
INTERNATIONAL
FINTECH REVIEW
2023 / 24
Beaumont Capital Markets

IRELAND
The International Fintech Review 2023/24

A&L GOODBODY

Patrick Brandt
Partner

pbrandt@algoodbody.com

+353 1 649 2337

www.algoodbody.com

BIO

Patrick Brandt is a partner and head of A&L Goodbody's Financial Regulation team. Before joining ALG, Patrick led Skadden Arps London office's financial regulatory group.

Patrick has extensive experience advising a wide variety of banks, payment institutions, asset managers, brokers and intermediaries on non-contentious and contentious regulatory issues. Patrick also spent time as a regulator, having worked in the UK Financial Services Authority's enforcement division.

A&L Goodbody

A&L GOODBODY

Louise Hogan
Associate

lahogan@algoodbody.com

+353 1 649 2961

www.algoodbody.com

BIO

Louise Hogan is an associate in A&L Goodbody's Financial Regulation group. Louise has experience advising a wide variety of banks, payment institutions, electronic money institutions, asset managers, brokers and intermediaries on regulatory and compliance issues.

Her particular areas expertise include advice on conduct of business and prudential requirements, authorisation and passporting requirements, acquisitions and disposals, corporate governance, fitness and probity and AML/CFT.

A&L Goodbody

A&L GOODBODY

Sinéad Gleeson
Associate

sgleeson@algoodbody.com

+35316492171

www.algoodbody.com

BIO

Sinéad Gleeson is an associate in A&L Goodbody's Financial Regulation Advisory group. Sinéad advises a range of domestic and international clients across the financial services sector.

Clients include credit institutions, investment firms, payment institutions and electronic money institutions, as well as other regulated and unregulated entities. Sinéad advises on a variety of regulatory and compliance issues, for example conduct of business and prudential requirements, authorisation and passporting requirements, acquisitions and disposals, corporate governance, fitness and probity, along with AML/CFT.

A&L Goodbody

A&L Goodbody

Brief overview of fintech in Ireland

Home to a vibrant and dynamic technology sector as well as an established financial services landscape, Ireland continues to be a hub for fintech.

Fintech is a strong driver of growth and employment in the Irish economy, with the sector being supported by financial and non-financial government initiatives and strategies. The Irish fintech ecosystem has developed in the context of a favourable business environment, which includes an attractive corporate tax regime, a credible financial regulator, a skilled and relatively young English-speaking workforce and EU membership.

> “
>
> Key supervisory priorities for the Central Bank of Ireland (CBI) that are particularly relevant for the fintech sector include safeguarding of client funds, outsourcing, and operational and financial resilience.

The pace and scale of developments in fintech create significant opportunities as well as challenges for both market participants and regulators. A balance must be struck between innovation and regulation, ensuring that firms are able to innovate and harness opportunities while ensuring that this does not come at the cost of customers or financial stability.

In this article we consider some current trends and key developments in fintech, informed by our Irish market experience.

Regulatory focus

Supervisory priorities

Key supervisory priorities for the Central Bank of Ireland (**CBI**) that are particularly relevant for the fintech sector include safeguarding of client funds, outsourcing, and operational and financial resilience.

Safeguarding

Safeguarding rules require regulated fintechs to segregate and protect customer funds. In a January 2023 industry communication, the CBI noted that one in four Payment Institutions (**PIs**) and E-money Institutions (**EMIs**) had self-identified deficiencies in their safeguarding risk management frameworks during 2022. Accordingly, all PIs and EMIs were required to conduct a specific safeguarding audit, with the results to be provided to the CBI, reflecting intensified CBI scrutiny in this area. In our view, additional feedback and/or action by the CBI is likely to follow the submission of the safeguarding audits during the course of next year.

Outsourcing

The use of outsourcing arrangements has become the norm in the fintech industry. Outsourcing risk management continues to be a supervisory priority for the CBI. The CBI has highlighted the risks of sub-outsourcing, off-shoring and concentration risk. The CBI has also made clear that intragroup outsourcing carries the same risks as third-party outsourcing and expects such arrangements to be managed accordingly, with appropriate outsourcing agreements in place to manage risk.

An area of concern for firms has been the CBI's view that branch service provision should also be regarded as a form of intra-group service provision, as the risks are indistinguishable from those related to outsourcing. Whilst a formal legal agreement between a branch and its head office is obviously not possible, in order to meet CBI guidance, firms should nevertheless seek to have in place appropriate internal policies, procedures and controls providing for equivalent measures to ensure the effective oversight and supervision of any branch services.

Operational resilience

The need for fintechs, both regulated firms and their technical services providers, to guard against operational outages and cybercrime is obvious. The CBI has been increasingly focused on operational resilience and the need for firms to demonstrate readiness for, and resilience to, operational disruptions. The CBI has observed an increase in the number of major incidents/outages being reported by PIs and EMIs, with many of those having been as a result of issues with critical outsourced service providers (**OSPs**), both group and third-party. Firms are therefore expected to review and adopt appropriate measures to strengthen and improve their operational resilience frameworks in line with the CBI cross-industry guidance on operational resilience (published 2021) and cybersecurity (published 2016). These domestic requirements will be supplemented by the Digital Operational Resilience Act (**DORA**) when it comes into full force in January 2025.

In this regard, we have seen a specific regulatory focus on firms' ability to ensure continuation of services following unforeseen disruptions/outages, with low regulatory tolerance for such incidents. It is therefore important for firms to ensure adequate resources and focus on these risks. Accordingly, regardless of the technology used, firms should seek to follow the pillars of operational resilience, namely:

- **Identification:** identifying and preparing critical impact areas in advance
- **Mapping:** mapping operational interdependencies between systems and service providers
- **Testing:** ensure that there is regular and rigorous testing of systems and dependencies
- **Look-back:** where operational incidents occur, a formal look-back review should be undertaken to understand where issues arose, as well as what operational risk management measures performed well

Financial resilience

It is important that fintech firms are financially resilient so that business failures in the regulated area are kept to the bare minimum. The CBI completed a thematic review of business model and strategic risk across a number of PIs and EMIs during 2022. It found that certain firms did not have defined or embedded Board-approved business strategies in place.

> “
>
> We have seen a specific regulatory focus on firms' ability to ensure continuation of services following unforeseen disruptions/outage.

The CBI noted that, while firms may operate within and be reliant on group strategic decisions to inform local strategy, it is critical that firms ensure there is sufficient financial (capital and liquidity) and operational (including resources, IT etc.) capacity and capability to execute that strategy. It further noted weaknesses in firms' financial projections and reiterated its expectations that firms have robust strategic and capital planning frameworks.

Market trends

Use of contactless payments

The latest figures from the Banking & Payments Federation Ireland's Payments Monitor (published 13 October 2023) show a strong move towards use of contactless payments in Ireland. Almost 85% of credit and debit card transactions in H2 2023 were contactless payments, with 41% of those being made with mobile wallets instead of physical cards. The Payments Monitor also shows that the number of online and mobile banking payments grew by 4% year on year in H1 2023. Since H1 2018, these forms of payment have risen by 60%.

Increased fintech offerings

A number of Irish fintechs are seeking to expand their product and service offering, with a lot of activity around digital wallets and embedded payments, potentially requiring an expansion of their authorisation/permissions. This includes a number of UK fintech firms who chose Ireland as their European base post-Brexit, who have matured and settled into the European market and are now looking to expand. The withdrawal of two retail banks from the Irish market (Ulster Bank and KBC) also means that the Irish retail banking and payments market is now smaller, potentially prompting further offerings from non-bank service providers.

The CBI has highlighted the importance of early regulatory engagement, and ensuring that appropriate governance and risk management frameworks are put in place with sufficient financial and operational capacity to deliver on the proposed business strategy. In our experience, there is also a related general European trend, with a shift in regulatory expectations for firms seeking authorisation as EMIs or PIs in terms of the level of local substance a firm is required to have irrespective of Member State.

> “
>
> We continue to see an increase in firms using regtech solutions to assist with compliance and risk management and monitoring.

The blurring of lines between more traditional finance models and fintech also continues, with more software providers diversifying into finance or finance adjacent sectors, and seeking regulatory licences to provide new regulated services themselves.

Financial institutions are also seeking to broaden their product offering by embracing fintech, often through partnering with fintech companies (e.g. in the area of strong customer authentication). Conversely, there is also an observable trend of fintechs moving into the provision of more traditional financial services (e.g. mortgages). On the crypto-asset side, we are continuing to see strong interest from issuers and exchanges in establishing in Ireland.

Use of regtech solutions

We continue to see an increase in firms using regtech solutions to assist with compliance and risk management and monitoring. While this helps drive efficiencies and deliver other benefits for both firms and customers, it also involves increased reliance on OSPs. This in turn has created increased risks from cyber threats, as well as increasing firms' operational risk profiles from the CBI's perspective. Firms should therefore have a clear understanding of the benefits, risks, and operational interdependencies and vulnerabilities of any new systems or software solutions being deployed.

Key developments

Regulatory approach to technology

The CBI takes a 'technology-neutral' approach to regulation, focusing on the risks associated with the use of technology solutions. Firms are expected to do sufficient due diligence on systems to understand how those systems work and their potential risks, including customer impact and ability to comply with regulatory requirements.

In particular, the CBI is focused on the risks that can arise for consumers, potential risks to personal data, and the increased exposure of firms and consumers to operational issues such as system weaknesses, outages, and cyber vulnerability.

In the context of AI, as the first sector to be reviewed, the CBI has expressed concern about the ethical use of data in relation to the insurance sector. It identified the risk of financial exclusion of consumers, data protection and cybersecurity issues, complex outsourcing risks and the importance of informed consent from consumers.

The use of AI in the EU will soon be regulated by the AI Act, the world's first comprehensive AI law. The AI Act will adopt a risk-based approach, categorising AI systems into four risk categories from 'minimal' to 'unacceptable', with corresponding compliance requirements attached to each category (and systems categorised as 'unacceptable' being prohibited). The majority of obligations will attach to high-risk systems. In terms of AI systems likely to be used in the fintech space, from the current text it seems likely that systems used to evaluate credit scores or determine creditworthiness of an induvial would fall into the high-risk categorisation, while chatbots that use generative AI or systems that flag fraudulent transactions would not. The AI Act also proposes requirements around the design and development of AI technology such as transparency, human oversight, risk management, technical documentation demonstrating compliance, and security.

The AI Act is expected to pass before the end of 2023 and will likely enter into force towards the end of 2025 or early 2026.

Digital Operational Resilience

DORA is a key current area of focus in the fintech sector. It aims to harmonise rules across the EU to address Information and Communications Technology (**ICT**) risk in the financial sector, and create a regulatory framework for firms to ensure that they can withstand, respond to, and recover from, ICT-related disruptions and threats, including cyber-attacks.

DORA aims to mitigate ICT risk by setting targeted rules relating to:

- ICT risk management
- ICT third-party risk management
- incident reporting
- digital operational resilience testing
- information and intelligence sharing

It applies to a wide range of financial services entities, including PIs, investment firms, and crypto-asset service providers, as well as to critical ICT third-party service providers.

Given the CBI's existing guidance on operational resilience, Irish firms should be ahead of the curve when it comes to DORA implementation. Nevertheless, we have seen some concern from firms around how CBI expectations will square with the upcoming European requirements. Although the CBI has stated that its expectations should not be inconsistent with DORA, the prescriptive obligations are not identical. Firms will therefore need to review their existing ICT governance and risk management frameworks to ensure DORA compliance.

DORA is a key current area of focus in the fintech sector.

Firms might also note the revised Network Information Security Directive which introduces stricter procedures around incident reporting, expands the scope of security measures firms must have in place, as well as requirements around supply chain security, cyber security training for staff, encryption and penetration testing.

Markets in Crypto-Assets Regulation (MiCA)

MiCA forms part of the EU's Digital Finance Package and aims to create a comprehensive regulatory regime for cryptocurrencies across the EU, implementing a regulatory framework for crypto-assets not already covered by existing legislation. MiCA primarily focuses on the issuance of crypto-assets and the provision of crypto-asset services, by requiring providers to meet consumer protection, transparency, conflict of interest and governance standards. Many of the measures set out in MiCA will be familiar to those working in currently regulated sectors, as it seeks to introduce similar protections for consumers and the market more generally.

MiCA introduces requirements including:

- offerings and marketing to the public of crypto-assets, including an obligation to publish an information document called a "white paper"
- asset-reference tokens and e-money tokens (e.g. stablecoins), including an obligation for issuers to be authorised in the EEA and the publication of a white paper in respect of the relevant offering
- crypto-asset service providers, including regulatory licensing requirements, and in respect of specific services such as custody of crypto-assets, trading platforms for crypto-assets, exchange of crypto-assets for fiat currency or for other crypto-assets, and order execution

"

The upcoming implementation of the SEPA Instant Payment Regulation will also be a significant development in rolling out instant payments across the EEA.

MiCA also introduces a market abuse regime, based on prohibitions of unlawful disclosure of inside information, insider dealing, and market manipulation.

Revised Payment Services Directive (PSD3)

In June 2023, the European Commission put forward a proposal to amend and modernise payments through PSD3. Specific proposals include:

- allowing payment service providers (**PSPs**) to share fraud-related information between themselves, increasing consumers' awareness
- levelling the playing field between banks and non-banks, in particular by allowing non-bank PSPs access to all EU payment systems, with appropriate safeguards, and securing those providers' rights to a bank account
- combating and mitigating fraud by making a system for checking alignment of payees' IBAN numbers with their account names mandatory for all credit transfers

These clarifications will be welcomed by industry. It is also hoped that PSD3 will cut down on regulatory divergence between Member States, including greater consistency in the application of exemptions. However, certain changes could have the potential to result in some firms currently operating in Ireland under exemptions needing to become licensed as an EMI or PI going forward, or otherwise to cease providing payment services themselves (likely partnering with existing regulated PSPs to facilitate transactions in the future).

The upcoming implementation of the SEPA Instant Payment Regulation will also be a significant development in rolling out instant payments across the EEA.

Individual accountability

The Individual Accountability Framework (**IAF**) is one of the most important Irish regulatory developments in recent years. It became law in 2023, and seeks to make fundamental changes to the existing individual liability and enforcement regimes for members of senior management in regulated entities.

The IAF contains the following key elements:

- The Senior Executive Accountability Regime (**SEAR**)
- common conduct standards (applying to individuals in all regulated firms) and additional conduct standards (applicable to senior executives)
- enhancements to the existing Fitness & Probity regime
- amendments to the CBI's Administrative Sanctions Procedure

The IAF is being introduced in light of regulatory focus on individual accountability, good governance, risk management, and firms' culture and conduct over the last number of years. Although it provides for significant legal changes, the CBI's message has been consistent in that it does not mean a change in regulatory approach overall. Instead the IAF signifies a move away from more rules-based prescribed contraventions towards a focus on conducts standards more akin to general principles.

Conclusion

There are significant regulatory and supervisory changes due to come into effect in the Irish fintech market over the next year or so. These changes reflect both new ways in which firms are doing business, as well as reflecting insights gained by the CBI and other regulators as part of their supervisory and regulatory engagements.

The ever-increasing use of technology, both for delivery of services and to support compliance by regulated entities, poses opportunities for fintechs. However, firms will need to be conscious of the additional risks, interdependencies, and reliance on third parties that this creates. Firms will need to manage these challenges proactively to ensure appropriate and robust oversight and management of their systems and services providers.

Ireland nevertheless remains an attractive jurisdiction in which to base new fintechs, developing and offering new and novel products and services to customers both in Ireland and across the EU.

“

There are significant regulatory and supervisory changes due to come into effect in the Irish fintech market over the next year or so.