IRELAND

Law and Practice

Contributed by:
Niall Esler, Shane Martin, James O'Doherty and Laura Whitson
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 include Fortune 100 and FTSE 100 companies, and some of 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 regularly advises innovative fintech firms on legal and regulatory considerations arising from offering their products to the Irish and European market, often for the first time and in novel areas. It leverages its expertise in multiple areas of regulated financial services when assessing fintech proposals to provide clear mapping of product features that could trigger regulatory issues. It has also assisted start-up clients in engaging with the Central Bank of Ireland's Innovation Hub, which is only open to innovative services.

Authors

Niall Esler is a partner and head of 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, crypto-asset service providers and issuers, credit institutions, investment firms, asset managers, funds and other institutions. Niall's areas of focus include advising on payment services, e-money, AML, banking, consumer lending, crypto-asset services and investment services, from both a prudential and conduct of business perspective. He is a member of the Incorporated Law Society of Ireland, the Compliance Institute in Ireland and the Blockchain Ireland Legal Working Group on Digital Assets.

Shane Martin is a partner in the regulatory group in Walkers' Ireland office. He has significant experience in regulatory risk and compliance in domestic and international financial services across the banking, funds, asset management, payment services and credit union sectors. Prior to joining Walkers, Shane worked for a number of years for the Central Bank of Ireland, where he managed a specialist AML supervision team. He is a member of the Incorporated Law Society of Ireland, the Compliance Institute in Ireland and the FATF Private Sector Consultative Forum.

James O'Doherty is based in Walkers' Ireland office, where he is an of counsel in the regulatory group. He advises on all areas of Irish and EU financial regulation and compliance, acting for credit institutions, insurers and reinsurers, investment firms, asset managers and payment service providers on Irish and EU financial regulation. He is a member of the Incorporated Law Society of Ireland.

Laura Whitson is based in Walkers' Ireland office, where she is an associate in the regulatory group. She advises on Irish and EU financial regulation and compliance, acting for domestic and international credit institutions, investment firms, international payment/e-money institutions, crypto-asset service providers and issuers, asset managers and other institutions.

Walkers (Ireland) LLP

The Exchange
George's Dock
IFSC
Dublin 1
Ireland

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

1. Fintech Market

1.1 Evolution of the Fintech Market

Ireland is home to well-developed and globally recognised technology and financial services sectors, and is one of the leading European jurisdictions for fintech activity. The Central Bank of Ireland (Central Bank) has recognised that the fintech sector is of increasing importance to both the Irish and EU financial services landscape, and that the industry has seen significant growth in recent years.

Key Trends Over the Past 12 Months

Fintech activity continues to be particularly prevalent in the payments sector, although it is not limited to this area. The 2023 update published by the Central Bank's Innovation Hub notes that, by the end of 2023, it had held 389 engagements across a number of sectors, including payments, regtech, blockchain, crypto and insurtech.

Four new e-money or payment institutions were authorised by the Central Bank in 2024. Significant growth has appeared in the virtual asset service provider (VASP) sector, with 22 VASPs registered with the Central Bank since the regime came into effect in April 2021.

Regulatory Developments

Fintech developments in Ireland are expected to continue to focus on the payments sector, regtech, AI and blockchain over the next 12 months, among other areas. The Markets in Crypto-Assets Regulation (MiCAR) came into application at the end of 2024 and is expected to generate market activity with existing Irish-registered VASPs and new entrants alike choosing Ireland as their EU base and seeking authorisation as a crypto-asset service provider (CASP) under MiCAR in Ireland.

Crypto-assets

On 30 December 2024, MiCAR became applicable to CASPs as well as offerors and persons seeking admission to trading of crypto-assets in the EU. Stablecoin issuers have been subject to MiCAR since 30 June 2024.

Entities providing certain crypto-asset services within the EU are required to be authorised as CASPs. CASPs authorised under MiCAR will be subject to a range of obligations, including the prudential and conduct of business requirements under MiCAR as well as other requirements, such as in relation to anti-money laundering.

VASPs that were registered with the Central Bank and operating in Ireland as a VASP by 30 December 2024 may avail of a transitional period of 12 months or until they are granted a CASP authorisation, whichever is sooner. These entities can continue to provide services in Ireland during the transitional period.

Offerors and persons seeking admission to trading of a crypto-asset in the EU are now subject to obligations under MiCAR.

A person cannot make an offer to the public or seek admission to trading of an asset-referenced token (ART) or an electronic money token (EMT) unless that person is the issuer and:

- in the case of an ART, that issuer is established in the EU and authorised under MiCAR, or alternatively is authorised as a credit institution; or
- in the case of an EMT, the issuer is authorised as a credit institution or an e-money institution, unless an exemption applies.

Digital Operational Resilience Act

Of broader application is the EU Digital Operational Resilience Act (DORA), which entered into force in January 2023 and became applicable from 17 January 2025. DORA applies to certain financial services firms with the objective of ensuring that entities operating in the EU financial services industry can withstand, respond to and recover from all types of disruptions and threats relating to information and communication technology (ICT). DORA also applies to critical ICT third-party service providers to the financial services industry, and provides a framework for the oversight of such entities by the European Supervisory Authorities (ESAs) – ie, the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

Payments

In response to the advancements in payments and financial services technologies and the increasing challenges faced by the industry with instances of fraud and financial crime, the European Commission evaluated the Payment Services Directive (PSD2) and found a number of positives and some shortcomings. The review culminated in the publication of proposals for an updated Payment Services Directive (PSD3) and Payment Services Regulation (EU PSR). The proposed amendments include:

- the strengthening of measures to combat payment fraud;
- improving the functioning of open banking;
- reinforcing the enforcement powers;
- further improving consumer information and rights; and
- merging the legal frameworks applicable to electronic money and payment services.

The PSD3 and EU PSR are expected to take effect by the end of 2026, although the timeline is not yet clear.

The Instant Payments Regulation entered into force on 8 April 2024, with a phased implementation schedule extending from January 2025 to July 2027. It aims to ensure that instant euro payments are accessible to both consumers and businesses throughout the EU by amending existing EU payments regulations.

Artificial intelligence

On 9 December 2023, the European Parliament and the Council of the EU reached a provisional agreement on the AI Act, which was subsequently approved in its final form on 21 May 2024. The AI Act entered into force on 1 August 2024, with most of its provisions set to apply two years after this date, although certain exceptions apply. The ban on prohibited AI systems applies from 2 February 2025. The AI Act establishes a regulatory framework aimed at harmonising rules for AI across the EU. It seeks to regulate providers who market or deploy AI systems within the EU, as well as users of these systems.

2. Fintech Business Models and Regulation in General

2.1 Predominant Business Models

The Central Bank has commented that there was a greater than four-fold growth in the number of payment firms authorised in Ireland between 2018 and 2022.

Outside of payments business, which has driven the majority of fintech activity, it is notable that the number of registered VASPs and authorised crowdfunding service providers has increased. Existing VASPs and new entrants are expected

to be interested in seeking authorisation in Ireland as a CASP under MiCAR.

Other areas for innovation include regtech, insurance, digital identity and asset management. Firms are also looking to incorporate new technology such as blockchain and AI into their operations.

2.2 Regulatory Regime

Fintech firms must look to the existing regulatory regimes that may be applicable to their business model on a case-by-case basis.

Payments

In relation to the provision of payment services or the issuance of electronic money, the primary rules to be considered are:

- the European Union (Payment Services) Regulations 2018 (PSR), which transpose PSD2 into Irish law; and
- the European Communities (Electronic Money) Regulations 2011 (EMR), which transpose Directive 2009/110/EC (the *"Electronic Money Directive"*) into Irish law.

The domestic Irish regime governing money transmission businesses under the Central Bank Act, 1997 (CBA 1997) may be relevant to a money transmission service falling outside the PSR.

Banking

Challenger banks seeking to undertake *"banking business"* or accept deposits from the public require a bank licence under the Central Bank Act, 1971 (CBA 1971) and will be subject to the Irish implementation of the EU Capital Requirements Directive (Directive 2013/36/EU) (as amended) and the directly applicable EU Capital Requirements Regulation (Regulation 575/2013/EU).

Credit institutions authorised in other European Economic Area (EEA) jurisdictions may passport their authorisation into Ireland, which requires notification to their regulator in the first instance. All companies that are not licensed banks (or passported credit institutions) must avoid including *"bank"* or similar in their name or advertising and certain other materials.

Investment Services/Asset Management

Depending on the services provided, a fintech firm providing investment services or asset management solutions may be subject to regulation. For example, if the activities constitute *"investment services"* in respect of *"financial instruments"* for the purposes of the European Union (Markets in Financial Instruments) Regulations 2017 (the *"MiFID Regulations"*), an investment firm authorisation will be required, unless an exemption applies. The MiFID Regulations implement Directive 2014/65/EU (MiFID II) into Irish law. Investment services include:

- the provision of investment advice;
- the receipt and transmission of orders;
- the execution of orders on behalf of clients; and
- the provision of portfolio management services.

Firms appointed to manage a collective investment undertaking (such as a UCITS fund or an alternative investment fund) will require authorisation under the European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations 2011 or the European Union (Alternative Investment Fund Managers) Regulations 2013, as appropriate, unless an exemption applies.

Crowdfunding
The operation of a loan or investment-based crowdfunding platform is a regulated activity under Regulation (EU) 2020/1503 (the *"Crowdfunding Regulation"*).

Blockchain and Crypto-Assets
In relation to the application of MiCAR to CASPs, stablecoin issuers and offerors/person seeking admission to trading of crypto-assets, please see **1.1 Evolution of the Fintech Market**.

Anti-Money Laundering (AML)
The applicability of AML rules, including customer due diligence and ongoing monitoring requirements, will depend primarily on whether a fintech company falls within the categories of *"designated persons"* under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended (CJA 2010). Designated persons include a wide range of financial services companies as well as certain other entities – eg, casinos, or persons trading or acting as an intermediary in the trade of works of art.

The Transfer of Funds Regulation (Regulation (EU) 2023/1113) (TFR) became applicable on 30 December 2024 and extends the obligation to include information about the originator and beneficiary (the so-called *"travel rule"*) to CASPs. The TFR also subjects CASPs to the same AML/CFT requirements and AML/CFT supervision as credit and financial institutions.

Security Requirements
Fintech firms will also need to be aware of and comply with specific security requirements introduced under PSD2 (eg, strong customer authentication) if they provide payment services, and, more broadly, cross-industry and industry-specific guidance from the Central Bank and EU regulators in relation to ICT and cyber-risks.

DORA and the Central Bank's Guidance on Outsourcing and on Operational Resilience also set out specific requirements for certain financial institutions in the context of the security of network and information systems. Other cybersecurity and criminal legislation or guidance may also be relevant.

Furthermore, the technical, operational and organisational cybersecurity measures contained in Directive (EU) 2022/255 (NIS2), once transposed, will be applicable to in-scope essential and important entities, which include cloud computing service providers.

Data Privacy
Fintech firms will need to comply with data privacy laws, including the European Union General Data Protection Regulation (Regulation (EU) 2016/679 – GDPR), in respect of any processing of personal data. The GDPR is broad in application, such that the vast majority of companies are impacted regardless of their regulatory status or the services being provided.

Fitness and Probity (F&P) Regime
The Central Bank's F&P Regime was established under the Central Bank Reform Act 2010 and applies to persons performing certain roles in regulated financial service providers (RFSPs). It applies to persons performing certain prescribed *"controlled functions"* (CFs) and *"pre-approval controlled functions"* (PCFs). PCFs include directors, chairs of the board and committees, the chief executive and heads of certain internal control functions, amongst other functions. A regulated firm must not permit a person to perform a CF or PCF unless it is satisfied on reasonable grounds that the person complies with the Central Bank's Standards of Fitness and Probity.

Individual Accountability Framework and the Senior Executive Accountability Regime (SEAR)

The Central Bank (Individual Accountability Framework) Act 2023 (the *"IAF Act"*) introduced, amongst other things, a requirement for persons in CF and PCF roles in regulated firms to take any steps reasonable in the circumstances to ensure that certain prescribed conduct standards are met. Business standards will also be imposed on regulated firms in due course.

The SEAR, which imposes additional requirements on firms, will initially apply to a limited range of regulated firms from July 2024, including credit institutions, insurance undertakings and certain investment firms; certain requirement under the SEAR will apply from July 2025. Fintech firms will generally not be in these categories, but the SEAR will be applied to other sectors on a phased basis.

2.3 Compensation Models

The permissible compensation models and disclosure requirements will depend on the type of service firms provide, their customer base and regulatory status, and the rules applicable to those services or customer types.

2.4 Variations Between the Regulation of Fintech and Legacy Players

As a general rule, there is no differentiation between services provided by fintech firms or legacy players but some regulated activities are more likely to be performed by fintech firms.

2.5 Regulatory Sandbox

The Central Bank has recently established an Innovation Sandbox Programme to inform the early-stage development of selected innovative initiatives and provide regulatory advice and support to firms on their innovative projects. The Innovation Sandbox Programme will take a thematic approach, with the theme of the first programme being *"Combatting Financial Crime"*. The Sandbox Programme framework comprises workshops, ongoing bespoke engagement with dedicated Sandbox Relationship Managers, and access to data platforms.

As part of the Digital Finance Package, the EU DLT pilot regime commenced in March 2023, creating a sandbox for successful applicant operators of market infrastructure to conduct the trading and settlement of DLT financial instruments.

2.6 Jurisdiction of Regulators

The Central Bank is the financial services regulator in Ireland, with responsibility for the authorisation and supervision of financial services providers. It supervises Irish firms from both a prudential and conduct of business perspective. For EEA passporting firms, the Central Bank will generally have a level of competence in relation to conduct of business requirements, rather than prudential requirements.

The European Central Bank is the competent licensing authority for new Irish credit institutions (banks), and supervises significant credit institutions directly.

The Data Protection Commission is the Irish supervisory authority for the GDPR.

The Irish Digital Services Act 2024 (Irish DSA) designates Coimisiún na Meán as the designated Digital Services Co-ordinator in Ireland, implementing and enforcing the Irish DSA in Ireland. The Competition and Consumer Protection Commission is also designated for certain matters relating to online marketplaces.

2.7 No-Action Letters

The Central Bank does not issue *"no-action"* letters as part of its enforcement regime.

Nonetheless, the ESAs have a legal basis to issue no-action letters if they consider that the application of one of the relevant legislative acts is liable to raise significant issues as provisions contained in such act may directly conflict with another relevant act, and if they have received relevant information and consider on the basis of that information that the application of the relevant provisions raises significant exceptional issues pertaining to:

- market confidence;
- consumer, customer or investor protection;
- the orderly functioning and integrity of financial markets or commodity markets; or
- the stability of the whole or part of the financial system in the EU.

Where the ESAs issue a no-action letter stating that competent authorities should not prioritise any supervisory or enforcement action in relation to a certain legislative act, this may indirectly influence actions taken by the Central Bank.

2.8 Outsourcing of Regulated Functions

If a regulated function is outsourced, the vendor is likely to require authorisation to provide that service, unless it can rely on an exemption.

Separately, a number of rules and requirements may apply to already regulated firms that are engaged in the outsourcing of regulated and unregulated functions. These are generally sector-specific – eg, the PSR and MiFID II contain outsourcing requirements that are relevant to in-scope firms.

By contrast, the Central Bank Cross-Industry Guidance on Outsourcing (the *"CBI Outsourcing Guidance"*) applies across sectors to all regulated firms and must be considered alongside specific outsourcing rules under the various sectoral legislation. The CBI Outsourcing Guidance is heavily influenced by the EBA Guidelines on outsourcing arrangements (the *"EBA Outsourcing Guidelines"*), which are applicable to credit institutions, certain investment firms, payment institutions and electronic money institutions.

ESMA has also implemented guidelines on outsourcing to cloud service providers (the *"ESMA Cloud Guidelines"*), which apply to a broad range of RFSPs falling under ESMA's remit. The EIOPA has also published guidelines on outsourcing to cloud service providers (the *"EIOPA Cloud Guidelines"*).

In addition, DORA applies to in-scope financial entities and requires that all contracts between financial entities and ICT third-party service providers for the use of outsourced ICT services must meet certain minimum contractual requirements.

2.9 Gatekeeper Liability

The extent to which any fintech provider is deemed *"gatekeeper"* for activities on its platform will depend on its activities or the services it provides. Fintech providers may be subject to various authorisation requirements or may fall within the scope of Irish AML legislation.

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

The Digital Markets Act (Regulation (EU) 2022/1925) (DMA) entered into force on 1 November 2022 and became applicable from May 2023. It requires gatekeepers that have established *"core platform service"* search engines, social networking services, app stores, web browsers, etc – to abide by various requirements around fairness and transparency.

2.10 Significant Enforcement Actions

The Central Bank has taken enforcement actions in a broad range of areas where breaches of financial services legislation have been committed by regulated entities. In 2024, the Central Bank took enforcement actions against three entities relating to breaches of the PSR, funds legislation and market abuse rules.

2.11 Implications of Additional, Non-Financial Services Regulations

Firms will need to ensure that they operate in accordance with non-financial services requirements in Ireland, including data protection laws, cybersecurity requirements, consumer protection legislation, company law and intellectual property law.

The Digital Services Act (Regulation (EU) 2022/2065) (DSA) and the DMA form a single set of rules to create a fairer digital space for users. The DMA applies to online gatekeepers that reach certain turnover volumes. The DSA regulates online intermediaries and platforms.

2.12 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. In 2023, the Central Bank required Irish payment and e-money firms to obtain a safeguarding audit.

As part of its supervisory expectations, the Central Bank expects CASPs to ensure that independent third-party assurance is provided on an annual basis, confirming that the safeguarding framework CASPs have in place is compliant with requirements.

A broad range of authorities may be relevant during a firm's life cycle, including tax authorities, the Office of the Director of Corporate Enforcement, exchanges and the Financial Services and Pensions Ombudsman.

2.13 Conjunction of Unregulated and Regulated Products and Services

For the most part, it is possible for a regulated entity to offer regulated and unregulated services, unless it is restricted by its financial services licence. Under both the PSR and EMR, the Central Bank is empowered to require firms that undertake additional activities to establish separate entities.

In their Joint Report on recent developments in crypto-assets, the EBA and ESMA highlighted examples of regulated entities providing both regulated and unregulated services.

2.14 Impact of AML and Sanctions Rules

The applicability of AML rules will depend primarily on whether a fintech company falls within the categories of *"designated persons"* under the CJA 2010. Where a fintech firm is regulated by the Central Bank, it will typically be a designated person.

EU and Irish financial sanctions rules will apply to all fintech firms regardless of authorisation status.

2.15 Financial Action Task Force Standards

Ireland has been a member of the Financial Action Task Force (FATF) since 1991. The AML and sanctions rules in Ireland closely follow the laws issued by the EU, which in turn are heavily influenced by the FATF standards.

2.16 Reverse Solicitation

The legislative framework under MiFID II and MiCAR provides for a reverse solicitation regime.

MiFID II

Under the MiFID Regulations, a third-country firm, as defined, will generally need to establish a branch in Ireland and obtain prior authorisation from the Central Bank before providing investment services or activities to retail clients and opted-up professional clients. However, there is an exemption where retail clients or opted-up professional clients initiate the provision of an investment service by a third-country firm, at their own exclusive initiative. Where a third-country firm solicits clients or potential clients in the EU, including through an entity acting on its behalf or having close links with it, it is not deemed a service provided at the own exclusive initiative of the client. Reverse solicitation does not entitle the third-country firm to market new categories of investment products or investment services to that individual.

The Markets in Financial Instruments Regulation (MiFIR) requires third-country firms that deal with certain *"per se"* professional clients or eligible counterparties to register with ESMA, unless the service was provided at the exclusive initiative of the client. The registration requirement only applies following the adoption of an equivalence decision by the European Commission and is not currently in force, as no equivalency determinations yet exist. As a result, national laws govern the access of third-country firms to these client types.

MiCAR

MiCAR also provides for a reverse solicitation exemption for the provision of CASP services by third-country firms to EU clients. In December 2024, ESMA published its final report on the guidelines on reverse solicitation under MiCAR, providing a non-exhaustive list of examples of solicitation.

It is generally accepted that the reverse solicitation rules contained in MiFID II and MiCAR will be interpreted very strictly.

3. Robo-Advisers

3.1 Requirement for Different Business Models

Once the activities of a robo-adviser constitute MiFID II *"investment services"* in respect of *"financial instruments"*, the robo-adviser will require authorisation as a MiFID II investment firm under the MiFID Regulations, unless an exemption applies.

The MiFID II investment services most likely to be triggered by robo-adviser activity are portfolio management and/or the provision of investment advice. MiFID II financial instruments include:

- transferable securities;
- units in collective investment undertakings;
- certain options, futures, swaps and other derivatives; and
- emissions allowances.

The MiFID Regulations requirements in relation to suitability assessments will also affect robo-advisers, and certain of the ESMA Guidelines

on MiFID Suitability are stated to be particularly applicable to robo-advisers, given the limited amount or total absence of human involvement.

Developers of robo-advisers involving crypto-assets will also need to consider their licensing and related conduct requirements under MiCAR, including in relation to suitability assessments where providing advice or providing portfolio management services.

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

No information is available in this jurisdiction.

3.3 Issues Relating to Best Execution of Customer Trades

A robo-adviser that is authorised under the MiFID Regulations and executes orders on behalf of clients is subject to the MiFID II rules, including the client order handling rules and best execution requirements. MiFID II and the MiFID Regulations also set out related requirements for portfolio managers placing orders or where firms receive and transmit orders. MiCAR introduces best execution requirements for CASPs.

4. Online Lenders

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

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

Commercial Lending

Commercial lending (ie, lending to corporates) does not generally require a financial services licence in Ireland, although AML registration and reporting to the Central Credit Register may be required.

Loans to Individuals and SMEs

By contrast, lending to individuals may require a retail credit firm authorisation under the CBA 1997, subject to certain exemptions. The scope of the Irish retail credit regime captures credit agreements, including buy-now-pay-later products or other indirect credit, as well as hire-purchase agreements and consumer-hire agreements. The Consumer Credit Act, 1995 contains another domestic-only regime for persons providing *"high-cost credit"* to consumers.

Lending to consumers is subject to a range of consumer protection requirements.

RFSPs (including EEA 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 Consumer Protection Code 2012 (CPC) and the Central Bank (Supervision and Enforcement) Act 2013 (Section 48) (Lending to Small and Medium-Sized Enterprises) Regulations 2015 (the *"SME Regulations"*).

Credit Servicing

Credit servicing (including legal title loan ownership, managing or administering a credit agreement and related borrower communications) in relation to loans to individuals and SMEs requires authorisation in certain circumstances under the CBA 1997. This regime also applies to hire-purchase agreements and consumer-hire agreements.

Separately, the EU-wide credit servicers directive (Directive (EU) 2021/2167) has been intro-

duced and regulates credit servicers in certain circumstances.

Crowdfunding

The Crowdfunding Regulation facilitates peer-to-peer business lending, with regulated crowdfunding service providers being authorised to facilitate the granting of loans. Crowdfunding service providers can also perform individual portfolio management of loans for investors within certain criteria.

4.2 Underwriting Processes

Irish conduct of business rules and legislation require creditworthiness or suitability assessments in certain circumstances; for example, the European Communities (Consumer Credit Agreements) Regulations 2010, the CPC and the SME Regulations are relevant in this regard.

Ireland has established a Central Credit Register under the Credit Reporting Act 2013, which lenders must check before advancing in-scope credit; the Act also requires lenders to report lending information.

4.3 Sources of Funds for Fiat Currency Loans

Credit institutions such as banks raise funds for their lending activities from a wide range of sources, including deposits, inter-bank lending, issuing debt 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 (eg, a retail credit firm) may raise funds for their lending activities from securitisations or lending from other investors or institutions. Funds may also be sourced through peer-to-peer lending (eg, via a crowdfunding service provider).

4.4 Syndication of Fiat Currency Loans

It is not typical for consumer loans or loans to small businesses to be syndicated. The Crowdfunding Regulation provides a European framework for peer-to-peer lending platforms.

5. Payment Processors

5.1 Payment Processors' Use of Payment Rails

Payment processors may use existing payment infrastructure or create or implement new payment rails, as long as they operate within the bounds of their financial services authorisation and adhere to relevant regulatory requirements.

5.2 Regulation of Cross-Border Payments and Remittances

Cross-border payments may be regulated under the PSR. There are also requirements in respect of wire transfers, credit transfers and direct debits (eg, the Single Euro Payments Area). The oversight framework for electronic payment instruments, schemes and arrangements (the *"PISA Framework"*) is also relevant to companies enabling or supporting the use of payment cards, credit transfers, direct debits, e-money transfers and digital payment tokens, including e-wallets.

6. Marketplaces, Exchanges and Trading Platforms

6.1 Permissible Trading Platforms

Crowdfunding Platforms

The activity of operating a peer-to-peer crowdfunding platform is regulated under the Crowdfunding Regulation, which provides a European framework for loan and investment-based crowdfunding.

Investment Services, Exchanges and Trading Platforms

The provision of investment services, 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 market operators and investment firms operating various types of trading venues, such as regulated markets, multilateral trading facilities (MTFs) and organised trading facilities (OTFs).

Crypto-Asset Exchanges

The operation of a crypto-asset exchange from Ireland involving exchange services between crypto-assets and/or crypto-assets and fiat currencies and/or the operation of a trading platform for crypto-assets will require authorisation as a CASP under MiCAR.

6.2 Regulation of Different Asset Classes

MiCAR applies only to crypto-assets that are not covered by existing EU legislation. MiCAR categorises in-scope crypto-assets into ARTs, EMTs and other type of crypto-assets, including utility tokens.

The provision of investment services (such as operating a trading venue) in relation to MiFID financial instruments (including those issued through DLT) is regulated under the MiFID Regulations.

6.3 Impact of the Emergence of Cryptocurrency Exchanges

MiCAR regulates the provision of crypto-asset exchange services and the operation of a trading platform for crypto-assets. MiCAR will apply to persons and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, including when part of such activities or services is performed in a decentralised manner.

Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of the MiCAR authorisation requirement, although each model will need to be considered separately.

6.4 Listing Standards

No formal listing standards exist for unregulated platforms. General contractual principles should apply, and certain general consumer protection rules may also apply. Trading venues established under MiFID or MiCAR are required to have detailed operating rules.

6.5 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 of MiCAR CASPs when executing orders.

6.6 Rise of Peer-to-Peer Trading Platforms

No information is available in this jurisdiction.

6.7 Rules of Payment for Order Flow

The MiFID II inducements, conflicts of interest and best execution rules will apply to all MiFID II investment firms, including in the context of payment for order flow, which is the practice of brokers receiving payments from third parties for directing client order flow to them as execution venues.

MiFIR prohibits financial intermediaries, when acting on behalf of retail clients or clients that have opted up to the professional client, from receiving a fee, commission or non-monetary

benefit from any third party for their execution on a particular execution venue, or for forwarding orders of those clients to any third party for their execution on a particular execution venue.

Under MiCAR, CASPs receiving and transmitting orders for crypto-assets on behalf of clients are prohibited from receiving any remuneration, discount or non-monetary benefit in return for routing orders received from clients to a particular trading platform or to another CASP.

6.8 Market Integrity Principles

In addition to domestic requirements, Ireland has implemented EU securities markets legislation, some of which is directly applicable. This legislation includes:

- the Prospectus Regulation;
- the Market Abuse Regulation;
- the Transparency Directive;
- the Short Selling Regulation;
- the Securities Financing Transaction Regulation;
- Regulation 648/2012 on OTC Derivatives, Central Counterparties and Trade Repositories (EMIR); and
- MiFID II.

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"*), and measures to prevent market abuse. It 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 other financial instruments, the price or value of which depends or has an effect on the price or value of the above and emission allowances. MAR can apply to other instruments and is not limited to transactions, orders or behaviour on a trading venue.

Market manipulation, as defined under the European Union (Market Abuse) Regulations 2016 (the *"MAR Regulations"*), is an offence in Ireland.

MiCAR introduces provisions to prevent and prohibit market abuse involving certain crypto-assets, as well as white paper requirements for crypto-asset issuances.

7. High-Frequency and Algorithmic Trading

7.1 Creation and Usage Regulations

The primary method of regulating 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.

For asset classes outside the scope of regulation under the MiFID Regulations, it would be important to consult the requirements applicable to the particular asset class.

7.2 Requirement to Be Licensed or Otherwise Register as Market Makers When Functioning in a Principal Capacity

Market makers in financial instruments will generally require authorisation under MiFID and must comply with specific rules if engaging in algorithmic trading to pursue a market-making strategy.

7.3 Regulatory Distinction Between Funds and Dealers

No information is available in this jurisdiction.

7.4 Regulation of Programmers and Programming

If programs or programmers are carrying out regulated activities, the applicable regulations will be relevant, but this will need to be assessed on a case-by-case basis. The AI Act will apply to providers who place on the market or put into service AI systems in the EU, and to users of AI systems located or with establishments within the EU.

8. Insurtech

8.1 Underwriting Processes

Only authorised insurance companies are permitted to underwrite insurance contracts in Ireland. Some insurtech companies are authorised as insurance companies, while others act as insurance intermediaries and require authorisation for that activity.

8.2 Treatment of Different Types of Insurance

Insurance companies must be authorised as a life insurer or a non-life insurer but not both (with limited exceptions). Life and non-life insurers are subject to different requirements.

Specific requirements in relation to motor insurance are set out in the European Union (Motor Insurance) Regulations 2023 due to the requirement for minimum compulsory cover for third-party motor insurance. There are a limited number of other kinds of compulsory insurance – eg, in relation to aircrafts and shipping.

Insurance products with an investment component are treated differently to other insurance products and are subject to the Packaged Retail and Insurance Based Investment Products (PRIIPs) Regulation.

Commercial and consumer insurance products are treated differently. Additional obligations apply when dealing with consumers, including the Central Bank's CPC, the Consumer Protection Act 2007 and the Consumer Insurance Contracts Act 2019.

9. Regtech

9.1 Regulation of Regtech Providers

Generally speaking, the provision of regtech services is less likely to be a regulated activity, but this will depend on the nature of the regtech service performed and the nature of the entity to which such services are provided.

9.2 Contractual Terms to Assure Performance and Accuracy

When outsourcing or sourcing ICT services, regulated entities may be obliged to impose certain contractual provisions on their service providers.

The CBI Outsourcing Guidance

Outsourcing is a particularly topical issue for the Central Bank. The CBI Outsourcing Guidance applies to all Irish regulated firms and is to be implemented alongside any specific sectoral legislative outsourcing requirements. It imposes similar contractual requirements to the EBA Outsourcing Guidelines (which apply directly to credit institutions, certain investment firms and payments/e-money institutions).

The EBA Outsourcing Guidelines

The EBA Outsourcing Guidelines 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. Specific termination rights, provisions around business continuity, data and access and audit rights for the regulated firm and its regulators are also required. The ESMA Cloud Guidelines and the EIOPA Cloud Guidelines may also be relevant to applicable entities where services are provided on a cloud basis.

DORA

A key requirement of DORA is that all contracts between financial entities (as defined in DORA) and ICT third-party service providers for the use of ICT services must meet certain minimum contractual requirements. Additional contractual requirements are placed on arrangements with ICT third-party service providers that support a critical or important function of the financial entity.

10. Blockchain

10.1 Use of Blockchain in the Financial Services Industry

Traditional domestic and international institutions operating in Ireland are investigating the use of blockchain, and certain institutions have conducted trials in this area. Ireland is also home to a number of crypto-led businesses, and this population is expected to grow.

10.2 Local Regulators' Approach to Blockchain

The Central Bank's Approach

Firms providing certain services in relation to crypto-assets are required to obtain a CASP authorisation (see **1.1 Evolution of the Fintech Market**). In December 2024, the Central Bank released its supervisory expectation for CASPs, outlining its risk appetite for crypto-asset services in Ireland.

Outside of these processes, the Central Bank has issued consumer explainers and warnings, and remains cautious on the benefits and risks of crypto. However, it has acknowledged that technological innovation is a key feature of the environment in which it seeks to deliver its mandate.

On 22 October 2024, the Department of Finance published its final report on the review of the *"Funds Sector 2030"*. One of the areas being examined is how technological change and innovation will influence future development, including mapping a pathway for the broader adoption of tokenisation.

10.3 Classification of Blockchain Assets

The Central Bank has confirmed in a consumer warning that virtual currencies are not legal tender.

Crypto-Assets in Scope of MiCAR

MiCAR defines crypto-assets as *"a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology"*. It applies only to crypto-assets that are not covered by existing EU legislation, and categorises in-scope crypto-assets into ARTs, EMTs and other type of crypto-assets, including utility tokens.

Significance of MiFID II Definition of Transferable Securities to Regulatory Approach

The MiFID Regulations apply to financial instruments, including those issued by means of DLT.

One area of focus has been whether a particular blockchain asset qualifies to be considered as a MiFID II financial instrument, typically focused on the definition of a transferable security.

Certain types of crypto-assets could instead qualify as other MiFID II financial instruments, such as units in collective investment undertakings, money-market instruments or derivatives; a case-by-case analysis is required. Depending on classification, a range of other regimes could be triggered – eg, a transferable security falls within the regulatory scope of, inter alia, MiFID II, the Prospectus Regulation and MAR.

In December 2024, ESMA published its Final Report on the Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments, which provides further clarity on the approach to be taken.

Crypto-Assets and Payment Services Under the Electronic Money Directive

Only electronic money institutions authorised under the Electronic Money Directive and credit institutions can issue EMTs – ie, crypto-assets that purport to maintain a stable value by referencing the value of one official currency.

If a person performs *"payment service"* as listed in PSD2 with a blockchain asset that qualifies as *"electronic money"* under the Electronic Money Directive, such activity would fall within the scope of PSD2 by virtue of constituting *"funds"*.

In a recent letter to the EBA and ESMA, the European Commission called for *"no-action letter"* with regard to the enforcement of the requirements on authorisation in PSD2 in terms of services with EMTs provided by CASPs that may be inadvertently covered by the PSD2.

10.4 Regulation of "Issuers" of Blockchain Assets

Assuming the blockchain assets are not governed by any existing EU legislation, the issuance of crypto-assets is governed by MiCAR.

See **1.1 Evolution of the Fintech Market** regarding the regulatory framework in MiCAR for issuers of crypto-assets, including issuers of ARTs and EMTs.

10.5 Regulation of Blockchain Asset Trading Platforms

Where blockchain assets constitute MiFID II financial instruments such as transferable securities, the operation of a trading platform will be in the scope of existing regulatory regimes.

The operation of a trading platform may involve the issuance of electronic money or the provision of payment services, in order to facilitate wallet and payment features.

MiCAR imposes requirements on CASPs operating a trading platform for crypto-assets or engaging in exchange services between crypto-assets and/or crypto-assets and funds.

10.6 Staking

MiCAR does not contain provisions specific to staking and therefore does not create specific requirements or licensing obligations for staking. However, the European Commission confirmed that where the staking service provider holds the private keys to the staked crypto-assets, the ser-

vice provider is required to be authorised under MiCAR to provide custody and administration of crypto-assets on behalf of clients. Depending on the arrangements between staking service providers and customers, other MiCAR CASP services may be relevant.

Providing staking services may fall within existing regulatory regimes depending on the legal classification of the crypto-asset in question.

10.7 Crypto-Related Lending

MiCAR does not specifically address the lending and borrowing of crypto-assets, including EMTs; instead, it proposes that the Commission shall present a report to the European Parliament containing an assessment of the necessity and feasibility of regulating lending and borrowing of crypto-assets. To assist the European Commission with this report, the EBA and ESMA have published a Joint Report on recent developments in crypto-assets, including lending and borrowing of crypto-assets.

Lending services relating to crypto-assets may fall within existing regulatory regimes depending on the legal classification of the crypto-asset in question.

10.8 Cryptocurrency Derivatives

In December 2024, ESMA published its Final Report on the Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments, which provides further clarity on the classification of crypto-assets as derivative contracts.

Firstly, with regards to crypto-assets as an underlying asset for derivatives, ESMA notes that national competent authorities and financial market participants should consider the possibility for crypto-assets to be eligible underlying assets in derivative contracts for the purposes of MiFID II.

Secondly, ESMA notes that crypto-assets themselves can be qualified as derivatives. In this regard, national competent authorities and financial market participants should consider the following as part of their assessment:

- whether the rights of the crypto-asset holders are contingent upon a contract based on a future commitment, creating a time-lag between the conclusion and performance of the obligations under such contract;
- whether the crypto-asset's value is derived from that of an underlying asset; and
- whether the crypto-asset follows the settlement modalities as referred to in MiFID II.

Where the crypto-asset serves as an eligible asset in derivative contracts for the purposes of MiFID, or where the crypto-asset itself amounts to a derivative contract within scope of MiFID II, entities providing investment services, as defined in MiFID II, in relation to such crypto derivatives may need to consider the impact of MiFID II on their business.

10.9 Decentralised Finance (DeFi)

DeFi presents challenges for EU regulatory authorities, as it does not sit neatly within the existing regulatory landscape.

DeFi transactions will require a case-by-case analysis to determine the regulatory categorisation of the activities involved and jurisdictional questions regarding applicable legislation and relevant regulatory bodies. This is a rapidly developing area, and there is expected to be increasing regulatory interest in DeFi.

MiCAR should not apply where crypto-asset services are provided in a fully decentralised manner without any intermediary. MiCAR instead proposes that the Commission shall present a report to the European Parliament containing an assessment of the development of DeFi in the crypto-assets markets and of the adequate regulatory treatment of decentralised crypto-asset systems without an issuer or CASP, including an assessment of the necessity and feasibility of regulating DeFi. In January 2025, the EBA and ESMA published a Joint Report on recent developments in crypto-assets, including DeFi.

10.10 Regulation of Funds

Irish regulated investment funds are authorised either as UCITS or as alternative investment funds (AIFs).

Distinctions Between Digital Assets

The Central Bank has provided guidance on investment in digital assets, which are generally considered to be assets that exist in digital form and that attach ownership rights that depend primarily on cryptography and distributed ledger or similar technology. This guidance recognises that the nature and characteristics of digital assets vary considerably, and distinguishes, for example, between digital assets that are tokenised traditional assets and digital assets that are based on intangible or non-traditional underlying assets.

For the purposes of its requirements, the Central Bank considers *"digital assets"* to be the latter type of digital asset. Its guidance states that the Central Bank is highly unlikely to approve a UCITS or an AIF marketed to retail investors proposing any exposure (either direct or indirect) to digital assets.

In April 2023, the Central Bank increased the investment limits for QIAIFs seeking exposure to the latter type of digital assets, as follows:

- where a QIAIF is open-ended, it can gain exposure to digital assets of up to 20% of NAV; and
- where a QIAIF is closed-ended or is open-ended with limited liquidity, it can gain exposure to digital assets of up to 50% of NAV.

In order to avail of these limits, AIF managers must ensure the following requirements are satisfied:

- an effective risk management policy is implemented to address all risks relevant to investment in digital assets, at a minimum addressing risk relating to liquidity, credit, market, custody, operational, exchange risk, money laundering, legal, reputational and cyber-risk;
- appropriate stress testing on the proposed investment in digital assets, reflecting the asset price volatility of digital assets, including the potential entire loss of value in the investment;
- an effective liquidity management policy is in place, which includes a sufficient suite of tools to enable the AIF manager to manage liquidity events arising in the QIAIF;
- the prospectus of the QIAIF must contain clear disclosure in relation to the nature of the proposed investment in digital assets and a clear articulation of the risks associated with that investment; and
- the QIAIF should assess the overall construction of its portfolio to ensure that there is alignment between the redemption profile, the level of investment in digital assets and the likelihood of illiquidity (in both normal and stressed conditions) in the types of digital assets invested in.

Direct exposure by QIAIFs to digital assets continues to be prohibited by the Central Bank, pending satisfactory demonstration that the depositary safekeeping obligations can be complied with in accordance with the Alternative Investment Fund Managers Directive (Directive 2011/61/EU). The Central Bank provides for a pre-submission approval process in the event a QIAIF proposes to invest indirectly in digital assets in excess of the thresholds outlined above or to seek to make any direct investment in digital assets.

On 7 May 2024, ESMA issued its Call for Evidence on the review of the UCITS Eligible Assets Directive (2007/16/EC) to assess possible changes to the eligibility rules under which UCITS may gain direct and indirect exposures, including in respect of certain asset categories that may give rise to divergent interpretations and/or risk for retail investors, including crypto-assets. With respect to indirect exposures, ESMA is particularly interested in stakeholder input on exchange-traded products, including ETFs with crypto-assets as an underlying. ESMA is due to deliver its technical advice to the European Commission by April 2025.

10.11 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. Typically, a pure cryptocurrency will not be considered a financial instrument under MiFID II but would be considered a crypto-asset within the scope of MiCAR.

10.12 Non-Fungible Tokens (NFTs)

MiCAR will not apply to crypto-assets that are unique and not fungible with other crypto-assets. The recitals to MiCAR state that the fractional parts of a unique and non-fungible crypto-asset should not be considered unique and non-fungible, and that the issuance of crypto-assets as NFTs in a large series should be considered as an indicator of their fungibility. Therefore, categorisation will depend on the individual characteristics of an NFT.

A case-by-case analysis is also required to understand if an NFT would be considered a financial instrument under MiFID.

11. Open Banking

11.1 Regulation of Open Banking

PSD2 introduced two new regulated payment services which, in summary, allow customers to use third parties to obtain payment initiation services, and enable third parties to access payment data to provide account information services. This facilitates open banking. Application programming interfaces are to be used for third-party access to online payment accounts.

As part of the review of PSD2, the Commission carried out a targeted consultation on open finance framework and data sharing in the financial sector. PSD3 will seek to improve the functioning of open banking through the removal of the remaining obstacles to the provision of open banking services, by improving customers' control over their payment data and by enabling new innovative services to enter the market.

11.2 Concerns Raised by Open Banking

PSD2 imposes certain conditions on access to and use of data by firms providing a payment initiation service or account information service. This includes a requirement 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 rights to withdraw consent, to access data and for information to be erased. In sharing data with third parties such as account information service providers, banks will need to be aware of the potential for fraud or other risks.

12. Fraud

12.1 Elements of Fraud

Fintech firms are at the forefront of fraud-related incidents, with the most common examples being credit card fraud, identity fraud and scam-related activity. Many firms, including VASPs, have reported concerns relating to transactions and access or ownership of virtual asset wallets, prominent use of fake identification documents or stolen KYC data, and the involvement of shell companies and bank accounts opened by a third party.

Given the increasing prevalence of fraud in the fintech space, it has been paramount to address through regulation. PSD2 actively addressed account takeover fraud via Strong Customer Authentication (SCA), but steps are now being taken to update PSD2 to help stem the tide of the emerging types of fraud.

12.2 Areas of Regulatory Focus

The Central Bank noted in its Regulatory Supervisory Outlook Report 2024 that, while digitalisation continues to deliver concrete benefits for consumers, it also introduces new risks in terms of frauds and scams. The Central Bank sees smishing, phishing and push payment fraud increasing in frequency and becoming more sophisticated. The Central Bank wrote to regulated firms, communicating its expectations with respect to their effective measures to mitigate the risks of fraud or scams and, in particular, Authorised Push Payment fraud.

12.3 Responsibility for Losses

Under the MiFID Regulations, investment firms that safeguard client financial instruments and funds must introduce adequate organisational arrangements to minimise the risk of the loss or diminution of client assets, or of rights in connection with those assets, as a result of misuse of the assets, fraud, poor administration, inadequate record-keeping or negligence.

Investment firms are required to participate in investor compensation schemes. Such schemes compensate investors, for instance, if an investment firm goes bankrupt and is unable to return financial instruments belonging to an investor.

PSD2 provides that, in the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, in certain circumstances, the payment service provider should be able to conduct an investigation, within a reasonable time, before refunding the payer.

The payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument. There should be no liability where the payer is not in a position to become aware of the loss, theft or misappropriation of the payment instrument. The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently.

MiCAR provides that CASPs providing custody and administration of crypto-assets on behalf of clients shall be liable to their clients for the loss of any crypto-assets or of the means of access to the crypto-assets as a result of an incident that is attributable to them. The liability of the CASP shall be capped at the market value of the crypto-asset that was lost, at the time the loss occurred. Incidents not attributable to the CASP include any event in respect of which the CASP demonstrates that it occurred independently of the provision of the relevant service, or independently of the operations of the CASP, such as a problem inherent in the operation of the distributed ledger that the CASP does not control. In contrast to the rules under the MiFID Regulations for investment services, crypto-assets will not be covered by an investor compensation scheme.

Regulated financial service providers may also be subject to fines and compensation requests for contraventions of financial services legislation as part of the administrative sanction procedure or pursuant to a private right of action for damages by customers who suffered loss or damage as a result of such contraventions.