WILLIAM FRY

Financial Regulation Unit Briefing

The Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018

On 14 November 2018, the President of Ireland signed the Criminal Justice (Money Laundering and Terrorist Financing) Act 2018 (the **2018 Act**) which fully transposes the Fourth Anti-Money Laundering Directive **(MLD4)** in Ireland. The Act will commence following a Ministerial Order anticipated to be made before the end of November 2018.

What is the current state of play?

In 2015 the EU adopted MLD4 repealing and replacing the Third Anti-Money Laundering Directive **(MLD3)**. MLD4 aims to rectify the weaknesses in MLD3 and to take account of evolving technologies and standards. A Fifth Anti-Money Laundering Directive **(MLD5)** entered into force on 9 July 2018. The deadline for its transposition by Member States for most provisions is 10 January 2020.

The 2018 Act transposes MLD4 by amending primarily the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (the 2010 Act). Article 30(1) of MLD4, which deals with the requirement for corporates to maintain a register of beneficial owners, has already been transposed via The European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2016. See our Beneficial Ownership of Corporates briefing here.

How does the current regime work?

Money Laundering Offences	Obligations	Compliance
Broadly, there are three types of criminal money laundering offences — to conceal, convert, or remove from the State, the proceeds of criminal conduct. An offence may be committed by the doing, or attempting to do, one of these acts. Since money laundering is a criminal offence, aiding, abetting, counselling or procuring one of these acts attracts secondary liability. Directors or other responsible persons may become liable for offences committed by a company if their consent, connivance or wilful neglect is proven.	Obligations are placed on 'designated persons' (rather than 'obliged entities' which is the term used in MLD4) to carry out a range of checks and internal procedures when dealing with customers or transactions. Such measures aim to identify and combat the occurrence of money laundering/terrorist financing related crimes. Such designated persons include credit and financial institutions, auditors, independent legal professionals, trust or company service providers, estate agents and providers of gambling services. A failure to adhere to these statutory compliance measures constitutes an offence under the 2010 Act.	Designated persons achieve statutory compliance with money laundering legislation by: (i) identifying the level of risk presented by interacting with a particular customer; (ii) executing customer due diligence (**CDD**) which involves know-your-customer checks that vary in severity depending on the level of risk associated with that customer or transaction; and (iii) continuing to monitor customers and transactions and making suspicious activity reports to the relevant competent authorities if necessary.

Key Amendments in the 2018 Act

DESIGNATED PERSONS AND BENEFICIAL OWNERS

1. Designated persons

Any person trading in goods that involve cash transactions of at least €10,000 is now included as a 'designated person', lowering the previous threshold from €15,000.

2. 'Beneficial ownership' – wider scope of persons

Bodies Corporate: under the former legislation, any individual who ultimately owned or controlled, either directly or indirectly, more than 25% of the shares or voting rights in the body corporate or otherwise exercised control over the management of the entity would have been considered a beneficial owner. The 2018 Act adopts the definition contained in MLD4 of a 'beneficial owner' and includes any natural person who ultimately owns or controls the relevant body through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity or through control via other means. A shareholding of 25% plus one share or an ownership interest of more than 25% held by a natural person will be an indication of direct ownership, whereas a shareholding of 25% plus one share or an ownership interest of more than 25% held by a corporate entity(ies) under the control of a natural person(s) will be an indication of indirect ownership. In summary, the 2018 Act removes the hard threshold of 25%, meaning that an individual with less than a 25% shareholding or ownership interest could be considered a beneficial owner of a body corporate.

Trusts: previously, a 'beneficial owner' included persons with at least a 25% interest in possession, remainder or reversion of the capital of the trust property. Under the 2018 Act, any individual who is entitled to a vested interest in the trust property may be considered a beneficial owner. Additionally, settlors, trustees and protectors of a trust may now also be considered beneficial owners.

Partnerships: previously, a 'beneficial owner' meant any individual who ultimately was entitled to or controlled, directly or indirectly, more than 25% of the share capital or profits of the partnership or more than 25% of the voting rights of the partnership, or who otherwise exercised control over the management of the partnership. The 2018 Act expands on this notion of control by stating instead that any individual who otherwise controls the partnership may be considered a beneficial owner. Thus, the requirement that the control be related to management functions is removed.

3. Designated Persons and Responding to Queries

All designated persons must be in a position to respond to queries from An Garda Síochána with respect to any business relationship that that person held within the previous five years. Under the former legislation, this requirement only applied to banks and financial institutions and the relevant time frame was six years.

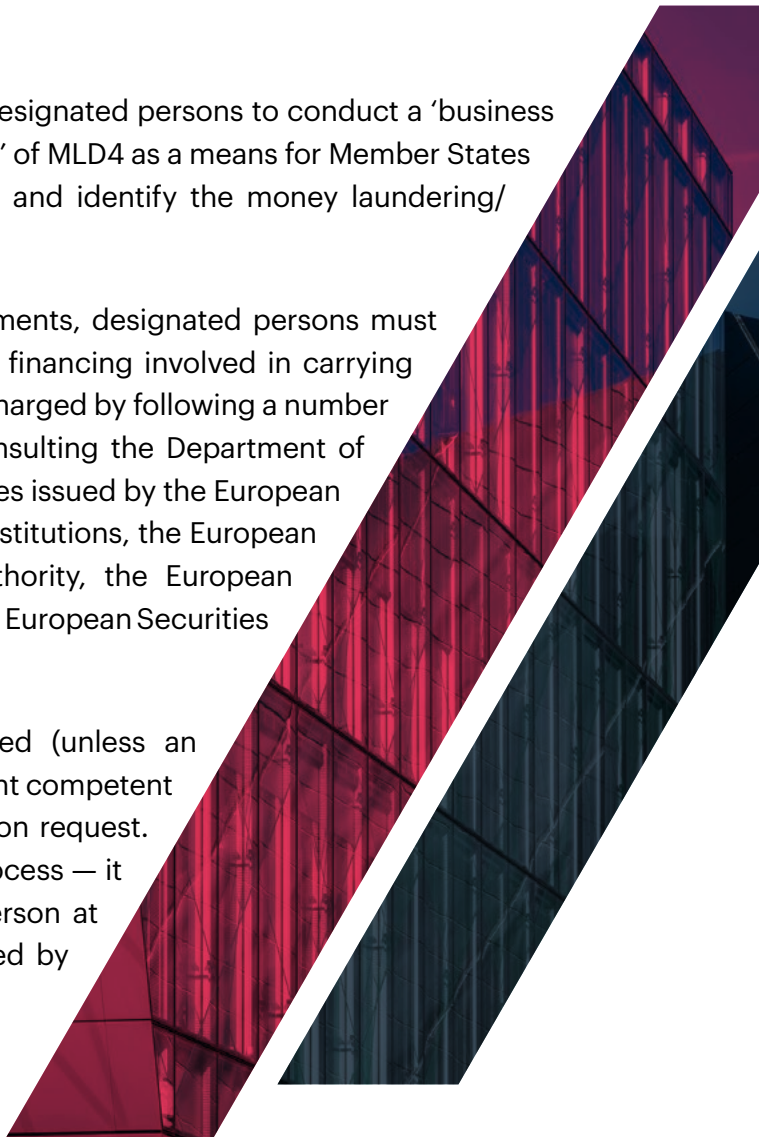
RISK AND DUE DILIGENCE

4. Introduction of Business Risk Assessment

The 2018 Act introduces a statutory requirement for designated persons to conduct a 'business risk assessment'. This reflects the 'risk-based approach' of MLD4 as a means for Member States and designated persons to more clearly understand and identify the money laundering/terrorist financing risks that affect them.

In addition to the usual know-your-customer requirements, designated persons must assess the level of risk of money laundering/terrorist financing involved in carrying out their own business activities. The obligation is discharged by following a number of procedures set out in the 2018 Act, including consulting the Department of Finance's National Risk Assessment and other guidelines issued by the European Central Bank, and in the case of credit and financial institutions, the European Supervisory Authorities (the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority (together **ESAs**)).

The business risk assessment must be documented (unless an exemption applies) and must be available to the relevant competent authority (depending on the industry in question) upon request. The business risk assessment must also be a living process — it must be reviewed and managed by a designated person at regular, pre-defined intervals and it must be approved by senior management.



The 2018 Act proposes to append schedules to the 2010 Act which contain non-exhaustive lists of factors suggesting lower or higher risk levels that might attach to particular customers or transactions. Additionally, the Minister for Justice and Equality may prescribe additional risk factors to be considered in a business risk assessment.

5. How the risk assessment affects CDD

The 2018 Act prescribes that in deciding the level of CDD to be applied when undertaking a transaction or entering a business relationship, the designated person must consider a number of factors, including: the relevant business risk assessment, the purpose of the account or relationship, the level of assets deposited or the size of the transaction, and any factor listed in the 2010 Act's schedules, as amended, indicative of higher or lower risk.

6. Timing of CDD and verification of agents

A designated person is obliged to carry out CDD prior to establishing a business relationship or carrying out a transaction or providing a service and must refrain from providing such services if the customer or counterparty to a business relationship cannot provide the required information. The 2018 Act adds that CDD must be executed at any time, including a situation where the relevant circumstances of a customer have changed, where the risk of money laundering/terrorist financing warrants its application.

There is an exception to the timing requirements of CDD which allows credit institutions to open an account for a customer in advance of completing CDD, as long as the account is not being opened by an agent of the customer or beneficial owner. Under the 2018 Act, this exemption is extended to financial institutions opening an account for a customer, including an account facilitating transactions in transferable securities.

The 2018 Act adds that when applying CDD measures, a designated person must verify that any person purporting to act on behalf of a customer is so authorised.

7. Simplified CDD (**SCDD**) and Enhanced CDD (**ECDD**)

Under the former regime, SCDD could be applied to specified low-risk categories of customers or business relationships. In line with the risk-based approach under MLD4, these rigid category-based exemptions have been removed by the 2018 Act. Instead, decisions by designated persons on when to apply SCDD must be justified on a case-by-case basis informed by, inter alia, the relevant 'business risk assessment'.

The designated person must, upon request from the relevant competent authority, document its justification for adopting SCDD and make such documentation available upon request. Sources that must be consulted include: the appended schedules to the 2010 Act indicating potential risk factors; the National Risk Assessment; and in the case of credit and financial institutions, guidelines issued by the relevant ESAs.

ECDD works in much the same way and must be applied when the perceived risk level is heightened. Such instances include transactions that involve high-risk third countries or unusually complex and large transactions.

8. ECDD and politically exposed persons (**PEPs**)

The ECDD procedures that apply to PEPs, and their immediate family members and close associates, previously only applied to PEPs residing outside the State. This scope is extended by the 2018 Act to persons residing inside the State and shall include any beneficiary of a life assurance or other investment-related policy and members of the governing body of a political party.

MONITORING AND REPORTING

9. Reliance on third parties to carry out CDD

The 2018 Act extends the ability for designated persons to rely on third parties to carry out CDD on their behalf to those located outside the EU, provided that the third party is a branch or a majority-owned subsidiary of an EU designated person. Additional conditions must be met, and the outsourcing party retains ultimate responsibility for meeting CDD requirements. Designated persons must also ensure that they have possession of copies of the required documentation and verification data.

10. Monitoring

The 2018 Act introduces a definition of 'monitoring' and requires that designated persons monitor any business relationship that it has with a customer to the extent reasonably warranted by the risk of money laundering or terrorist financing. If a designated person applies SCDD, it must carry out sufficient monitoring of the transaction or business relationship to enable the designated person to detect any unusual or suspicious transactions.

Under the 2018 Act, a designated person must apply enhanced monitoring of a business relationship when dealing with a customer established or residing in a high-risk third country. The 2018 Act additionally requires that a designated person examine any complex or unusually large transaction and increase the degree and nature of monitoring of a business relationship or transaction accordingly.

INTERNAL POLICIES AND PROCEDURES

11. Internal compliance

The 2018 Act substitutes section 54 of the 2010 Act with a significantly more prescriptive version mandating the types of policies and procedures that designated persons must have in place to prevent and detect money laundering/terrorist financing. Of note is the requirement that additional measures be taken to counter risks that may arise from the use of new products of practices arising from technological developments.

Additionally, policies and procedures must be kept under review to retain their currency and must be approved by senior management.

12. Group-wide policies and procedures

Groups of companies are required to unify their anti-money laundering/terrorist financing policies, and where this is not possible owing to local laws, to take additional measures to counter commensurate risks.

FINANCIAL INSTITUTIONS

13. Expanded scope

The definition of 'financial institutions' is updated to harmonise it with current EU regulations. The conditional requirements that banks must satisfy in advance of commencing 'correspondent relationships' with banks outside the EU, as well as the prohibition on entering relationships with shell banks, is extended to financial institutions. Designated persons, including financial institutions, which are not otherwise authorised, licensed or registered with the Central Bank of Ireland are required to do so to enable the Central Bank of Ireland to fulfil its supervisory role for money laundering purposes.

PREPAID CARDS

Designated persons are exempt from carrying out CDD requirements with respect to certain electronic money products (ie certain prepaid cards). Prepaid cards that are not reloadable, cannot be used outside the State and have a maximum monthly transaction limit of €250 are exempt. Prepaid cards that are reloadable and that carry a maximum store of value of €250 are exempt, as are reloadable cards that carry a maximum store of value of €500 if they cannot be used outside the State.

OTHER NOTEWORTHY AMENDMENTS

- The Financial Intelligence Unit (**FIU**) is granted additional powers with respect to requesting information from designated persons and accessing beneficial ownership registers.
- A member of An Garda Síochána, under certain conditions, may request that certain documents or records relating to a business relationship or a transaction be retained by a designated person for a maximum additional period of five years, beyond the required retention period of five years, notwithstanding the fact that a decision to institute proceedings against a person may not have been taken.
- Two additional defences to money laundering crimes are introduced: the broadening of the defence to 'tipping off' in circumstances where the disclosure was made by one member of a group of companies to another, with attendant conditions; and a defence of 'all reasonable steps' having been taken to avoid the commission of an offence.
- The 2018 Act provides for a 'Certificate of Fitness' regime for managers and beneficial owners of private members' clubs.

SANCTIONS

The 2018 Act introduces monetary penalties which are to apply where the Central Bank of Ireland invokes its administrative sanctions procedure contained in the Central Bank Act 1942 (as amended) in respect of money laundering/terrorist financing contraventions.

Where the designated person:

- is a body corporate, the penalty is the greater of either €10 million or twice the amount of the benefit derived from the contravention or 10% of the body corporate's turnover for the last financial year;
- is a natural person, the penalty is the greater of either €1 million or twice the amount of the benefit derived from the contravention;
- is a credit or financial institution, the penalty is the greater of either €5 million or twice the amount of any benefit derived from the contravention.

GUIDELINES

The Central Bank of Ireland has indicated that it will publish draft money laundering and terrorist financing guidelines in November 2018 to accompany the amended statutory regime. The draft Guidelines will be subject to a public consultation period of three months before they become final.

The Department of Finance and the Department of Justice co-authored the previous 2012 Guidelines which will be replaced. Neither of these Departments nor the Central Bank of Ireland proposes to publish renewed sector-specific guidelines. However, the Central Bank of Ireland has indicated that it will endorse Guidelines issued by the ESAs. Additionally, the Financial Action Task Force has recently published some sector-specific guidance.

On 8 November 2018, the Joint Committee of the ESAs launched a three-month public consultation on draft Guidelines on the cooperation and information exchange between competent authorities supervising credit and financial institutions for the purposes of anti-money laundering and counter-terrorist financing supervision. The Guidelines propose that 'AML/CTF colleges' be established where there are three or more competent authorities from different Member States involved in supervising the same entity. The purpose of an AML/CTF college is to provide a framework for cross-border supervision by Member States' competent authorities.

HOW CAN WILLIAM FRY HELP?

William Fry can assist designated persons in relation to:

- reviewing internal policies and procedures, and contracts, to ensure they comply with the updated legislation; reviewing and updating processes in carrying out CDD;
- providing training and advice with regards to anti-money laundering/counter-terrorist financing compliance; and
- AML/CTF inspections and regulatory enforcement action.

CONTACT OUR FINANCIAL REGULATION UNIT

For further information, please contact Shane Kelleher, Louise McNabola or any member of the William Fry Financial Regulation Unit.

Shane Kelleher
Partner,
Head of Financial Regulation Unit
+353 1 639 5148
shane.kelleher@williamfry.com

Lisa Carty
Partner,
Litigation & Dispute Resolution
+353 1 639 5386
lisa.carty@williamfry.com

Patricia Taylor
Partner, Asset Management &
Investment Funds
+353 1 639 5222
patricia.taylor@williamfry.com

Naoise Harnett
Partner,
Insurance & Reinsurance
+353 1 639 5259
naoise.harnett@williamfry.com

John Aherne
Partner, Asset Management &
Investment Funds
+353 1 639 5321
john.aherne@williamfry.com

Louise McNabola
Associate,
Banking & Finance
+353 1 639 5196
louise.mcnabola@williamfry.com