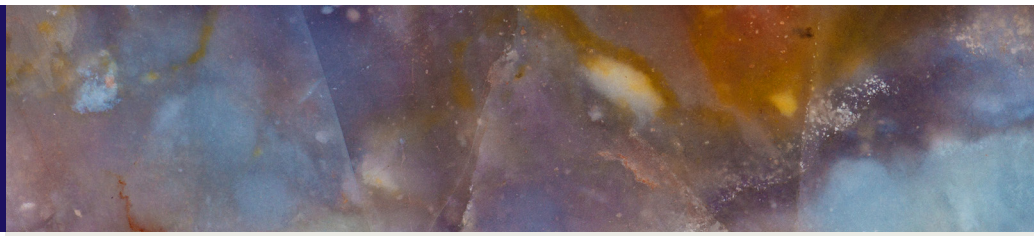
McCann FitzGerald

Financial Services Regulatory Group

Bulletin

DECEMBER 2016



IN THIS ISSUE:

Financial Services Regulatory Group Bulletin

IN THIS ISSUE:

Introduction

Our latest Financial Services Regulatory Group Bulletin contains new updates on significant developments in financial services regulation regarding cyber security, money-laundering, payment service providers and the definition of a consumer.

Because of the fast-moving nature of financial services regulation and the sheer volume of regulatory material being produced, we regularly upload briefings on the firm's website dealing with significant developments. In this bulletin we have included an easy way to access the briefings we have published over the past few months, in case you have not had a chance to look at them yet.

Financial Services Regulatory Group

The Financial Services Regulatory Group forms part of McCann FitzGerald's wider Finance Group which is the leading Finance Practice in the Irish market. Our Financial Services Regulatory Group advises regulated financial services providers and other clients on the complex regulatory and compliance issues arising in relation to the establishment and authorisation of new financial services providers; corporate governance and conduct of business issues; the provision of retail and wholesale financial services; regulatory capital requirements; insider dealing and market abuse issues; consumer credit matters; anti-money laundering; and the administrative sanctions process.

Josh Hogan

Partner, Head of Financial Services Regulatory Group

Financial Services Regulatory Group Bulletin

IN THIS ISSUE:

EMIR

The past few months have seen a number of significant developments regarding the EMIR clearing obligation as well as the finalisation of the regulatory technical standards on risk mitigation techniques for non-centrally cleared over-the-counter ("**OTC**") derivatives. The Central Bank of Ireland has also published its Recommendations for EMIR Regulatory Returns.

Link to briefing: *EMIR Update - Margin Requirements for Non-Centrally Cleared Over-the-Counter Derivatives*

Link to briefing: *Second Delegated Regulation on the EMIR Clearing Obligation*

Link to briefing: *EMIR Update: The Clearing Obligation and Risk Mitigation Techniques for Non Centrally Cleared OTC Derivatives*

Link to briefing: *EMIR Update - Risk Mitigation Techniques for Non-Centrally Cleared OTC Derivatives*

Link to briefing: *EMIR: Central Bank of Ireland Recommendations for EMIR Regulatory Returns*

Link to briefing: *Small FCs to have more time for EMIR Clearing*

Link to briefing: *New EMIR Margin Requirements for Uncleared OTC Derivatives*

Financial Services Regulation

We have published on a number of notable developments in financial services regulation over the last number of months affecting a diverse range of subjects, including payment services, mortgages, credit reporting and money laundering. We have also published a number of briefings outlining the legal framework applicable to diverse financial service providers, including banks, MiFID firms and e-money and payment institutions.

Link to briefing: *Coming Soon - A New Regulatory Framework for Payment Service Providers*

Link to briefing: *Latest Developments in Crowdfunding*

Link to briefing: *New Rules for Mortgage Credit and Property Related Loans*

Link to briefing: *Increased Protection for Variable Rate Mortgage Holders*

Link to briefing: *Are You Ready? SME Regulations 2015 Come Into Force on 1 July 2016*

Link to briefing: *Ireland as a Location for Electronic Money and Payment Institutions*

Link to briefing: *Ireland as a Location for MiFID Investment Firms*

Link to briefing: *Ireland as a Location for Banks*

Link to briefing: *Deadline Approaching for Collateral Reuse Compliance*

Link to briefing: *Creditors Be Aware: Credit Reporting Starts Soon*

Link to briefing: *Update on the MiFIR Trading Obligation for Derivatives*

Link to briefing: *Do you Need to Establish a Register of Beneficial Owners?*

Financial Services Regulatory Group Bulletin

IN THIS ISSUE:

Insurance

Our briefing on Ireland as a Location for Insurance Undertakings outlines the regulatory framework applicable to insurers in Ireland. Another briefing focuses on governance requirements for insurers, which have been a key area of focus for regulators under Solvency II. In addition, we have published two briefings on the PRIIPs Regulation 1286/2014.

Link to briefing: *Ireland as a Location for Insurance Undertakings*

Link to briefing: *EU Regulatory Developments – Governance Requirements for Insurers*

Link to briefing: *Q&A on the PRIIPs Regulation*

Link to briefing: *Commission Proposes New PRIIPs Deadline*

Investment Management Updates

We have published several updates on topical developments in investment management, including on UCITS share classes, the delegated regulation on UCITS' depositaries' obligations, PRIIPs, the new Market Abuse Regulation, statutory audits and loan origination. We have also published briefings outlining the general legislative framework applicable to investment funds in Ireland as well as to qualifying investor alternative investment funds.

Link to briefing: *EU Regulatory Updates for Funds and Fund Managers*

Link to briefing: *Updates for Fund Managers: Fund Management Company Governance*

Link to briefing: *Update for Funds on the Main Securities Market*

Link to briefing: *Q&A on the PRIIPs Regulation*

Link to briefing: *Asset Management & Investment Funds in Ireland: An EU Platform*

Link to briefing: *Irish Qualifying Investor Alternative Investment Funds*

Link to briefing: *Investment Funds in Ireland*

Link to briefing: *Commission Proposes New PRIIPs Deadline*

Link to briefing: *Central Bank of Ireland Relaxes Restrictions on Loan Originating Funds*

IN THIS ISSUE:

Market Abuse

The new framework regulating market abuse, which has been in effect since 3 July 2016, considerably expands the scope of the pre-existing market abuse rules in terms of the markets and products covered. We have published a number of briefings on this development, both specifically relating to issuers of debt securities and more generally.

Link to briefing: *The Market Abuse Regulation for Issuers of Debt Securities*

Other

In addition to our financial services publications, McCann FitzGerald publishes briefings across the full range of its service offering, many of which may be of interest to financial service providers. This section highlights a selection of recent briefings addressing a diverse range of topics, including Brexit, bribery, corporate governance, data protection, employment law, European Account Perservation Orders, lobbying and whistleblowing.

Link to briefing: *Guarding the Guardians - Audit Reform and its Implications for Directors and Companies*

Link to briefing: *Irish Bribery Law: Change is Coming*

Link to briefing: *Company Secretarial and Compliance Services*

Link to briefing: *New Cyber Security Laws*

Link to briefing: *Updates on the Lobbying Act*

Link to briefing: *Central Bank Publishes its Latest Whistleblowing Report*

Link to briefing: *Could your Business be the Next 'Emailgate'*

Link to briefing: *"Up to the Minute": Record-Keeping in Board and Company Meetings*

Link to briefing: *Employment Law in Ireland*

Link to briefing: *General Data Protection Regulation Brochure*

Link to briefing: *New DPC Guidance on Anonymisation and Pseudonymisation*

Link to briefing: *Privacy Shield - A New and Improved Safe Harbor*

Link to briefing: *Evidential and Legal Professional Privilege Issues when Drafting Board Minutes*

Link to briefing: *Breyer Broadens 'Personal Data'*

Link to briefing: *Brexit Tracker II - Keeping you informed*

Link to briefing: *New European 'Freezers' will Provide a Fast and Effective Tool in Preserving Funds in Cross-Border Cases from January 2017*

Link to briefing: *Guarantees – Robust or Bust?*

Link to briefing: *Bankers Beware as European Freezing Orders Edge Ever Closer*

Financial Services Regulatory Group Bulletin

IN THIS ISSUE:

Central Bank Guidance on IT and Cyber Security Risks

In September 2016 the Central Bank of Ireland ("**Central Bank**") issued Cross-Industry Guidance in respect of IT and Cyber Security Risks ("**Guidance**") which sets out its current thinking as to good practices that regulated firms should use to develop effective IT and cyber security governance and risk management frameworks. Regulated entities will need to take on board this recent guidance and incorporate it into their governance and risk management frameworks as the Central Bank intends to use it to inform its future supervisory decisions.

In particular, regulated entities should take into account the Central Bank's concerns and criticisms regarding many firms' current contractual arrangements with their outsourcing service providers and ensure that these arrangements are adapted to reflect the Guidance.

The Central Bank and IT and Cyber Security Risks

The Central Bank's concerns around cyber security risks have been well signalled. During the course of 2015 it carried out a thematic inspection in relation to cyber security/ operational risk. Later, in September 2015, it communicated the results of its inspections, in the form of a "Dear CEO Letter", to the boards and senior management of investment firms, funds, fund service providers and stock-brokers. In that letter, the Central Bank outlined examples of best practice in dealing with cyber security risk as well as a self-assessment questionnaire for firms regarding their cyber security capabilities. In July 2015, the Central Bank also published a "Dear CEO Letter" in which it emphasised to investment fund boards the need for delegate oversight and the importance of specific reporting by delegates at board meetings on the policies and procedures in place to counter cyber attacks. See our related briefings here and here.

The Guidance - Key Takeaways

In its latest Guidance the Central Bank sets out its current thinking as to good practices that regulated firms should use to inform the development of effective IT and cyber security governance and risk management frameworks. It is based on Central Bank inspections, thematic reviews and ongoing supervisory engagement, which have highlighted a number of areas where IT and cyber security governance and risk management have fallen short of the expected standards. According to the Central Bank:

"[t]he nature and number of inadequate practices identified indicate a lack of prioritisation, awareness and understanding of IT and cyber security related risks and that more work is required at Board and Senior Management level to ensure that firms are effectively managing these risks."

The Guidance has four sections which deal with Governance, Risk Management, Cyber Security and Outsourcing. The Guidance does not address all aspects of the management of IT and cyber security risk but rather focuses on those areas that the Central Bank deems most pertinent at this time. The Guidance also acknowledges that the relevance and importance of the issues that it raises will vary according to the business model, size and technological complexity of the institution and the sensitivity and value of its information and data assets.

Governance

The Board of Directors and Senior Management are responsible for setting and overseeing the firm's business strategy and risk appetite and must ensure that IT risk is considered in this context. The Board and Senior Management must possess sufficient knowledge and understanding of the IT related risks facing the firm and take steps to ensure that these risks are well understood and properly managed throughout the firm. The Board must receive updates on key IT issues as well as regular reports on key IT risks.

IN THIS ISSUE:

Central Bank Guidance on IT and Cyber Security Risks (continued)

The Board approved IT strategy must be aligned with the overall business strategy and there must be sufficient resources to execute that strategy, including an adequate IT budget, staff levels and relevant expertise. Firms must have a sufficiently robust IT governance structure in place to facilitate effective oversight of the management of IT risks. They must also have documented IT policies and procedures addressing the identification, mitigation and reporting of the firm's IT related risks, as well as clearly defined roles and responsibilities including a senior role which is responsible for IT and cyber security matters.

Group driven IT strategies and governance documents must be appropriately tailored for the Irish firm from a regulatory and operational perspective. The governance structure must also provide for independent assurance on the effectiveness of the IT risk management, internal controls and governance processes within the firm.

Risk management

Firms must develop, implement, maintain and communicate an appropriate IT Risk Management Framework ("**ITRM**") which incorporates, as appropriate, relevant best practices and internationally adopted frameworks for IT risk management. They must establish and maintain a thorough inventory of IT assets, classified by business criticality, and put in place a Business Impact Analysis process to regularly assess the business criticality of IT assets. Firms must also develop and maintain an up-to-date IT risk register as well as adequate management processes and plans for IT incident detection, notification, and escalation. Critical or sensitive data must be correctly identified and adequately safeguarded. Firms must ensure that the effectiveness of IT controls is subject to periodic independent review and that penetration testing is carried out if warranted.

A firm must be able to demonstrate that it has assessed the risks associated with the maintenance of older IT systems and must have a strategy in place for dealing with those systems where they support critical business operations. More broadly, firms must have formal IT change management processes in place. Major proposed changes to the IT infrastructure must be subject to a thorough prior risk and impact analysis.

The Central Bank also expects firms to dedicate sufficient resources to support IT disaster recovery and business continuity planning, test and execution. Firms must have a documented disaster recovery and business continuity plan in place as well as a strategy for backing up critical data.

A firm must notify the Central Bank when it becomes aware of an IT (or cyber security) incident that could have a significant and adverse effect on the firm's ability to provide adequate services to its customers, its reputation or financial condition.

Cyber security

Cyber risk must be managed within the context of overall IT risk management. Firms must have a well-considered and documented Board approved strategy to address cyber risks, as well as documented cyber security policies and procedures. Cyber risk assessments must be performed regularly and robust safeguards put in place to protect against cyber security events and incidents.

Firms must implement strong controls over access to their IT systems. They must also put in place processes and procedures to detect a breach in a timely manner and have a documented cyber security incident response plan as well as a documented recovery plan for the rapid resumption of critical services.

Outsourcing

Firms must have adequate governance and risk management processes in place to effectively address the risks associated with the outsourcing of IT services, including cloud services. There must be clear lines of responsibility for ongoing management, operational oversight, risk management and regular review of the firm's outsourcing service providers ("**OSPs**").

IN THIS ISSUE:

Central Bank Guidance on IT and Cyber Security Risks (continued)

Firms must conduct thorough due diligence on prospective OSPs. In addition, the contract between the firm and its selected OSP must include a documented service level agreement ("**SLA**") or its equivalent, which deals with, among other things; the nature, quality and scope of the service to be delivered; the roles and responsibilities of the contracting parties; the requirements for service levels, availability and reliability; and system and information/ data security, business continuity and disaster recovery.

Firms must also:

- develop and maintain an exit management strategy to reduce the risks of business disruption should key IT outsourced services be unexpectedly withdrawn by the OSP, or voluntarily terminated by the firm;
- monitor for the development of potential concentration risks and take appropriate action if the firm is, or is likely to become reliant on a small number of OSPs to provide critical IT services; and
- ensure that the outsourcing policy includes a provision that any outsourcing arrangements do not impede effective on or off-site supervision of the firm by the Central Bank; this must also be reflected in any specific contracts entered into by the firm.

Comment and Next Steps

IT risks present ongoing challenges for financial services firms, both because of the increasing importance of technological developments in the sector and the increasing sophistication of criminal attacks. The financial services sector is among the most heavily targeted sectors by cyber criminals and recent years have seen a number of different types of attacks including data breaches, ransom demands and distributed denial of service attacks. For example, in February 2016, cyber criminals gained access to the Swift Codes of the Bangladesh Central Bank and attempted to transfer $951 million from its accounts. While the cyber criminals ultimately "only" obtained $81 million this is still likely to have been one of the biggest (individual) bank robberies in history. A year previously, Europol and other investigative authorities uncovered the theft of up to $1 billion from financial institutions worldwide, over about a two year period.

Regulators, including the Central Bank, have taken note of these risks. According to the Central Bank, it intends to continue to intensify its supervisory oversight of IT and cyber security related risks over the coming years and the Guidance will inform its supervisory approach. Consequently, each financial services firm should consider the issues outlined in the Guidance when reviewing its existing IT related governance and risk management arrangements and use the Guidance to inform the future development of those arrangements.

More broadly, firms, including in particular the Board of Directors and senior management, will need to keep up-to-date with the ever changing nature of IT risks and their potential impact. Best practice in countering IT risks is also evolving and firms will need to ensure that they keep up-to-date as IT/cyber security best practice continues to develop.

In this respect firms should in particular take note of the EU's Network and Information Security Directive which will apply from 9 May 2018. The Directive is designed to boost the overall level of cyber security in the EU. It will bring about significant changes to cyber security laws and will impose cyber security obligations on 'operators of essential services', including financial market infrastructures, and digital service providers. See our related briefing here.

Firms updating their IT and cyber security in response to the Central Bank's recommendations may also wish to review their data protection policies and procedures in anticipation of the General Data Protection Regulation's entry into effect in 2018, as there is some overlap between the two.

IN THIS ISSUE:

Anti-Money Laundering Developments

While, undoubtedly, the most significant anti-money laundering related development over the past few months was the adoption of the European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2016, there have also been several other notable developments. These relate to both the Fourth Anti-Money Laundering Directive 2015/849 ("**MLD4**"), which was adopted on 20 May 2015 and the European Commission's proposal to amend the fourth money laundering directive ("**MLD5**"), which was published on 5 July 2016.

The Fourth Money Laundering Directive (MLD4)

MLD4 seeks to strengthen the EU's anti-money laundering framework and, in doing, so recasts and replaces the Third Money Laundering Directive ("**MLD3**") which sets out the existing rules for combatting money laundering ("**ML**") and terrorist financing ("**TF**") at EU level. MLD4 was prompted in part by the Financial Action Task Force's decision to revise the Forty Recommendations underlying MLD3 with the publication of revised recommendations in 2012.

There are a number of differences between MLD3 and MLD4, the two most significant of which are: 1) the increased emphasis MLD4 places on the "risk-based approach" to ML/TF; and 2) the approach taken to the issue of beneficial ownership, including the MLD4 requirement to set up a central register of beneficial owners. MLD4 also differs from MLD3 as regards its scope; customer due diligence ("**CDD**") requirements; the approach taken to electronic money; the treatment of politically exposed persons; third party equivalence; and record keeping, as well as a variety of other matters. See our related briefings here and here.

High-risk countries

On 20 September 2016 Commission Delegated Regulation 2016/1675 supplementing Directive 2015/849 by identifying high-risk countries with strategic deficiencies, was published in the EU's Official Journal: it entered into force three days later. Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, Lao PDR, Syria, Uganda, Vanuatu, Yemen, Iran and the Democratic People's Republic of Korea are each listed as third-country jurisdictions which have strategic deficiencies in their anti-money laundering and counter-terrorist financing regimes that pose significant threats to the EU's financial system.

The purpose of the list is to protect the proper functioning of the EU's financial system from the ML/TF risks emanating from those countries. Obliged entities will be expected to apply enhanced CDD in case of financial flows to/from the high risk third countries identified in the Delegated Regulation.

On 24 November 2016 the Commission adopted a Commission Delegated Regulation amending Commission Delegated Regulation (EU) 2016/1675, by removing Guyana from the list of high-risk third countries under MLD4.

National Transposition

Member states must transpose MLD4 into national law by June 2017. In January 2016, the Department of Finance published a public consultation on member state discretions under MLD4 and the Funds Transfer Regulation 2015/847.

IN THIS ISSUE:

Anti-Money Laundering Developments (continued)

On 15 November 2016 the MLD4 requirement for corporates to establish a beneficial ownership register was implemented in Irish law through the European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2016. Broadly, these Regulations require entities incorporated in Ireland to keep and maintain a register of beneficial ownership. For further information see our briefing here.

National Risk Assessment

The Department of Finance together with the Department of Justice published, in September 2016, a national risk assessment ("**NRA**") for Ireland which seeks to identify, understand and assess the ML/TF risks faced by Ireland. This NRA was prepared as part of the preparations for the next mutual evaluation report on Ireland which is currently being prepared by the Financial Action Task Force. However, it also feeds into MLD4 which imposes obligations on member states, as well as the Commission and the ESAs, to contribute to an ongoing analysis of ML/TF risks at business, country and EU levels.

The purpose of the NRA is to provide a broad assessment of Ireland's ML/TF risks, to enhance the understanding of them and to develop effective strategies to address them. It is intended to assist the State, its law enforcement authorities, competent authorities, and the public to better understand Ireland's ML/TF risks, so that they can allocate resources and prioritise activities in a proportionate and risk-based manner. In so far as the financial services sector is concerned, the risk ratings are as follows:

- **High Risk** - Retail Banking, Money Remittance Firms and Bureau de Change;
- **Medium High Risk** - Non-retail Banking, Funds/Funds Administrators and Investment Firms (other than Asset Managers);
- **Medium Low Risk** - Payment Institutions (other than Money Remittance Firms), Life Assurance, Asset Managers, Credit Unions and Moneylenders: and
- **Low Risk** - Trust and Company Service Providers that are subsidiaries of credit or financial institutions.

The Commission is due to publish shortly a supra-national risk assessment of the risk of ML/TF across the EU.

In July 2016 the Basel Institute on Governance released its 2016 Basel Anti-Money Laundering (AML) Index, which is an annual ranking assessing 149 countries regarding ML/TF risks. Ireland is ranked 131 on that list, and is considered to be lower risk than other EU financial centres, including the United Kingdom (ranked 121), Netherlands (ranked 107) and Luxembourg (ranked 70).

The Fifth Money Laundering Directive (MLD5)

The Commission published MLD5 on 5 July 2016, in response to terror attacks in Europe and the leak of the Panama papers. MLD5 provides for a number of targeted amendments to MLD4 with the goal of countering the financing of terrorism and increasing the transparency of financial transactions and corporate entities. The principal amendments affect virtual currency exchange platforms/custodian wallet providers, prepaid instruments; the powers of financial intelligence units ("**FIUs**"); high-risk third countries; and access to beneficial ownership.

Virtual Currency Exchange Platforms/ Custodian Wallet Providers

MLD5 expands the list of 'obliged entities' set down in Article 2 of MLD4 to include; 1) virtual currency exchange platforms engaged primarily in exchange services between 'virtual currencies' and real currencies (or so called 'fiat currencies')

IN THIS ISSUE:

Anti-Money Laundering Developments (continued)

such as the Euro; and 2) wallet providers offering custodial services of credentials necessary to access virtual currencies. This would require such entities to have in place policies and procedures to detect, prevent and report ML/TF.

MLD5 defines the term "virtual currency". It also requires member states to ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers are licensed or registered and subjects those that own, or hold a management function in, these entities to fit and proper testing.

Pre-Paid Instruments

MLD4 permits any member state to allow obliged entities not to apply CDD measures with respect to electronic money, under certain conditions, including that:

- the card must not be reloadable; or
- the card has a maximum monthly payment transaction limit of €250 and can be used only in the member state where it is issued; or
- the maximum amount that can be stored on the card does not exceed €250.

MLD5 proposes lowering the above thresholds to €150.

MLD4 also provides that CDD need not be performed on a card holder trying to redeem or withdraw funds from a card providing that the amount is below €100. MLD5 reduces this amount to €50 and will require that CDD measures be undertaken where a card is used to make an online payment above this amount. Moreover, it will only be possible to use an anonymous prepaid card issued outside the EU where it can be considered to comply with requirements equivalent to those set out in EU legislation.

Financial Intelligence Units

MLD5 seeks to facilitate the ability of FIUs to access information in two ways. First, it requires member states to put in place centralised automated mechanisms or central electronic data retrieval systems, which would allow the identification, in a timely manner, of any natural or legal persons holding or controlling payment accounts and bank accounts held by a credit institution within their territory. Such a central register would be open to access by the FIUs and other competent authorities.

Secondly, it amends MLD4 to enable an FIU to obtain access to information from obliged entities, even without the individual obliged entity making a prior suspicious transaction report.

High-risk Third Countries

Under MLD4 an obliged entity must apply enhanced CDD measures when dealing with natural or legal entities established in high risk third countries. However, MLD4 does not set out a specific list of such measures. MLD5 contains a list of enhanced CDD measures which are to be considered as a minimum set of requirements applicable in all member states. It also sets out a list of additional mitigating measures that member states may require obliged entities to apply.

Beneficial Ownership Information

MLD4 sets out rules on the collection, storing and access to information on the ultimate beneficial owner(s) of companies, trusts and other types of legal arrangements. MLD5 strengthens and clarifies some of these provisions as well as expanding the scope of access to this information. In particular MLD5 provides for public access to certain beneficial ownership information held in registries regarding companies and trusts that engage in economic activities with a view to profit, by amending the First Company Law Directive 2009/101.

Financial Services Regulatory Group Bulletin

IN THIS ISSUE:

Anti-Money Laundering Developments (continued)

Comment and Next Steps

Both domestically and internationally, money laundering is an area of intense focus at the moment, fuelled in part by increasing concerns about terrorism and tax evasion. Entities subject to anti-money laundering requirements will welcome the NRA, which provides useful insight into current ML/ TF risks in Ireland and which should be used to inform ML/TF policies and procedures.

While MLD5 focuses on targeted changes to MLD4, a number of these changes are likely to have considerable implications including increased costs. The Commission has called for the MLD5 amendments to come into force at the same time as the rest of MLD4.

While initially the Commission had proposed that both MLD4 and MLD5 would need to be transposed into national law by January 2017, the transposition date for MLD5 (and MLD4) is likely to be June 2017, at the earliest.

In its Opinion on MLD5, published on 11 August 2016, the European Banking Authority queried the practicality of the Commission's proposed time frame. In this respect it observed that most member states are still consulting on changes to their national legal and regulatory frameworks necessitated by MLD4. Adding additional changes at this stage would risk exacerbating the already considerable legal uncertainty for both national authorities and obliged entities and create significant resource pressure. Virtual Currency Exchange Platforms and Custodian Wallet Providers would also have a very short time frame in which to implement AML policies and procedures.

Financial Services Regulatory Group Bulletin

IN THIS ISSUE:

New Requirements for Payment Service Providers

Recently adopted regulations place new obligations on banks and other payment service providers which are aimed at promoting transparency/fee comparability and facilitating account switching. They also require credit institutions to ensure that basic bank accounts are available to vulnerable EU residents.

The European Union (Payment Accounts) Regulations 2016 ("**Payment Accounts Regulations**") transpose into Irish law Directive 2014/92 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (the "**Payment Accounts Directive**" or "**PAD**").

Scope

The Payment Accounts Regulations apply to certain payment accounts held by a "consumer", namely a person acting for purposes outside his or her trade, business, craft or profession. Consequently, they do not cover accounts held by corporate entities, including small and medium enterprises.

To be in-scope, a consumer payment account must be used primarily for the execution of day-to-day payments transactions and the consumer must at least be able to place funds and withdraw cash from the payment account as well as execute and receive payment transactions, including credit transfers to and from a third party. Accounts with more limited functions do not fall within the scope of the Payment Accounts Regulations.

The provisions on transparency/fee comparability and account switching apply to payment service providers ("**PSPs**"), including, for example, banks, e-money institutions and firms listed on the Central Bank's Register of Payment Institutions. However, credit unions, friendly societies, An Post and the Central Bank are not in-scope.

The provisions on payment accounts with basic features apply to a 'relevant credit institution', namely an undertaking (other than a credit union):

- the business of which is to take deposits or other repayable funds from the public and grant credits for its own account, and
- that offers payment accounts to consumers in Ireland.

Transparency and Fee Comparability

One of PAD's key purposes is to ensure that consumers can understand fees so that they are able to compare offers from different PSPs and make informed decisions as to which payment account is most suitable for their needs. In order to facilitate fee comparisons, PAD provides for the standardisation of terminology at EU level for the terms and definitions of the most representative payment account-related services. Each member state must then define its own list of the most representative services based on that standardised terminology. PAD also provides for the creation of templates for the presentation of certain fee information which PSPs must provide to consumers, namely, (a) the fee information document ("**FID**") and glossary, and (b) the statement of all fees ("**SoF**").

Under the Payment Accounts Regulations, PSPs must provide the consumer with a FID and a glossary in good time before entering a framework payment account contract with that consumer. The FID must list the most representative services linked to a payment account at national level and state the corresponding fees for all those services offered by the PSP. The glossary must provide clear, non-technical and unambiguous explanations for at least the EU standardised terminology used in the payment account services list and related definitions.

PSPs must provide the consumer with a SoF, at least annually, containing information on the fees and interest paid by the consumer on the account, as well as any interest earned in the previous

IN THIS ISSUE:

New Requirements for Payment Service Providers (continued)

year. Its purpose is to enable a consumer to understand what fee expenditure relates to and to assess the need to either modify consumption patterns or change PSPs. Like the FID, the SoF must use the EU standardised terminology. PSPs must also use this terminology in other contractual, commercial and marketing information.

The Competition and Consumer Protection Commission ("**CCPC**") must operate a website that compares PSPs' fees for at least the services included in the payment account services list. Each PSP must inform the CCPC of its relevant fees and notify the CCPC at least five working days before making any changes to those fees.

The provisions in the Payment Accounts Regulations on fee comparability will not enter into force until nine months after the entry into force of the delegated act containing the technical standards setting out the standardised terminology for services linked to a payment account and the standardised format and common symbol of both the FID and the SoF. The EBA is currently consulting on the draft technical standards and this consultation will close on 21 December 2016.

Account Switching

PAD seeks to promote account switching by establishing a quick, simple and safe procedure both when a consumer wishes to switch from one PSP to another and when he or she wishes to switch between different payment accounts within the same PSP.

The Payment Accounts Regulations require PSPs to comply with the Central Bank of Ireland's Code of Conduct on the Switching of Payment Accounts with Payment Service Providers 2016 (the "**Code**") and to facilitate consumers who wish to close a payment account and open a payment account with a PSP located in another member state.

The Code replaces the Central Bank's 2010 Code of Conduct on the Switching of Current Accounts, which covered some but not all of the requirements set out in the Payment Accounts Regulations and which only applied to credit institutions. For its part, the Code, which came into effect on 21 September 2016, applies to all PSPs when providing payment accounts to consumers in Ireland. Among other things, once the consumer contacts the PSP to which he or she intends to switch his or her payments and provides consent to the switch, the relevant PSP is responsible for:

- contacting the transferring (previous) PSP and asking it to transfer data and cancel standing orders; and
- setting up new standing orders and accepting direct debits.

The Code also requires each PSP to have a payment account switching pack available in each branch and on its website containing information specified in the Code, including on the switching process. The Payment Accounts Regulations specify that consumers must be told of the roles of the transferring and receiving PSPs for each step of the switching process, the time-frame for completion, the fees (if any), any information the consumer will be asked to provide and details of alternative dispute resolution procedures.

Fees charged in connection with a switching service must be reasonable and reflect the actual cost to the PSP of providing the service.

Access to Payment Accounts

In line with PAD, the Payment Accounts Regulations prohibit a "relevant credit institution" from discriminating against a consumer who is an EU resident including by reason of his or her nationality or place of residence when he or she applies for or

IN THIS ISSUE:

New Requirements for Payment Service Providers (continued)

accesses a payment account. In addition, it requires that all consumers who are legally resident in the EU must be able to access a payment account with basic features free of charge or for a reasonable fee. The conditions applicable to holding a payment account with basic features must not be discriminatory.

A relevant credit institution may refuse an application for access to a payment account with basic features where the consumer already holds a payment account with a relevant credit institution save where a consumer declares that he or she has received notice that the payment account will be closed. It may also refuse an application to avoid infringing the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010. A relevant credit institution must either refuse an application or open an account without due delay and at the latest within 10 business days after receiving a complete application.

A payment account with basic features must enable the consumer to avail of the following services: opening, operating and closing accounts, placing funds, cash withdrawals at the counter or by ATM, direct debits, payment transactions through a payment card and credit transfers. However, a relevant credit institution need only offer these services to the extent that it already offers them to consumers holding other payment accounts.

The relevant credit institution must offer a payment account with basic features free of charge for the first 12 months at least. Thereafter, it may impose a reasonable fee, subject to compliance with certain conditions.

Comment

The Payment Accounts Regulations impose a number of new obligations on PSPs. The requirements relating to switching and access to payment accounts already apply. Once the delegated act on standardised terminology and standard form documents has entered into force, PSPs will have nine months in which to:

- produce two new account documents, namely a FID and a glossary, using the prescribed standardised terminology;
- review and re-format existing fee statements to ensure they employ the standardised terminology, comply with the new standard format and include all the information required under the Payment Account Regulations; and
- update documents, websites and other marketing tools to reflect the new standardised terminology.

Each PSP will also need to inform the CCPC of the fees that it charges for services included in the payment account services list and notify the CCPC in advance of any changes to those fees.

IN THIS ISSUE:

Identifying the Irish Consumer - Recent Case-law

Consumers have a special status in financial services law and are afforded additional protections under a number of legislative provisions that are not available to other borrowers. This can mean that identifying whether or not someone is acting as a consumer is crucially important and correspondingly, highly controversial. Over the past few years the courts have been called upon to consider the circumstances in which a borrower will be acting as a consumer on numerous occasions. Most recently, in the context of summary High Court proceedings in *Stapleford Finance Ltd v Lavelle* [2016] IEHC 385, Baker J again considered this issue. Her summary judgment in that case further develops the case law on the definition of a consumer in a number of respects without, however, adding much by way of additional clarity.

The Facts

Mr Lavelle amassed considerable wealth while working as a City of London Trader. On his return to Ireland in 2005 he sought to diversify his savings and to put in place pension type investments to secure his, and his family's, future. Consequently, he sought advice from Anglo Wealth Management which introduced him to Quinlan Private, a private investment fund, through which Mr Lavelle invested in a number of commercial transactions. For tax reasons, Mr Lavelle funded many of his investments through borrowings from Anglo Irish Bank ("**Anglo**"), drawing down seven loans in total. When Mr Lavelle subsequently failed to repay these loans, Irish Bank Resolution Corporation Limited ("**IBRC**"), which had taken over the loans from Anglo, sought summary judgment against him in the sum of close to €6 million. During the course of the summary judgment proceedings, Stapleford Finance Ltd successfully applied to be substituted as the plaintiff in lieu of IBRC.

Mr Lavelle did not dispute that he had drawn down the loans, but claimed that he should be able to defend the proceedings against him, partially on the grounds that he had an arguable case that he was acting as a consumer for the purpose of each of the loans and that the mandatory statutory requirements had not been met.

In considering whether or not to grant Mr Lavelle liberty to defend the proceedings, Baker J addressed a number of issues, including, a) the significance of the parties' description of the borrower; b) the relevance of the scale of the borrowing, c) whether a loan for investment purposes can be a consumer loan; and d) whether or not there is a presumption that a natural person is acting as a consumer.

The Parties' Description of the Agreement

The loans to Mr Lavelle were based on five facility letters, the first two of which were made by documentation in a form suitable for use as a credit agreement regulated by the Consumer Credit Act 1995 ("**CCA**"). In conjunction with the other three facility letters, Mr Lavelle executed a certificate that he was not acting as a consumer for the purposes of the CCA, the European Communities (Unfair Terms in Consumer Contracts) Regulations 1995, and that as the facility was being advanced for the purpose of his trade, business or profession, he was not a consumer within the meaning of the CCA or the Regulations.

In the context of the summary proceedings, Mr Lavelle argued that Anglo had treated him as a consumer for the purposes of the first two loans, nothing

IN THIS ISSUE:

Identifying the Irish Consumer - Recent Case-law (continued)

had changed in his personal circumstances between the first two loans and the later loans, and all of the loans were taken out by him for the same general purpose, namely to make pension or long term investments to secure his family's future.

In her judgment Baker J observed that it is uncontroversial that the question of whether a person is a consumer is a matter to be determined objectively and irrespective of the characterisation that the parties might have applied to the loan. She also accepted Stapleford Finance's argument that the fact that Anglo proceeded as if the loans were regulated under the CCA did not itself comprise an acknowledgement by Anglo that Mr Lavelle was a consumer and "that the Bank did no more than conduct its business so as to ensure that it did not fall foul of the legislation."

However, Baker J ultimately decided that the characterisation of the loans could not be resolved at summary hearing on the basis of two letters, sent by IBRC and its solicitors respectively, which she thought "might amount to an acknowledgment by IBRC that Mr Lavelle was a consumer for the purpose of the first two loans". Accordingly, Baker J held that Mr Lavelle had succeeded in raising an arguable defence that he could have been a consumer for at least the first two loans, and that Anglo had no reason to treat him differently for the purposes of the other facilities.

The Scale of the Borrowing

A number of recent judgments have appeared to suggest that in the case of borrowing for personal investment purposes in the context of a commercial transaction, the scale of the borrowing is a relevant factor in determining the character of the transaction. In particular, in *Ulster Bank Ireland Ltd v Healy* [2014] IEHC 96, Barrett J considered that an individual who had borrowed €600,000 for the stated purpose of investing in UK properties as pension type investments, was not necessarily acting as a professional investor or property investor. He went on to say:

"Of course there must come a point when a person crosses the Rubicon from consumer to professional. However, it could be contended that a man such as Mr Healy who has invested not insignificant but not extravagant sums in property in order to provide for his retirement and to benefit his family has not necessarily crossed this line."

In *Stapleford v Lavelle*, Baker J explicitly rejected the size of a loan as a factor to be taken into consideration when determining whether or not a borrower is acting as a consumer, observing that Barrett J's above comment was made on an obiter basis, did not find support in the authorities and was not binding on her. Baker J emphasised that a loan's defining or identifying characteristic is its purpose and not its amount, and stated that "it is perfectly possible for a person to borrow a very substantial amount of money for the purposes of acquiring a private residence or a holiday home for personal use and in that circumstance, such a person would be readily identified as a consumer".

Loans for Investment Purposes

It is well-established that a borrower acting in the course of an ancillary trade, profession or employment will not be acting outside his or her trade, profession or employment. In other words, a borrower can have more than one trade, profession or employment. For example, in *AIB v Higgins* [2010] IEHC 219, Kelly J had no difficulty in holding that the defendants who had entered into a partnership arrangement with a view to acquiring and developing lands were not acting as consumers despite the fact that none of them were professionally involved in the business of property development and each was engaged in other activities on a fulltime basis.

IN THIS ISSUE:

Identifying the Irish Consumer - Recent Case-law (continued)

However, in the context of investment loans, the courts, including Barrett J in *Ulster Bank Ltd v Healy*, have been prepared to recognise that the mere fact that a person borrows money in order to make an investment in property does not necessarily mean that that person is carrying out the trade or profession of property investment. In *Stapleford v Lavelle*, Baker J followed this case-law holding that the question of whether or not a person who borrows money to make a personal investment can be a consumer is one that "*may not readily be determined on a summary hearing*".

In reaching this conclusion, Baker J also rejected the plaintiff's argument that the concept of a consumer is one which should be strictly construed. The plaintiff's argument was based on the approach taken by the Court of Justice of the European Union ("**CJEU**") in Case C-269/95 *Benincasa v Dentalkit* [1997] ECR I-3763 and Case C-464/01 *Gruber v Bay* [2005] ECR I-439. Both of these cases concerned the Brussels Convention of 1968 on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters which allows certain derogations from the general rule on jurisdiction in the case of consumers. The CJEU's judgments in those cases were partially based on the fact that a provision which derogates from a general rule should be interpreted strictly. However, according to Baker J, it is not readily apparent that the definition of a consumer for the purposes of national consumer protection legislation should also be viewed as a derogation from any general rule. Rather, it is an attempt by EU and domestic law to offer special protection to a person who might have a deficit of bargaining power. In this respect, Baker J's judgment echos remarks made by the Advocate General in Case C-110/14 *Costea* [2015] ECR I-271.

Burden of Proof

Finally, Baker J addressed the issue of whether there is a presumption that a natural person is acting as a consumer. In an earlier case, *ACC Loan Management Ltd v Browne* [2015] IEHC 722 Baker J had stated that she considered "that the legislation is such that a person is a consumer unless it can be shown that the person is acting inside the person's business". However, in *KBC Bank Ireland Plc v Osborne* [2015] IEHC 795, Barrett J expressly refused to agree with this statement. In *Stapleford Finance Ltd v Lavelle*, Baker J referred to her "infelicitous statement" in *Browne* and acknowledged that it was "not borne out by the authorities and is not correct as a matter of law."

Comment

Stapleford Finance Ltd v Lavelle further develops the case law regarding the definition of a consumer in a number of ways. However, in some respects it raises more questions regarding this definition than it answers, particularly regarding loans for personal investments in commercial transactions. Hopefully each of the issues addressed by Baker J in her summary judgment will be the subject of full consideration by the courts in the near future.

Financial Services Regulatory Group

Josh Hogan
Partner, Head of Financial Services Regulatory Group

DDI
+353-1-607 1720

EMAIL
josh.hogan@
mccannfitzgerald.com

Fergus Gillen
Partner, Head of Finance Group

DDI
+353-1-611 9146

EMAIL
fergus.gillen@
mccannfitzgerald.com

Adrian Farrell
Partner, Finance

DDI
+353-1-607 1312

EMAIL
adrian.farrell@
mccannfitzgerald.com

Ambrose Loughlin
Partner, Finance

DDI
+353-1-607 1253

EMAIL
ambrose.loughlin@
mccannfitzgerald.com

Judith Lawless
Partner, Finance

DDI
+353-1-607 1256

EMAIL
judith.lawless@
mccannfitzgerald.com

Darragh Murphy
Partner, Finance

DDI
+353-1-607 1433

EMAIL
darragh.murphy@
mccannfitzgerald.com

Peter Osborne
Consultant, Finance, Corporate

DDI
+353-1-611 9159

EMAIL
peter.osborne@
mccannfitzgerald.com

Roy Parker
Partner, Finance

DDI
+353-1-607 1249

EMAIL
roy.parker@
mccannfitzgerald.com

Brian Quigley
Partner, Dispute Resolution & Litigation

DDI
+353-1-607 1471

EMAIL
brian.quigley@
mccannfitzgerald.com

McCann FitzGerald

Principal Office
Riverside One
Sir John Rogerson's Quay
Dublin 2
D02 X576

Tel: +353-1-829 0000

London
Tower 42
Level 38C
25 Old Broad Street
London EC2N 1HQ

Tel: +44-20-7621 1000

New York
Tower 45
120 West 45th Street
19th Floor
New York, NY 10036

Tel: +1-646-952 6001

Brussels
40 Square de Meeûs
1000 Brussels

Tel: +32-2-740 0370

Email

inquiries@mccannfitzgerald.com

www.mccannfitzgerald.com