Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

FinTech

Ireland
Walkers

chambers.com

2019

Law and Practice

Contributed by Walkers

Contents

Walkers is a leading international firm that provides legal, corporate and fiduciary services to global corporations, financial institutions, capital markets participants and investment fund managers. Clients are Fortune 100 and FTSE 100 companies as well as the most innovative firms and institutions across the financial markets. The firm has ten offices, in Bermuda*, the British Virgin Islands, the Cayman Islands, Dubai, Guernsey, Hong Kong, Ireland, Jersey, London and Singapore. It advises businesses partnering with or investing in FinTech firms as well as financial institutions and asset managers developing their own FinTech products and services. The FinTech group, which consists of 14 partners and 17 other qualified lawyers globally, also works closely with policymakers, regulators and governments to facilitate appropriate legislation and regulation that keeps pace with innovation. Walkers covers FinTech's core financial industry sectors – asset management, investment, banking, finance, insurance and payments – with particular expertise of advising businesses specialising in blockchain, digital assets and alternative model finance.

*Walkers works in exclusive association with Kevin Taylor, trading as 'Walkers Bermuda', a full-service commercial law firm providing advice on all aspects of Bermuda law.

Authors

Niall Esler is a consultant in the Regulatory Group in Walkers' Ireland office and a member of the Walkers FinTech Group. He specialises in Irish and EU financial services regulation and advises domestic and international payment/e-money institutions, credit institutions, investment firms, asset managers, funds and other institutions. Niall's areas of focus include advising on legislation, regulatory codes and guidance in relation to payment services, e-money, anti-money laundering, banking, consumer lending and investment services, from both a prudential and conduct of business perspective. He has advised on the establishment of investment firms, credit institutions and e-money institutions in Ireland, the implementation of regulatory change projects or remediation exercises, financial institution or utility company M&A, regulated asset sale transactions and the winding down of regulated business. He has also acted for clients facing Central Bank of Ireland inspections, themed reviews and administrative sanctions procedures.

Bill Laffan is an associate in the Regulatory Group in Walkers' Ireland office and a member of the Walkers FinTech Group. He acts for domestic and international banks, investment firms, international payment/e-money institutions, asset managers, funds and fund promoters, and international law firms. Bill advises on all areas of Irish and EU financial regulation and compliance, including PSD 2/e-money, anti-money laundering, MiFID II, CRD IV, market abuse, financial institution M&A, domestic banking regulation and the Central Bank of Ireland's fitness and probity regime. He has advised on the establishment of investment firms, credit institutions and e-money institutions in Ireland, including several large Brexit migration projects, and on the acquisition of multiple Irish-regulated asset managers. He has also acted for clients engaged in Central Bank of Ireland inspections and risk mitigation programmes.

Eoin O'Connor is based in Walkers' Ireland office, where he is a partner in the Global Investment Funds Group and the Head of Regulatory for Ireland. His experience includes acting for a wide range of domestic and international financial institutions, including payment/e-money institutions, commercial banks, investment firms and asset managers, funds, fund promoters and services providers, and international law firms. Eoin provides advice on compliance with industry guidance, legislation and codes issued by the Central Bank of Ireland, prudential requirements, Irish authorisation and licensing issues, asset disposal projects by Irish and international clients, ongoing compliance with conduct of business, consumer protection and other requirements, anti-money laundering, data protection, financial institution M&A and the regulation of securitisation activities. He is the MiFiD II lecturer at the Law Society of Ireland's Finance Law Diploma programme.

1. FinTech Market

1.1 Evolution of the FinTech Market

Ireland is home to well-developed and globally recognised technology and financial services sectors. The Irish Industrial Development Agency ("IDA") has stated that Ireland is the world's second largest software exporter, and firms including Microsoft, Google, Apple and Facebook have strategic operations in Ireland. In addition, Ireland is the fourth largest provider of wholesale financial services in the European Union ("EU"), with more than 400 international financial institutions.

Ireland has a thriving tech sector and the FinTech sector is estimated to employ 7,000 people. The IDA has reported that more than 55 FinTech or financial services companies established a presence in Ireland during 2018.

While the past 12 months have seen further economic growth in Ireland, uncertainty over the UK's anticipated withdrawal from the EU ("Brexit") has been an ever-present factor. The uncertainty over the ability of UK-regulated firms to provide financial services into the EU post-Brexit has led to more than 100 applications to the Central Bank of Ireland ("Central Bank") for authorisation.

In late 2018 and early 2019, the first of the Brexit-related applicants were granted authorisation by the Central Bank. It is understood that remaining applicants include around 40 payment institutions and electronic money institutions. These firms would join Google and Facebook as recent additions to the Central Bank's register of regulated financial service-providers. Brexit will continue to be one of the key business and regulatory challenges over the next 12 months.

The Financial Stability Board published a report on 14 February 2019 highlighting that the competitive impact and scalability of large, established technology companies ("BigTech") may be greater than that of FinTech firms. The move into FinTech by BigTech firms is an interesting trend for Ireland.

The past 12-18 months have also witnessed the introduction of significant legislative changes affecting the FinTech industry. Across the EU, this includes the Second Payment Services Directive (Directive (EU) 2015/2366) ("PSD 2"), the revised Markets in Financial Instruments Directive (Directive (2014/65/EU) and Markets in Financial Instruments Regulation (Regulation (EU) 600/2014) (together with implementing regulations, "MiFID II"), the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") and the Insurance Distribution Directive (Directive (EU) 2016/97).

In November 2018, Ireland completed the delayed implementation of the Fourth Money Laundering Directive (Directive (EU) 2015/849) ("4MLD") into Irish law. The Fifth Money Laundering Directive (Directive (EU) 2018/843) ("5MLD") must be implemented into Irish law by January 2020, again with significant impacts for certain sectors of the FinTech industry (for example, bringing cryptocurrency exchange platforms and custodian wallet-providers into the scope of anti-money laundering "AML" regulation, as well as providing for electronic verification).

It is anticipated that proposals for the regulation of crowdfunding at a domestic level and an EU level (allowing for the provision of cross-border services) will be further developed in the next 12 months.

The Irish Department of Finance published a Discussion Paper on Virtual Currencies and Blockchain Technology in March 2018 ("DoF Paper"). In January 2019 the European Banking Authority ("EBA") published a report with advice for the European Commission on cryptoassets ("EBA Crypto Report"), and the European Securities and Markets Authority ("ESMA") published advice in relation to initial coin offerings and cryptoassets ("ESMA Crypto Report"). These publications reflect the increased activity in Ireland and the EU, as well as providing an insight into the Irish Government's and EU regulators' views on the regulatory framework applicable to blockchain assets.

In October 2018, Coinbase (a cryptocurrency exchange) announced that it would establish in Ireland. Consensys (a blockchain company) opened its Dublin hub in 2018. More recently, it was reported that an Irish issuer issued commercial paper using distributed ledger technology ("DLT") to reduce settlement times. It is expected that new developments will continue to gather pace in Ireland in relation to blockchain assets in the next 12 months.

The Central Bank established its Innovation Hub in May 2018 to provide a direct and dedicated point of contact for firms developing or implementing innovations in financial services based on new technologies, outside of the existing formal regulator/firm engagement processes. The Central Bank's 2018 update (published in February 2019) states that it has engaged with more than 78 firms and stakeholders, most frequently with payments and regulatory technology ("RegTech") businesses.

The European Commission published its FinTech Action Plan and the EBA published its Roadmap on FinTech in March 2018.

2. FinTech Verticals

2.1 Predominant Business Models

The Central Bank has commented that FinTech activity in Ireland is at its most intense in the payments sector. With

new authorisations under the European Union (Payment Services) Regulations 2018 ("Payment Services Regulations") (which transpose PSD 2 into Irish law) or the European Communities (Electronic Money) Regulations 2011 ("Electronic Money Regulations") (which transpose (Directive 2009/110/EC) ("Electronic Money Directive") into Irish law), and BigTech firms establishing in this space, it is likely that payment services will continue to be an area of focus in Ireland.

Firms may seek to avail of the opportunities under PSD 2 to become payment institutions authorised to provide payment initiation services and/or account information services ("PISPs/AISPs"), and thus to provide open banking services. PISPs are authorised to initiate payments from account servicing payments service-providers (such as credit institutions, including banks) ("ASPSPs") and AISPs to access customer data.

The provision of account aggregator services is already a well-developed model in some EU jurisdictions, but not yet in Ireland.

Currently there are two firms authorised in Ireland to provide account information services (Fire Financial Services Limited ("Fire") and Circit Limited). Fire also holds authorisation to provide payment initiation services. At present, Ireland does not have a separate open banking regime, unlike the UK, which encourages the development of open banking. However, as any PISPs/AISPs will most likely seek to export their services, initiatives in other EU jurisdictions to promote open banking are also relevant.

2.2 Regulatory Regime

Firms seeking to become PISPs/AISPs must seek authorisation from the Central Bank under the Payment Services Regulations or the Electronic Money Regulations (if they are also seeking to issue electronic money). As PSD 2 is within the competence of the EBA, EBA guidance, as well as regulatory and technical standards, will be applicable and relevant to the Central Bank and Irish payment service-providers. Smaller firms may seek to be appointed and registered as an agent of an authorised firm to provide services.

Commission Delegated Regulation (EU) 2018/389 ("Article 98 RTS") sets out how ASPSPs and PISPs/AISPs are to communicate, as well as requirements for payment service providers in respect of safely authenticating customers. Article 98 RTS applies from 14 September 2019 and, from that date, there may be more PISP/AISP activity, as ASPSPs will have been required to provide an interface to allow account access to PISPs/AISPs.

2.3 Variations Between the Regulation of FinTech and Legacy Players

Credit institutions providing payment services must also comply with the conduct of business rules contained in the Payment Services Regulations.

2.4 Regulatory Sandbox

There is currently no regulatory sandbox in Ireland. As referenced elsewhere, the Central Bank launched its Innovation Hub in May 2018 to provide a direct and dedicated point of contact for firms developing or implementing innovations in financial services based on new technologies, outside of existing formal regulator/firm engagement processes.

2.5 Jurisdiction of Regulators

The Central Bank authorises and supervises payment institutions in Ireland. The Data Protection Commission is the Irish supervisory authority for the GDPR.

2.6 Outsourcing of Regulated Functions

Under the Payment Services Regulations, the outsourcing of important operational functions, including information technology systems, must not be undertaken in a manner that materially impairs the quality of the payment institution's internal control and the ability of the Central Bank to monitor and review the payment institution's compliance with the Payment Services Regulations. The Central Bank must also be notified of proposals to outsource operational functions not less than 30 days prior to commencement of the outsourcing.

A payment institution may only outsource an important operational function where it meets certain requirements. The payment institution remains fully liable for any acts of any entity to which activities are outsourced.

Where a payment institution is only authorised as an AISP, the above requirements do not apply but the Central Bank's expectations are likely to be similar.

The obligations of the vendor (often referred to as a service-provider) will largely be dictated by the contractual relationship it has with the relevant PISP/AISP. In this context, it is expected that PISPs/AISPs would require their service-providers to provide the services in a manner that enables the PISPs/AISPs to comply with their legal and regulatory obligations. The Central Bank will have certain powers in relation to the outsourced activity, including the ability to carry out on-site inspections on the premises of a service-provider.

In November 2018 the Central Bank issued an Outsourcing Discussion Paper ("CBI Outsourcing Paper"), setting out certain regulatory expectations it has for outsourcing by entities that it regulates, including in relation to outsourcing contracts. More recently, in February 2019, the EBA issued

its Final Report on Guidelines on outsourcing arrangements ("EBA Outsourcing Guidelines"). The EBA Outsourcing Guidelines will be applicable, inter alia, to payment institutions (although the EBA Outsourcing Guidelines are not addressed to payment institutions that are only authorised as AISPs) from 30 September 2019, and set out a number of requirements for outsourcing contracts, as referenced elsewhere.

2.7 Significant Enforcement Actions

Western Union Payment Services Ireland Limited, an authorised payment institution, was fined EUR1,750,000 in 2015 for breaches of AML legislation.

2.8 Implications of Additional Regulation

Payment institutions are required to adhere to the data security requirements of the Payment Services Regulations (including applicable Regulatory Technical Standards), and to adhere to the GDPR. Payment institutions should also be aware of relevant guidelines.

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended ("CJA 2010") implements 4MLD into Irish law.

Entities such as credit institutions are also subject to conduct of business obligations under the Payment Services Regulations, and must comply with the GDPR and the CJA 2010.

2.9 Regulation of Social Media and Similar Tools

Conduct of business rules apply in relation to advertising by regulated firms. In addition, general consumer protection legislation prohibits certain activity, such as misleading advertising. There are also restrictions in Ireland on unsolicited direct marketing in certain circumstances.

2.10 Review of Industry Participants by Parties Other Than Regulators

Where companies are required to produce audited financial statements, their statutory auditors will review their financial accounts. There are certain exemptions to the audit requirement.

3. Robo-advisers

3.1 Requirement for Different Business Models

Per the EBA Glossary for Financial Innovation ("EBA Glossary"), Robo-advisers are defined as "Applications that combine digital interfaces and algorithms, and can also include machine learning, in order to provide services ranging from automated financial recommendations to contract brokering to portfolio management to their clients. Such advisors may be standalone firms and platforms, or can be in-house applications of incumbent financial institutions" ("Robo-adviser").

While the specific services and business models of differing Robo-advisers will vary, once the activities of the Robo-adviser constitute MiFID II 'investment services' in respect of 'financial instruments', they will require authorisation as an investment firm under the European Union (Markets in Financial Instruments) Regulations 2017 ("MiFID Regulations") (a "MiFID II Investment Firm"), unless an exemption applies. The MiFID Regulations implement MiFID II into Irish law.

The MiFID II investment services most likely to be triggered by Robo-adviser activity are portfolio management (defined as "managing portfolios in accordance with mandates given by clients on a discretionary client-by-client basis where such portfolios include one or more financial instruments") and/or the provision of investment advice (defined as "the provision of personal recommendations to a client, either upon its request or at the initiative of the investment firm, in respect of one or more transactions relating to financial instruments").

MiFID II financial instruments include, amongst other things, transferable securities, units in collective investment undertaking, certain options, futures swaps and other derivatives and emissions allowances (referred to in this guide as "MiFID II Financial Instruments").

MiFID II Investment Firms are subject to the extensive conduct of business rules when providing investment services. The authorisation requirements and process will largely shape and define a MiFID II Investment Firm's business model. MiFID II Investment Firms that provide 'independent' advice must implement additional organisational controls relating to inducements and conflicts of interests.

The MiFID Regulations requirements in relation to suitability assessments will also affect Robo-advisers, and certain of the ESMA Guidelines on MiFID Suitability – which define Robo-advice as "the provision of investment advice or portfolio management services (in whole or in part) through an automated or semi-automated system used as a client-facing tool" – are stated to be particularly applicable to Robo-advisers, given the limited amount or total absence of human involvement in the investment service performance process.

3.2 Legacy Players' Implementation of Solutions Introduced by Robo-advisers

As far as is known, there are no Irish domestic credit institutions or MiFID II Investment Firms offering Robo-advisory solutions on a widespread basis, nor is there a widespread use of Robo-advisers by Irish consumers at present. In the United States and the UK, however, international institutions such as RBS, UBS, Wells Fargo and Bank of America Merrill Lynch have taken steps in this area.

3.3 Issues Relating to Best Execution of Customer Trades

A Robo-adviser authorised under the MiFID Regulations that executes orders on behalf of clients is subject to the MiFID II rules and the obligation to execute orders on terms most favourable to its clients and the client order handling rules. These require, inter alia, the adoption of an order execution policy, the provision of information regarding its execution policy to clients, and the annual publication of its top five execution venues for each class of MiFID II Financial Instrument and details on the quality of execution achieved. MiFID II and the MiFID Regulations also set out related requirements for portfolio managers placing orders or where firms receive and transmit orders.

4. Online Lenders

4.1 Differences in the Business or Regulation of Loans Provided to Different Entities

There are significant differences between the regulation of lending to individuals and companies in Ireland.

Commercial lending (ie, lending to corporates) does not require a financial services licence in Ireland. By contrast, lending to individuals may breach the prohibition on acting as a retail credit firm, set out in the Central Bank Act 1997, as amended ("CBA 1997"). In summary, a retail credit firm is a person who holds itself out as carrying on a business of, and whose business consists wholly or partly of, providing credit (in the form of cash loans) directly to individuals in Ireland, or a firm that has been prescribed as a "credit institution" under the Consumer Credit Act, 1995, as amended ("CCA").

In addition, the CCA contains a further domestic-only regime whereby a person who meets the definition of a "moneylender" is required to obtain authorisation from the Central Bank in order to provide moneylending services, unless an exemption applies. Moneylending means credit supplied by a moneylender to a natural person acting outside the person's business, including their trade or profession (a "Consumer") on foot of a moneylending agreement.

Credit servicing (including loan ownership) in relation to loans to individuals and small and medium enterprises ("SMEs") requires authorisation in certain circumstances. Where a business provides payment services (eg, issuing a payment instrument) as part of its business model, it may be required to seek authorisation under the Payment Services Regulations or the Electronic Money Regulations. The domestic Irish regime governing money transmission businesses under the CBA 1997 may also be relevant.

The activity of operating a Peer-to-Peer crowdfunding lending platform is not currently regulated in Ireland as a distinct activity. However, crowdfunding may be within the scope of investment services legislation (such as MiFID II or prospectus requirements where MiFID II Financial Instruments are offered) and/or funds regulation where collective investment under takings are involved. In addition, crowdfunding lending platforms facilitating loans to Consumers may require authorisation as credit intermediaries under the CCA. The European Commission has published a proposal for the regulation of crowdfunding in the context of business lending to establish a European label for investment and lending-based crowdfunding platforms that enables cross-border activity. Similarly, a domestic Irish crowdfunding regime is proposed.

Credit institutions, such as licensed banks, are the traditional source of credit in Ireland. All companies that are not licensed banks (or EU passported banks) must avoid including "bank" in their name, as this is restricted under the Central Bank Act 1971.

Lending to Consumers is subject to the requirements of consumer protection legislation, which includes the CCA, the European Communities (Distance Marketing of Consumer Financial Services) Regulations 2004, the European Communities (Consumer Credit Agreements) Regulations 2010 ("Consumer Credit Regulations") and the European Communities (Unfair Terms in Consumer Contracts) Regulations 1995.

Regulated financial service-providers (including EU lenders operating in Ireland on a cross-border basis) may also be subject to certain conduct of business rules when lending to individuals, certain small companies or SMEs. These rules include the Central Bank's Consumer Protection Code 2012 ("CPC 2012") and the Central Bank (Supervision and Enforcement) Act 2013 (Section 48) (Lending to Small and Medium-Sized Enterprises) Regulations 2015 ("SME Regulations").

4.2 Underwriting Processes

Irish conduct of business rules and legislation requires creditworthiness or suitability assessments in certain circumstances. For example, the Consumer Credit Regulations, the CPC 2012 and the SME Regulations are relevant in this regard.

Ireland has established a Central Credit Register ("CCR") under the Credit Reporting Act 2013 ("CRA"). The CRA requires lenders to check the CCR prior to advancing any credit for an amount of EUR2,000 or greater, and also imposes a requirement on lenders to report information relating to certain loans and borrowers.

4.3 Sources of Funds for Loans

Credit institutions such as banks raise funds for their lending activities from a wide range of sources, including deposits, inter-bank lending and securitisations. Deposit-taking in

Ireland triggers a requirement for a banking licence, and securitisations are subject to a number of Irish and EU rules.

Dedicated lending entities – for example, a retail credit firm – may raise funds for their lending activities from securitisations or lending from other investors or institutions.

Where a lender is providing finance through a crowdfunding platform, financing may be provided by individuals using their own personal funds.

4.4 Syndication of Loans

It is not typical for consumer loans or loans to small businesses to be syndicated.

5. Fund Administrators

5.1 Regulation of Fund Administrators

Fund administrators are generally authorised pursuant to the Investment Intermediaries Act 1995 ("IIA") but may also be authorised pursuant to the MiFID Regulations. In addition, fund administrators are subject to the Central Bank (Supervision and Enforcement) Act 2013 (Section 48(1)) (Investment Firms) Regulations 2017 and the Investor Compensation Act, 1998.

5.2 Contractual Terms

The increasing reliance by firms operating within the global financial sector on information technology has led to a focus by regulators and firms alike on improving cybersecurity and data protection within the financial industry. As fund administrators maintain trading data, account details and extremely sensitive investor information, they are at particular risk from the evolving sophistication of cyber-attacks and the heightened frequency of data breaches. Accordingly, fund advisers are increasingly seeking to impose contractual terms that ensure fund administrators have appropriate IT and cybersecurity risk management procedures and frameworks in place to protect against cybercrime and data breaches, as well as IT disaster recovery and business continuity planning arrangements encompassing the recovery and resumption of daily operations should a disruptive event occur. These provisions stem from the sharpened focus of regulators on data protection as well as the management of cybersecurity across the financial sector, but also from an increasing awareness by industry of the devastating financial and reputational implications that a successful cyber-attack could yield.

Regulators are also becoming increasingly focused on the oversight exercised by funds and their advisers on fund administrators and, accordingly, contractual terms requiring ongoing reporting from the fund administrator to the fund are becoming increasingly important.

5.3 Fund Administrators as 'Gatekeepers'

Generally, fund administrators do not act as 'gatekeepers'; however, they are likely to be under a contractual obligation to report any data breaches and cybersecurity issues that may impact their client. They may also be subject to industry guidance and best practice in this regard.

In addition, where a fund administrator provides transfer agency activities that typically include performing due diligence on investors in line with applicable AML and counter-terrorist financing legislation, the fund administrator would have an obligation to identify and escalate transactions it determines to be suspicious or unlawful. In this situation, fund administrators would also have an affirmative duty to conduct regular testing to ensure that there are no unexplained gaps in the required due diligence documentation and records of the underlying investor, and to ensure that the documentation is updated at the appropriate frequency.

In addition, the Criminal Justice Act 2011 ("CJA 2011") imposes a reporting obligation on a person that has information that said person "knows or believes might be of material assistance" in preventing or prosecuting a "relevant offence" to disclose this information to the Garda Síochána (the Irish police force).

6. Exchanges and Trading Platforms

6.1 Permissible Trading Platforms

Cryptocurrency platforms are permissible in Ireland, as cryptocurrency as an asset class is not currently regulated in Ireland (this point is considered in further detail elsewhere). However, 5MLD will bring custodian wallet-providers and cryptocurrency exchange platforms within the scope of EU/Irish AML requirements. Ireland has until 10 January 2020 to implement this directive. Further detail is set out elsewhere, in relation to blockchain.

As referenced elsewhere, commercial lending (ie, lending to corporates) is not a regulated financial services activity in Ireland, and consequently Peer-to-Peer crowdfunding lending platforms for commercial lending can currently operate on an unregulated basis. However, platforms that facilitate lending to Consumers, or that involve equity or investment-based finance, may trigger authorisation and conduct of business requirements.

Payment services involving fiat currencies will typically have to be carried out by a regulated payment service provider, in accordance with the conduct of business rules contained in the Payment Services Regulations. The Irish regime of governing money transmission businesses under the CBA 1997 may also be relevant.

The provision of exchanges and trading platforms in respect of MiFID II Financial Instruments is primarily regulated by the Central Bank under the MiFID Regulations, which provide for the regulation of various types of securities exchanges, including market operators, regulated markets, multilateral trading facilities ("MTFs") and organised trading facilities ("OTFs").

6.2 Listing Standards

No formal listing standards exist for unregulated platforms. General contractual principles should apply, and certain general consumer protection rules may also apply. Exchanges for MiFID II Financial Instruments established under the MiFID Regulations will usually have detailed listing/admission to trading rules to ensure transparency and compliance with applicable laws and regulation (eg, the Euronext Dublin Listing Rules), while rules in relation to the requirement to publish prospectus may also be relevant.

6.3 Order-handling Rules

No formal order handling rules apply for unregulated platforms; general contractual principles should apply. Detailed order handling rules apply to MiFID II Investment Firms when executing orders in MiFID II Financial Instruments.

6.4 Rise of Peer-to-Peer Trading Platforms

There are a small number of crowdfunding platforms active in Ireland. Peer-to-Peer trading platforms for commercial loans, crypto-currencies or crowdfunding are currently unregulated in Ireland. Further detail in relation to Peer-to-Peer crowdfunding lending platforms is referenced elsewhere.

6.5 Issues Relating to Best Execution of Customer Trades

No formal best execution standards apply to an unregulated platform in Ireland; general contractual principles should apply.

Detailed best execution standards apply for MiFID II Investment Firms dealing in MiFID II Financial Instruments. In summary, this includes a requirement for MiFID II Investment Firms to take steps and adopt policies and procedures to ensure they achieve the best results for customers when executing orders in financial instruments.

6.6 Rules of Payment for Order Flow

The MiFID II inducements regime will apply to all MiFID II Investment Firms.

7. High-frequency and Algorithmic Trading

7.1 Creation and Usage Regulations

The primary method of regulation of these technologies is under the MiFID Regulations. The definition of algorithmic trading contained in the MiFID Regulations is limited to trading in MiFID II Financial Instruments, so asset classes outside the scope of regulation under the MiFID Regulations will not be regulated.

7.2 Exchange-like Platform Participants

All MiFID II Investment Firms and exchange like-platforms that allow for the trading of MiFID II Financial Instruments will be in scope.

7.3 Requirement to Register as Market Makers When Functioning in a Principal Capacity

Specific, detailed rules apply where a MiFID II Investment Firm engages in algorithmic trading to pursue a market making strategy. These include carrying out the market-making continuously during a specified proportion of the trading venue's trading hours, and entering into a binding written agreement with the trading venue.

7.4 Issues Relating to the Best Execution of Trades

The MiFID II and MiFID Regulations rules governing algorithmic trading impose specific systems and risk controls on in-scope MiFID II Investment Firms, including ensuring their trading systems are resilient, with sufficient capacity, subject to trading thresholds and limits, and prevent the sending of erroneous orders.

7.5 Regulatory Distinction Between Funds and Dealers

The "dealing on own account" exemption for proprietary trading has been narrowed in MiFID II to specify that any firm that is dealing on own account but operates "a high-frequency algorithmic trading technique" will be subject to the MiFID II regime, including those rules around algorithmic trading.

7.6 Rules of Payment for Order Flow

The MiFID II inducements regime will apply to all MiFID II Investment Firms engaged in algorithmic trading.

8. Financial Research Platforms

8.1 Registration

Platforms providing financial research are not specifically regulated by the Central Bank. However, participants and platforms should consider whether a regulated investment service is being provided.

The provision of investment research and financial analysis or other forms of general recommendation relating to transactions in financial instruments is an ancillary service under Part 2 of Schedule 1 of the MiFID Regulations. The provision of this service without any other MiFID II investment services would not trigger a requirement for authorisation as a MiFID II Investment Firm.

In contrast, the provision of investment advice (as defined in MiFID II) in relation to MiFID II Financial Instruments is an activity requiring authorisation under the MiFID Regulations, unless an exemption applies.

The MiFID Regulations and Commission Delegated Regulation (EU) 2017/565 provide requirements in relation to conflicts of interest and inducements that apply to regulated MiFID II Investment Firms in relation to research.

The IIA regulates the provision of investment advice in relation to investment instruments, subject to certain exemptions. The IIA definition of investment instruments captures certain instruments that are not MiFID II Financial Instruments and certain activities or firms that might fall outside the MiFID Regulations.

8.2 Regulation of Unverified Information

The Market Abuse Regulation (Regulation (EU) 596/2014) ("MAR") establishes a common EU regulatory framework on insider dealing, the unlawful disclosure of inside information and market manipulation ("Market Abuse") as well as measures to prevent Market Abuse.

MAR prohibits insider dealing, the unlawful disclosure of inside information, market manipulation and attempted market manipulation. Market manipulation is broadly defined under MAR, and amongst other things includes disseminating information through the media, including the internet, or by any other means, which gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of a financial instrument, a related spot commodity contract or an auctioned product based on emission allowances or secures, or is likely to secure, the price of one or several MiFID II Financial Instruments, a related spot commodity contract or an auctioned product based on emission allowances at an abnormal or artificial level, including the dissemination of rumours, where the person who made the dissemination knew, or ought to have known, that the information was false or misleading.

Recital 48 to MAR confirms that, given the rise in the use of websites, blogs and social media, disseminating false or misleading information via the internet (including through social media sites or unattributable blogs) should be considered to be equivalent to doing so via more traditional communication channels for the purposes of MAR.

MAR applies to MiFID II Financial Instruments admitted to trading on an EU-regulated market or for which a request for admission to trading has been made, as well as any MiFID II Financial Instruments traded on an MTF, admitted to trading on an MTF or for which a request for admission to trading on an MTF has been made or traded on an OTF and certain over-the-counter instruments, including derivatives. MAR can apply to other instruments and is not limited to transactions, orders or behaviour on a trading venue. The terms "regulated market", "MTF", "OTF" and "trading venue" are defined in MiFID II.

Market manipulation, as defined under the European Union (Market Abuse) Regulations 2016 ("MAR Regulations"), is an offence in Ireland. The MAR Regulations also provide for certain civil sanctions for breaches of MAR, such as a breach of the prohibition on market manipulation.

8.3 Conversation Curation

The MAR prohibition on market manipulation (including attempted market manipulation) includes a prohibition on "taking advantage of occasional or regular access to the traditional or electronic media" to voice opinions about in-scope instruments with a view to profiting from the impact of those opinions, without having simultaneously publicly disclosed that conflict of interest.

MAR is also intended to ensure that the prohibitions against market abuse should also cover those persons who act in collaboration to commit market abuse, so the platform should ensure it takes steps to avoid being seen to collaborate with such activity.

8.4 Platform Providers as 'Gatekeepers'

Liability under the MAR Regulations can also attach to an entity that collaborates or facilitates market abuse/manipulation. MAR also requires member states (including Ireland) to put mechanisms in place to allow for the reporting of infringements of MAR (ie, whistleblowing mechanisms).

As noted elsewhere, it is an offence under the CJA 2011 to fail to disclose information to the authorities of a 'relevant offence' as defined under that act.

Where a financial research platform has been used in furtherance of illegal activity such as a breach of MAR or the MAR Regulations, the operators of that platform may potentially face legal exposure.

9. InsurTech

9.1 Underwriting Processes

The EU's Solvency II regime (as implemented in Ireland) applies to the majority of Irish (re)insurance undertakings, including the underwriting process of these undertakings.

The Solvency II framework sets out detailed requirements around capital, governance and risk management in all Irish and EU authorised (re)insurance undertakings.

9.2 Treatment of Different Types of Insurance

In broad summary, Solvency II Undertakings must obtain an authorisation under the European Union (Insurance and Reinsurance) Regulations 2015, to carry on either Life Insurance business, Non-Life Insurance business, or both.

10. RegTech

10.1 Regulation of RegTech Providers

Ireland is a hub for RegTech – defined per the EBA Glossary as "a commonly recognised term for technologies that can be used by market participants to follow regulatory and compliance requirements more effectively and efficiently."

Generally speaking, the provision of RegTech services is not a regulated activity in Ireland as these will typically be considered a provision of supporting technical services rather than regulated financial services. However, certain exceptions to this position could apply, depending on the nature of the RegTech service performed and the nature of the entity to which such services are provided.

In January 2018 the European Supervisory Authorities (comprising the EBA, ESMA and the European Insurance and Occupational Pensions Authority) issued a joint opinion to European regulators considering the potential benefits and risks of the use of innovative solutions in the customer due diligence process, which forms part of AML obligations.

10.2 Contractual Terms to Assure Performance and Accuracy

Depending on the particular service provided and the particular entity receiving those services, the provision of the services may fall within the legal and regulatory requirements governing outsourcing.

For example, where a MiFID II Investment Firm outsources "a critical or important function", outsourcing rules apply under the MiFID II framework. Similar issues would arise where regulated payment institutions, electronic money institutions, credit institutions and other regulated entities engage in outsourcing. In these circumstances regulated firms should require RegTech outsourcing agreements to reflect the applicable rules.

The Central Bank has issued the CBI Outsourcing Paper, wherein it sets out its minimum supervisory expectations for the outsourcing agreements of Irish regulated financial service-providers. The EBA Outsourcing Guidelines apply to EEA authorised credit institutions, investment firms, payment institutions and electronic money institutions, and require, inter alia, that outsourcing agreements specify service levels and precise quantitative and qualitative performance targets to allow for the timely monitoring of the performance of the outsourced function. In addition, specific termination rights, provisions around business continuity, data and regulator access are also required. The EBA has commented that it is imperative that business continuity and data protection are appropriately considered when outsourcing IT or data services.

As RegTech providers are likely to be providing compliance or other functionality, the outsourcing of services to them by regulated firms may fall within the remit of these requirements and, even if they do not, it is likely that such financial services firms would require similar contractual protections.

Outsourcing is a particularly topical issue for the Central Bank at the moment, evidenced by the publication of the CBI Outsourcing Paper and its focus on outsourcing when considering applications for new Brexit-related authorisations. As such, it is expected that firms in Ireland will be diligent in ensuring that new contractual frameworks meet the requirements of the EBA Outsourcing Guidelines from 30 September 2019 or earlier (there are transitional measures for existing arrangements).

10.3 RegTech Providers as 'Gatekeepers'

As noted elsewhere, it is an offence under the CJA 2011 to fail to disclose information to the authorities of a 'relevant offence' as defined under that Act. RegTech providers may have regulatory or contractual obligations to notify certain behaviour, depending on their regulatory status and contractual arrangements.

11. Blockchain

11.1 Use of Blockchain in the Financial Services Industry

Domestic institutions are investigating the use of blockchain, and certain institutions have conducted trials in this area, including in the area of payments. Other international institutions that have a presence in Ireland are further developed. A recent example is JP Morgan, which has created its own cryptocurrency and has tested issuances on blockchain. In addition, as described elsewhere, an Irish issuer recently issued commercial paper using DLT to reduce settlement times.

11.2 Local Regulators' Approach to Blockchain

Neither the Irish legislature nor the Central Bank has implemented specific legislative or regulatory updates, or updated guidance to address blockchain technology. The Central Bank has issued consumer warnings regarding the risks of both crypto-currencies and initial coin offerings ("ICOs").

The March 2018 DoF Paper considered the extent of blockchain and cryptocurrency activity in the Irish market and proposed the next steps for the Irish government.

In January 2019 the EBA Crypto Report and the ESMA Crypto Report were published. The reports provide useful information in relation to the interpretation of blockchain assets within existing rules and highlighting gaps, as well as suggesting that further consideration be given at an EU level to legislating in the area.

The Basel Committee on Banking Supervision made a statement on cryptoassets on 13 March 2019, noting potential financial stability concerns and increased risks faced by banks as a result of the continued growth of cryptoasset trading platforms and new financial products linked to cryptoassets. The statement sets out prudential expectations related to banks' exposures to cryptoassets and related services.

11.3 Classification of Blockchain Assets

There is currently no Irish or EU law or regulation that expressly classifies blockchain assets or crypto-currencies. However, blockchain assets and/or services in relation to those assets may fall within existing regulatory regimes and, depending on the features of a particular blockchain asset, its legal classification may vary.

The Central Bank has confirmed in a consumer warning that virtual currencies are not legal tender, and has also issued a consumer warning regarding the risks of ICOs.

One area of focus has been whether a particular blockchain asset qualifies to be considered as a MiFID II Financial Instrument. Given the variance in structure among blockchain assets, it is necessary to analyse individual blockchain assets against the criteria for the MiFID II Financial Instrument of "transferable securities", defined under Article 4 (1) (44) of MiFID II as those "classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as:

- shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;
- bonds or other forms of securitised debt, including depositary receipts in respect of such securities;
- any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures".

If a blockchain asset is determined to be a transferable security, then it falls within the regulatory scope of, inter alia, MiFID II, the Prospectus Directive (Directive 2003/71/EC as amended) ("Prospectus Directive"), and MAR. The ESMA Crypto Report also states that several European regulators considered that certain types of cryptoassets could qualify as units in collective investment undertakings, most likely alternative investment funds, and thus the Alternative Investment Fund Managers Directive (Directive 2011/61/EU) ("AIFMD") could be relevant. The ESMA Crypto Report notes that existing rules that may be applicable do not fit perfectly with the characteristics of blockchain.

In very broad terms, a blockchain asset with characteristics that are similar to shares, bonds or other securities, or related derivatives including being transferable, will be more likely to fall within the definition of a "transferable security". An investment-type blockchain asset may be more likely to have these characteristics, while the ESMA Crypto Report specifically notes that a pure payment-type cryptocurrency (such as Bitcoin) is less likely to be considered a "transferable security". The ESMA Crypto Report cautions against extrapolating its analysis against the entire cryptoasset universe.

Annex 1 to the ESMA Crypto Report sets out the results of a consultation with National Competent Authorities across EU member states regarding the classification of differing forms of cryptoassets as "transferrable securities".

In the EBA Crypto Report, the EBA notes that a cryptoasset can qualify as electronic money under the Electronic Money Directive, and thus fall to be regulated under that directive, provided the following circumstances are met:

- it is electronically stored;
- it has monetary value;
- it represents a claim on the issuer;
- it is issued on receipt of funds;
- it is issued for the purpose of making payment transactions; and
- it is accepted by persons other than the issuer.

Additionally, if a person performs a 'payment service' as listed in PSD 2 (such as the execution of payment transactions, including issuing 'payment instruments' and/or acquiring payment transactions and money remittance) with a blockchain asset that qualifies as 'electronic money' under the Electronic Money Directive, such activity would fall within the scope of PSD 2 by virtue of constituting 'funds'. More generally, PSD 2 and the domestic Irish regime of money transmission should also be considered in the context of fiat transfers or services related to blockchain activities.

11.4 Regulation of 'Issuers' of Blockchain Assets

There is currently no specific regulatory regime for or prohibition on the issuance of blockchain assets or ICOs in Ireland or at EU level.

However, as with the applicability of the existing legal or regulatory requirements to a blockchain asset depending on

its particular structure, an issuance may come within the scope of existing Irish legal regimes, depending on its specific characteristics. Thus, it is prudent to review the structure and terms of each issuance to determine whether it may be in scope of any existing legal or regulatory requirements. Given the broad divergence of blockchain asset issuances, it is likely that classifications of issuances will vary accordingly.

In two statements from November 2017, ESMA alerted participants in ICOs of the potential applicability of MiFID II, AIFMD, the Prospectus Directive and the applicable AML rules, depending on the structure of the issuance, and alerting investors of the risks of ICOs.

11.5 Regulation of Blockchain Asset-trading Platforms

Generally speaking, there is minimal regulation of blockchain asset trading platforms in Ireland (where the blockchain assets do not constitute MiFID II Financial Instruments – such as transferable securities – and are not otherwise in the scope of existing regulatory regimes). The EBA Crypto Report highlights the lack of regulatory consumer protection provided by blockchain asset-trading platforms and custodian wallet-providers.

The AML and counter-terrorist financing rules of the CJA 2010 may apply, depending on the nature of the blockchain asset/issuance (eg, whether it constitutes a MiFID II Financial Instrument, electronic money, etc), the nature of activities undertaken (eg, payment services, etc), the identity and regulated status of the actors and the method of payment. Once implemented, 5MLD will capture providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers. 5MLD is due to be transposed into Irish law by 20 January 2020.

11.6 Regulation of Invested Funds

Generally speaking, a UCITS fund (authorised pursuant to Directive 2009/65/EU) – which is a European regulated retail investment fund product for which Ireland is a popular jurisdiction of establishment – cannot directly hold blockchain assets such as crypto-currencies, as such assets would not appear to qualify as permitted investments under the applicable regulations in the absence of further clarification on this point from the relevant regulatory authorities. For alternative investment funds, the requirements are less restrictive; however, practical obstacles still exist in the market to the extent that currently many depositories are not comfortable that they can capably hold blockchain assets directly such as crypto-currencies while also meeting their safekeeping obligations.

11.7 Virtual Currencies

The legal treatment of any cryptocurrency or other blockchain asset will be determined by whether that particular asset's features come within the scope of existing legislative and regulatory regimes.

11.8 Impact of Privacy Regulation on Blockchain

There are inherent tensions between the GDPR and DLT. For example, where personal data is recorded on a public blockchain, by virtue of DLT, this will be publicly accessible. While personal data can be recorded in an encrypted (hashed) form, if it is technically possible for the encryption of such personal data to be reverse engineered – including with the use of other information (eg, details of a user's key) – then this should be considered as pseudonymous rather than anonymised data, and thus subject to the GDPR. Additional considerations arise, such as the implications of the permanent nature of blockchain-recorded personal data for the right to be forgotten provided for by Article 17 of the GDPR. The EU Blockchain Observatory and Forum published a report on blockchain technology and the GDPR in October 2018. Although this report does not seek to reconcile all of the inconsistencies between the GDPR and DLT, it sets out guidance for GDPR best practice when designing and using blockchains and DLT.

12. Open Banking

12.1 Regulation of Open Banking

PSD 2 introduced two new regulated payment services: payment initiation service and account information service. A disruptive aspect of PSD 2 is the ability for PISPs to initiate payments from ASPSPs, and for AISPs to access customer data.

A recent example of an Irish firm being authorised for both of these activities is Fire. Meanwhile, established credit institutions are taking steps to launch open application programming interfaces, including Allied Irish Banks and Ulster Bank Ireland, a member of the RBS Group, ahead of Article 98 RTS becoming applicable on 14 September 2019.

12.2 Concerns Raised by Open Banking

PSD 2 imposes certain conditions on the access to and use of data by firms providing a payment initiation service or account information service. This includes a requirement

Walkers

The Exchange,
George's Dock,
IFSC,
Dublin 1,
Ireland

WALKERS

Tel: +353 1 470 6600
Fax: +353 1 470 6601
Email: info@walkersglobal.com
Web: www.walkersglobal.com

for customer consent and other requirements in relation to security and the use of data. In addition, the GDPR requires customers to be made fully aware, in a clear, concise and transparent fashion, of how their personal data will be used and by whom. It also provides for the right to withdraw consent, access to data and a right for information to be erased. In sharing data with third parties such as AISPs, banks will need to be aware of the potential for fraud or other risks.