 GDPR) applies. Accessing personal data from a third country amounts to transferring the personal data outside the EEA. Appropriate safeguards include (amongst others):

- Use of Binding Corporate Rules (**BCRs**).
- EU-approved contractual provisions known as Standard Contractual Clauses (**SCCs**). The validity of the SCCs was examined by the Court of Justice of the European Union (the **CJEU**) in July 2020 (*DPC v. Facebook Ireland Limited & Maximillian Schrems*) (**Schrems II**). While the CJEU declared the EU-US Privacy Shield invalid, it upheld the validity of the SCCs as a lawful mechanism for data exports, subject to the data exporter and recipient verifying that the level of data protection required by EU law is respected in the third country concerned. Where those laws do not provide adequate protection, supplementary measures must be put in place or the data exporter or DPC must suspend or terminate the transfer. In November 2020, the EU Commission published a new draft set of SCCs for the transfer of data to third countries, which address the Schrems II judgment. The draft SCCs will replace the current SCCs once adopted by the EU Commission. In their current form, the draft SCCs provide businesses with a 12-month grace period to replace their current SCCs with the new SCCs.
- Approved codes of conduct and certification mechanisms, together with binding and enforceable commitments of the data controller or processor in the non-EEA country to apply the appropriate safeguards.

The impact of Brexit on data transfers from Irish controllers and processors to the UK is also of relevance to fintechs based here. The Brexit transition period ended on 1 January 2021, and the UK became a "third country" for the purposes of the GDPR and the transfer of personal data. However, as a result of the Trade and Cooperation Agreement between the EU and the UK being signed on 24 December 2020, personal data can continue to flow freely from the EU/EEA to the UK until 30 June 2021 or until an adequacy decision is adopted (whichever is sooner). The free flow of data during this period is subject to the proviso that the UK does not amend UK data protection legislation in place as of 31 December 2020, and does not exercise specified designated powers (including approving new SCCs or BCRs), unless the EU agrees to same.

The process of granting a UK adequacy decision is ongoing. Adequacy is a decision granted by the European Commission that a third country's data protection regime offers essentially equivalent levels of data protection as that offered by an EU/EEA country. It permits EU/EEA companies to transfer data freely to that third country, without implementing additional safeguards. On 19 February 2021, the European Commission published a draft UK adequacy decision. The publication of the draft decision is the beginning of a process towards its adoption. This involves obtaining an opinion from the EDPB and the green light from a committee composed of representatives of the EU Member States. Once this procedure is completed, the European Commission will adopt the adequacy decision.

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

Regulatory Action

The DPC is responsible for the enforcement of Data Protection Legislation and the E-Privacy Regulations. It has a proactive approach to identifying data protection issues and regularly engages with public and private sector organisations on these issues.

Under the GDPR, the DPC has the power to order controllers or processors to take corrective actions or to impose significant administrative fines on data controllers and processors for non-compliance. Two maximum thresholds for fines are provided for under the GDPR, which apply depending on which data protection obligation has been breached. Businesses may face administrative fines of up to: (a) €10 million or 2% of the total worldwide annual turnover of the preceding financial year; or (b) €20 million or 4% of the total worldwide annual turnover of the preceding financial year. Fines can be imposed in addition to, or instead of, any corrective measures such as reprimands or warnings.

The DPC's enhanced powers provide further protection to data subjects and increase the risk profile for companies processing personal data. Consequently, data protection should be a priority issue for fintech businesses.

In addition, there are a number of criminal offences under the DPA which are punishable by a fine of up to €5,000 and/or 12 months' imprisonment on summary conviction, or a fine of up to €250,000 and/or five years' imprisonment on conviction or indictment, depending on the nature of the offence. Offences under the DPA include:

- enforced access requests;
- unauthorised disclosure by a processor;
- disclosure of personal data obtained without authority;
- offences by directors, etc. of bodies corporate;
- knowingly or recklessly processing data relating to criminal convictions or offences;
- failure to cooperate with authorised officers during inspections, audits, and investigations;
- failure to comply with an information or enforcement notice; and
- obstructing a reviewer in the preparation of a report.

Damages

The GDPR provides data subjects with a right to take civil proceedings to recover damages for pecuniary or non-pecuniary loss (such as damages for distress) and the recitals to the GDPR note that the concept of damages is to be interpreted broadly. This is a significant change from the previous position under the Data Protection Acts 1988 and 2003, where non-pecuniary damage was not recoverable in an action for breach of the duty of care.

Joint and several liability between parties who engage in the same data processing has also been introduced. Claims can be taken against parties jointly where they are collectively responsible for the damage caused, and it will then be for the controller or processor to claim back from the other controller or processor

that part of the compensation corresponding to their responsibility for the damage.

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

The obvious growth in the fintech sector, while considered to be mainly positive, also increases the need for regulation to avoid the abuse of online financial payments.

Data Protection Legislation

- The GDPR contains enhanced security measures and requires data controllers and data processors to implement "appropriate technical and organisational measures" to ensure a level of security appropriate to the risks that are presented by the processing of the data. These measures, where appropriate, should include: (i) pseudonymisation and encryption of the data; (ii) integrity and resilience of processing systems; (iii) the ability to restore availability and access in the event of a physical or technical incident; and (iv) regular testing of security measures. The DPA also requires controllers and processors to take all reasonable steps to ensure their employees and other persons at their place of work are aware of the technical and organisational measures in place to prevent the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, the data concerned.
- As noted in question 4.3, the GDPR provides data subjects with a right to recover for pecuniary and non-pecuniary loss, and the recitals to the GDPR note that the concept of damages is to be interpreted broadly and lists the loss of control over personal data as an example of such damage. As such, controllers or processors may be subject to a claim for damages where a cybersecurity incident arises in causing such damages.
- The DPA has created several criminal offences including unauthorised disclosure of personal data by a processor and disclosure of personal data obtained without authority. The unlawful operation of a computer with the intent of making gain is also a criminal offence under the Criminal Justice (Theft and Fraud) Offences Act 2001.

Payment Services Regulations

- The Payment Services Regulations 2018 (the **2018 Regulations**), which came into force on 13 January 2018, enhance regulation in this area by: (i) increasing reporting obligations applicable to providers offering payment services; (ii) applying new authorisation requirements for providers offering payment services (payment initiation and account information service providers now require authorisation); and (iii) requiring that all remote and online payment transactions meet Strong Customer Authentication (**SCA**) requirements. Although implementation was initially delayed, requirements in relation to SCA were implemented from 31 December 2020.

Cybercrime

- The EU Cybersecurity Act entered into force in June 2019 and introduced an EU-wide certification scheme for ICT products, services and processes. Therefore, companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognised across the European Union. The Act further introduced a new and stronger mandate for the EU agency for Cybersecurity, ENISA. The Cybersecurity Act grants a permanent mandate to the agency complete with more tasks and resources. ENISA will have a key role in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes and informing the public on the certification schemes as well as the issued certificates through a dedicated website. ENISA is also mandated to increase operational cooperation at EU level, helping EU Member States that would request it to handle cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross-border cyber-attacks and crises.
- Measures for a High Common Level of Security of Network and Information Systems Regulations: The European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 were implemented in September 2018, transposed the EU NIS Directive into Irish law, and set out legal measures to boost the overall level of cybersecurity protection. These measures include imposing security requirements and incident notification obligations on banks and other "operators of essential services" together with certain digital service providers. While financial sanctions are available under the Regulations, for corporates it is the possible criminal prosecution that is the main fact to consider. The Regulations provide that where offences are committed by companies, but have been committed with the consent or connivance of one of its directors or other officers, or where such person has been acting with wilful neglect, that person as well as the company is guilty of an offence and may be prosecuted.
- In December 2020, the European Commission proposed the revised NIS Directive (**NIS2**). NIS2 is proposed to replace the original NIS Directive. NIS2 is currently under discussion in the European Council. It seeks to strengthen security obligations for companies, address the security of supply chains, introduce more stringent supervisory measures for national authorities and further increase information sharing and cooperation.
- Also in December 2020, the European Commission and the European External Action Service presented a new EU cybersecurity strategy (https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy), with the aim of strengthening Europe's resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The EU is also working on two legislative proposals to address current and future online and offline risks: an updated directive to better protect network and information systems; and a new directive on the resilience of critical entities.
- The Criminal Justice (Offences Relating to Information Systems) Act 2017 came into force on 12 June 2017. This Act creates a number of cybercrime offences including unauthorised access to information systems (e.g. hacking), interference with information systems or data and use of tools to facilitate the commission of these offences.
- The EU has adopted new rules to tackle non-cash payment fraud. In 2019, the EU directive on combating fraud and counterfeiting of non-cash means of payment (EU Directive 2019/713) was adopted. Member States must implement the new rules under the Directive by 31 May 2021. The main provisions include: harmonised definitions of some online crime offences, such as hacking a victim's computer or phishing; harmonised rules on penalties for natural persons: three to five years of prison, depending on the nature of the offence; assistance and support to ensure victims are sufficiently informed of their rights and citizens are advised on

how to protect themselves from such frauds; and clarification of the scope of jurisdiction to ensure cross-border fraud is tackled more effectively. The Directive provides for minimum rules, so Member States have discretion to go further and implement more stringent rules, including a broader definition of offences or higher penalties.

Regulatory Guidance

- Payment service providers must comply with the European Banking Authority Guidelines on security measures for operational and security risks under the 2018 Regulations. Other categories of fintech businesses regulated by the CBI may need to comply with the CBI's 2016 cross-industry guidance (https://www.centralbank.ie/docs/default-source/news-and-media/speeches/cross-industry-guidance-information-technology-cybersecurity-risks.pdf) in respect of IT and cybersecurity risks.

An organisation which suffers a data security incident may also be subject to a number of separate incident notification obligations, including under financial and payment services regulations, data protection and/or information security regulations.

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

Financial service providers are also required to comply with financial sanction requirements. In addition, Ireland's key anti-money laundering and terrorist financing legislation is set out in the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) (**CJA**).

The CJA involves a combination of risk-based and rules-based approaches to the prevention of money laundering and terrorist financing. Designated persons have statutory obligations to comply with the CJA provisions, including being required to apply customer due diligence, report suspicious transactions and have specific procedures in place to prevent money laundering and terrorist financing. Failure to comply with the CJA is an offence. The CBI has published guidelines to assist designated persons when taking steps to comply with requirements under the CJA.

Ireland implemented the Fourth EU Anti-Money Laundering Directive (**4MLD**) largely through amendments to the CJA. Key amendments include the introduction of requirements around business risk assessments, as well as enhancements to customer due diligence and transaction monitoring requirements. In addition, beneficial ownership rules contemplated by 4MLD were introduced by way of secondary legislation, pursuant to which a new "Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies" was established in July 2019.

As referenced in question 3.2, the Irish Government has taken steps in relation to the implementation of 5MLD and this legislation will impose obligations on the usage of cryptocurrency exchanges and custodians in certain instances. Member States were required to transposed 5MLD into national law by January 2020 but Ireland has yet to do so, although the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020 was enacted in March 2021.

The Sixth EU Anti-Money Laundering Directive (**6MLD**) was published on 12 November 20218. EU Member States were required to transpose 6MLD into national law by 3 December 2020. Ireland has exercised its right to opt out from 6MLD.

Bribery and corruption are criminalised in Ireland under the Criminal Justice (Corruption Offences) Act 2018, which provides for the criminal liability of individuals and companies if an officer, employee, agent or subsidiary has been involved in corruption in order to gain a business advantage for the company.

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

There is no fintech-specific regulatory regime in Ireland. The applicable regimes and legislation are described above. Any other applicable regulatory regimes would probably be specific to the sector in which a particular fintech business operates.

5 Accessing Talent

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

Hiring and Recruitment

Employees are entitled to receive written notification of certain core terms of employment (set out in the Employment Miscellaneous Provisions Act 2018) within five days of commencing employment. All other terms and conditions of employment must be provided within two months of commencement.

Employers must comply with equality legislation not only in the context of existing employees, but also in all aspects of recruitment, including job advertisements and candidate selection. Employers must ensure that in advertising and interviewing for a particular position, they do not give rise to an inference of discrimination on one of the nine protected grounds (gender, civil status, family status, sexual orientation, religion, race, age, disability, or membership of the Traveller Community). The maximum compensation available to non-employees who bring a successful discrimination claim in relation to a job application is €13,000.

Dismissing Staff

"Employment at will" does not exist as a concept in Ireland and employees are protected from dismissal without cause. Dismissal of employees is regulated in Ireland by statute and by the employee's employment contract. All employers are obliged to have in place a disciplinary procedure setting out the steps to be followed by an employer in dealing with issues of concern, such as conduct or performance.

The Unfair Dismissals Acts 1977 to 2015 (the **UD Acts**) govern the dismissal of staff. The UD Acts provide that every dismissal is deemed to be unfair unless it is based on one of the following fair grounds for dismissal:

- capability;
- conduct;
- qualification;
- redundancy of the role;
- competence of the employee;
- statutory prohibition; or
- some other substantial reason justifying dismissal.

The UD Acts provide that the onus is on employers to show the following: (i) substantial grounds justifying the dismissal based on one of the grounds set out above; and (ii) that fair procedures were followed in effecting the dismissal. The extent of fair procedures to be followed will depend on the circumstances and the reason for effecting the dismissal. Failure to follow fair procedures and/or establish a fair reason for dismissal may lead to a finding of unfair dismissal against the employer, notwithstanding the giving of notice.

The UD Acts apply to employees who have obtained one years' service (there are limited exceptions to the one years' service rule). Employees may also bring a claim for discriminatory

dismissal under the Employment Equality Acts 1998 to 2015 (the **EE Acts**) where their dismissal is connected with one of the nine protected grounds listed above, but they have not obtained the requisite one years' service to bring a claim under the UD Acts.

The maximum compensation available under the UD Acts (and the EE Acts for discriminatory dismissal) is: (i) two years' remuneration (five years' remuneration in the case of dismissal resulting from the making of a protected disclosure); (ii) re-engagement; or (iii) re-instatement.

In Ireland there is also a risk of an employee (particularly if they are senior/highly remunerated) applying to the High Court for an employment injunction, often to prohibit their employer suspending, dismissing or otherwise disciplining them on the basis that fair process and/or natural justice has not been afforded to the employee.

Redundancy

Irish legislation provides specific protection for employees where their position ceases to exist and they are not replaced. In a genuine redundancy situation, fair procedures require employers to consult with employees whose roles are identified to be "at risk" of redundancy prior to any final decision to confirm the redundancy of that role. The purpose of the consultation process is to identify any alternatives to the redundancy, including redeployment, etc.

Irish law entitles employees (with over two years' service) to a statutory redundancy payment which is tax-free. It is calculated on the basis of two weeks' pay per year of service, plus a bonus week's pay. A week's pay is capped at €600 per week. Depending on the industry, employers may pay enhanced severance terms, subject to the employees signing waiver agreements; however, this is not mandatory. Any enhanced redundancy package provided may set a precedent (by way of custom and practice) for future redundancy situations.

Where a collective redundancy situation arises, specific statutory consultation obligations and notifications to the Minister for Employment Affairs and Social Protection (as well as to employees via employee representatives) are triggered for the employer. These obligations apply to employers with a workforce of 21 employees or more.

A collective redundancy situation is one that involves making a specified number of employees redundant within a 30 consecutive-day period. A failure to comply with the notification and consultation requirements could result in substantial penalties.

Notice Period

Employees are entitled to certain minimum statutory notice periods depending on their length of service (ranging from one to eight weeks). An employee who does not receive this notice period (or pay *in lieu*) may bring a claim for wrongful dismissal and loss of earnings during the notice period. In practice, depending on the employee's role, their contract of employment may provide for a contractual notice period that is longer than their statutory entitlement.

In circumstances of gross misconduct, an employee may be summarily dismissed without notice or pay *in lieu* of notice. However, it is imperative that fair procedures would be adhered to in respect of any such dismissal to comply with unfair dismissal law (see above).

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

Under Irish law, an employer can engage employees on such terms as it deems appropriate, provided the following mandatory benefits are protected:

- **Annual Leave**: employees accrue paid vacation based on time actually worked, subject to a statutory minimum of four working weeks – pro-rated for part-time employees. Employees are also entitled to a paid day off or an additional day's pay in respect of nine Irish public holidays.
- **Rates of Pay**: the national minimum wage for employees in Ireland is €10.20 per hour. However, this rate may vary in certain sectors of employment, and is reduced for younger employees.

Leave	Entitlement	Obligation to pay
Maternity Leave	Up to 42 weeks (26 weeks' basic leave (State benefit paid by the State) and 16 weeks' unpaid leave).	No statutory obligation to pay. However, many employers top up the State benefit during the basic 26 weeks' entitlement.
Adoptive Leave	Up to 40 weeks (24 weeks' basic leave (State benefit paid by the State) and an additional 16 weeks' unpaid leave).	No statutory obligation to pay. However, many employers top up the State benefit during the basic 24 weeks' entitlement.
Paternity Leave	Up to two weeks' leave (State benefit paid by the State).	No statutory obligation to pay. However, many employers top up the State benefit during the paternity leave.
Carer's Leave	Available to employees with over one years' service to take care of a "relevant person". Up to a maximum of 104 weeks' unpaid leave.	No obligation to pay.
Parental Leave	Available to employees with over one years' service. 26 weeks' unpaid leave per child (up to the child's age of 12 with limited exceptions).	No obligation to pay.
Parent's Leave	Up to two weeks' leave during the first year of a child's life, or in the case of adoption, within one year of the placement of the child with the family (State benefit paid by the State).	No obligation to pay.

- **Pension**: outside of any contractual commitments, there is currently no legal obligation on an employer to establish a pension plan for employees based in Ireland. An employer is not required to contribute to a pension for an employee; however, it is required to provide employees with access to a pension scheme, which may include facilitating deductions to a personal retirement savings account (**PRSA**).
- **Protected Leave**: Ireland has the following protected leaves:

What's on the horizon?

Employers should be aware that the following changes will likely be implemented in Ireland in 2021:

- **Statutory Sick Pay**: Irish employees do not currently have an entitlement to sick pay from their employer. The Irish Government is currently drafting legislation to introduce a limited sick pay entitlement. It is expected that employers will be required to pay employees for a specified number of weeks of sick leave, subject to certain conditions and exemptions. It is expected the scheme will be introduced in late 2021.
- **Remote Working**: The Irish Government recently published a strategy on remote working entitled "Making Remote Work". Legislation is promised which will provide for a general statutory right to request remote work. Employers will likely be required to balance the business's interests with those of the employee in dealing with such requests and to provide objective business reasons if refusing a request. Employees will have a right to appeal any refusal.
- **Right to Disconnect**: The Irish Government has asked the Workplace Relations Commission (the body responsible for the adjudication and enforcement of employee rights in Ireland) to draw up a code of practice on the right to disconnect, which is expected in early-mid 2021. The European Parliament has published a proposed new directive on an EU-wide right to disconnect. Under this directive, Member States would have to ensure that employers take the necessary measures to provide workers with the means to exercise their right to disconnect. It is likely that this proposal will influence the incoming code of practice on this topic.

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

Under emergency public health measures introduced due to the COVID-19 pandemic, there are currently significant restrictions on the issuing of visas and employment permits for Ireland, as well as quarantine requirements upon arrival in Ireland. These travel restrictions are subject to ongoing change so up to date advice should be sought in advance of any travel to Ireland for the foreseeable future.

All EEA nationals have the right to work in Ireland. Non-EEA nationals must have a valid employment permit in order to work in the State. Permits are administered by the Employment Permit Section of the Department of Business, Enterprise and Innovation. There are nine different types of permits which may be applied for depending on the type of employment involved.

Special route for obtaining permission for individuals who work for fintech businesses

As part of a highly skilled workforce, many employees in the fintech industry can apply for a Critical Skills Employment Permit. In order to be eligible for such permits, the employee must have:

- a job offer of at least two years within the State; and
- an annual salary of €64,000 or more.

Jobs with annual salaries of €32,000 or more may also be eligible provided they are one of the occupations listed on the Highly Skilled Occupations List.

The permits are valid for two years, and on expiration, the employee may apply for a "Stamp 4" permission to remain and work in the State without an employment permit. This permission is renewable on an annual basis. Once the applicant has legally resided in Ireland for five years, they may then be eligible to apply for long-term residence permission.

Depending on the circumstances, the following permits may also be applied for in the context of fintech workers:

- **Intra-company Transfer Employment Permit**: Key management staff and management, as well as qualifying trainees, of an MNC can be transferred to an Irish branch of the company with this permit.
- **General Employment Permit**: This may be used where the job in question fails to satisfy the salary requirements of the Critical Skills Employment Permit. However, as applications for this permit must satisfy a "labour market means test", it is not a particularly common form of work permit.
- **Contract for Services Employment Permit**: This enables the transfer of non-EEA employees to work in Ireland whilst remaining employed under their contract of employment outside of the State.
- **Internship Employment Permit**: This permit is available to full-time students enrolled in third-level education outside of the State who have been offered an internship or work experience in Ireland.

Legally resident dependants of employees holding a critical skills/green card employment permit may also apply for Dependant/Partner/Spouse Employment Permits.

Employers and contractors in the fintech industry may also sign up to the Trusted Partner Initiative. Under this scheme, employers can apply for "Trusted Partner" status in order to fast track the permit application process.

Certain senior role holders in fintech businesses providing regulated activities would also need to obtain the CBI's approval prior to taking up that position, under the "Fitness and Probity" regime.

6 Technology

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

The Irish legislative framework gives significant comfort to companies creating and managing their IP assets in Ireland. Patents, copyright, design rights, trade marks and confidential information can be used to protect inventions and innovations. All of the core Irish legislation in relation to these forms of protection has been introduced in the relatively recent past. The Commercial Court, a division of the Irish High Court, deals with major commercial and IP cases on an expedited basis and offers an effective way for fintech businesses to enforce their IP rights. The Copyright and Other Intellectual Property Provisions Act 2019 confers jurisdiction on the District Court and the Circuit Court to hear and determine IP claims, including claims in relation to copyright infringement. This effectively allows for litigants to bring a claim alleging copyright or IP infringement in a more timely manner and at a significantly lower cost than before, when such claims were brought before the High Court or Commercial Court.

Copyright: Typically, copyright is the most useful protection for the kind of IP generated by fintech businesses, e.g.

copyright protects the underlying code in software and computer programs. There is no system of registration for copyright protection in Ireland as copyright attaches automatically on the creation of an original work. Trade secrets can also be useful in protecting software.

Patents: There are two types of patent protection available under Irish patent legislation: a full-term patent (20 years); and a short-term patent (10 years). In order for an invention to be patentable it must: (i) be new; (ii) involve an inventive step; and (iii) be capable of industrial application.

Trade marks and designs: Trade marks may be registered to protect the branding of fintech products and companies. Designs which are new and have individual character can be registered to protect the appearance of products.

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

Under Irish law, ownership of a patent rests with the inventor. If the invention is made by an employee in the course of their employment, the right to a patent will usually belong to the employer. In relation to copyright, the author of a work is the first owner. Similar to patent ownership, if a copyright work is made by an employee in the course of employment, the first owner of the work will be the employer, subject to any agreement to the contrary. Ownership of registered trade marks and designs will vest in the person who has applied for registration.

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

Copyright: Ireland is a party to and incurs obligations under the Berne Convention (Paris Act), the Rome Convention, the TRIPS Agreement, the World Intellectual Property Organisation (**WIPO**) Copyright Treaty, and the WIPO Performances and Phonograms Treaty. These international agreements provide for automatic reciprocal protection for Irish copyright works in the territories of the signatories.

Patents: Patent protection may be secured by applying for (i) national protection in the Intellectual Property Office of Ireland, (ii) protection via the European Patent Convention (**EPC**), or (iii) protection under the Patent Cooperation Treaty (**PCT**) which provides for an international search and examination system. The outcome of an EPC or PCT application will, depending on the results of the search and examination process and application of national patent rules, result in national patents being granted which may be enforced in the jurisdictions in which they are registered.

Plans are still underway to establish a single unitary patent offering protection across EU Member States; as well as a Unified Patent Court (**UPC**). The EU regulations establishing the Unitary Patent system (No 1257/2012 and No 1260/2012) entered into force on 20 January 2013, but they will only apply as from the date of entry into force of the Unified Patent Court Agreement (**UPCA**). The UPCA has faced stumbling blocks delaying its implementation. As matters stand, 15 contracting Member States have already ratified, including France and Italy, and once German ratification is complete it is anticipated that the final steps could be taken to set up the UPC in 2021 (with work likely starting in 2022), but more delays could be encountered. Further, a decision is to be made regarding the location of the Life Sciences Section of the Central Division of the UPC, with London no longer being an option as a result of the UK's withdrawal from the UPCA.

Ireland has yet to ratify the UPCA; a referendum will be required to amend the Irish Constitution.

Trade marks: Trade marks may be secured by applying for: (i) a national registration; (ii) an EU trade mark (**EUTM**) (which offers protection across all 27 EU Member States); or (iii) a registration under the Madrid System which provides for a single application through the national office, resulting in a bundle of national trade mark registrations for the countries designated in the application. Irish and EUTMs may be enforced in the Irish courts.

The impact of Brexit on trade marks is important here. From 1 January 2021, EUTMs and registered community designs (**RCD**) no longer cover the UK. Equivalent cloned UK trade marks and UK registered designs have been automatically created on the UK trade marks and UK designs registries, respectively. The existing EU registrations continue to apply in the remaining 27 Member States. The new cloned UK rights will be treated the same as any UK trade marks or registered designs that were applied for and registered under UK law. They will maintain the filing, priority, UK seniority and renewal dates of the original EU rights. The situation is slightly different for any applications for EUTMs and RCDs that were pending as at 1 January 2021. Those applications were not automatically cloned in the UK, and so applicants will need to re-file in the UK, pay the relevant fees, and, if they want to maintain the filing, priority and UK seniority dates recorded against the corresponding EU application, must do so within nine months (from 1 January 2021).

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

Licensing: In Ireland, licensing IP rights creates revenue streams whilst retaining ownership. An important consideration is that of an exclusive *versus* non-exclusive licence which has the potential to limit the use of the IP to one third party. If, for commercial reasons, an exclusive licence is granted, there are other options available that can be employed to maximise value; for example, by limiting exclusivity to a particular location or limiting the scope of use of the licence, thus retaining the ability to commercialise the same IP in other territories and/or other fields of use with other licensees. In any event, a licensor should retain sufficient control over its IP by ensuring sufficient obligations are imposed on the third party, including provisions allowing the licensor to monitor the licensee's use of the IP and appropriate termination rights. The granting of a licence for a patent, trade mark or design should be notified to the Controller of Patents, Designs and Trade Marks (the **Controller**).

Assignment: In general, assignments of IP must be in writing. One notable exception is that trade marks are now automatically transferred with a business under the European Union (Trade Marks) Regulations 2018 unless there is an agreement to the contrary, or circumstances clearly dictate otherwise. Assignment of patents, trade marks and designs must be registered with the Controller. Copyright may be freely assigned and is not subject to any specific registration requirement.

Granting a security interest: Security may be granted over IP (most commonly patents, trade marks and copyright) under Irish law. Particulars of a security interest which is granted by an Irish company must be registered with the Irish Companies Registration Office within 21 days of the granting of the interest. Security interests granted over patents, trade marks and designs must be notified to the Controller and an original or certified copy of the security interest evidencing the agreement between the parties must be submitted to support the application.

Kevin Allen is a Partner at A&L Goodbody's Financial Services Regulation and Compliance Group. He specialises in financial regulatory law, compliance and corporate governance, with particular expertise in financial services law as it applies to fintech.
Kevin advises banks and financial institutions on all aspects of financial regulation and compliance and related matters. He also advises both Irish domestic and international payment institutions, electronic money institutions, credit institutions, investment firms and other regulated financial services providers on regulatory and compliance issues, including conduct of business and prudential requirements, authorisation and passporting requirements, financial institution acquisitions and disposals, corporate governance and financial sanctions. Kevin also regularly speaks at client and industry events and has published a number of articles on fintech and regulatory matters.
Kevin is recognised as a "Leading lawyer" (*IFLR1000*) and a "Recommended Lawyer" (*Who's Who Legal*). He is a Member of the Irish Institute of Directors Legal Panel and is a former Chair of the Irish Funds Regulatory Working Group.

A&L Goodbody
IFSC, North Wall Quay
Dublin 1
Ireland

Tel: +353 1 649 2338
Email: kallen@algoodbody.com
URL: www.algoodbody.com

Peter Walker is a Partner at A&L Goodbody's Banking and Financial Services Department. His principal practice areas are asset-backed finance (including portfolio sales and acquisitions), debt capital markets, private equity finance, general banking & restructurings.

A&L Goodbody
IFSC, North Wall Quay
Dublin 1
Ireland

Tel: +353 1 649 2202
Email: pwalker@algoodbody.com
URL: www.algoodbody.com

Chris Martin is a Senior Associate at A&L Goodbody's Financial Services Regulation and Compliance Group. He specialises in financial regulatory law, compliance and corporate governance, with particular expertise in financial services law as it applies to fintech. He advises both domestic and international credit institutions, investment firms, payment institutions, and other regulated financial services providers on regulatory and compliance issues, including conduct of business and prudential requirements, authorisation and passporting requirements, financial institution acquisitions and disposals, corporate governance, regulated market requirements, the fitness and probity regime, anti-money laundering and terrorist financing, and financial sanctions. He also advises clients on novel financial services industry structuring matters and on establishing best practice norms. He was ranked by *Chambers* as an Associate to Watch for Fintech in 2019 and 2020.

A&L Goodbody
IFSC, North Wall Quay
Dublin 1
Ireland

Tel: +353 1 649 2604
Email: cdmartin@algoodbody.com
URL: www.algoodbody.com

With an established banking sector in Ireland and a rapidly evolving technology landscape, A&L Goodbody's FinTech Group's legal expertise facilitates a cutting-edge approach to advising companies in this sector. Our clients include domestic and international financial services and technology companies, and our team provides a complete legal service for related legal needs.
We advise on a wide range of fintech matters including: the development, acquisition and use of technologies and services; strategic software development agreements; IT-managed and shared services arrangements; complex transitional services agreements; transactional advice; and business process outsourcing. We also advise clients in relation to technology, financial regulation, compliance, risk management, data privacy, financing, cyber risk and the implications of Brexit.
In addition, A&L Goodbody is a member of the Fintech and Payments Association of Ireland.

www.algoodbody.com

A&L Goodbody