Seirbhís Leabharlainne 7 Taighde
Library & Research Service

Bill Digest

Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020

No. 23 of 2020

Hari Gupta, Senior Parliamentary Researcher, Law

21 September 2020

Abstract

The *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020* gives effect to provisions of the EU's Fifth Money Laundering Directive. The Bill proposes amendments to the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010* (as amended). These amendments aim to help prevent of the use of the financial system for the purposes of money laundering or terrorist financing by, among other things, outlining prescribed enhanced customer due diligence procedures, requiring more transparency of beneficial ownership, limiting the potential for anonymous financial transactions and providing more certainty to the definition of 'politically-exposed person'.

Tithe an Oireachtais
Houses of the Oireachtas

Contents

Bill published: 8 September 2020

Second stage debate: 22 September 2020

This L&RS Bill Digest may be cited as:

Houses of the Oireachtas Library & Research Service, 2020, *Bill Digest: Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020*

Legal Disclaimer

Glossary

AML/CFT	A widely used abbreviation for 'anti-money laundering/counter-terrorist financing'.
Beneficial Owner	A natural person who directly or indirectly owns or controls a corporate body, partnership or trust assets. Under EU Directives, beneficial ownership can be indicated through direct or indirect rights of ownership or by other means, such as control of the decisions of management or directors. Article 3(6) of the EU's Third Money Laundering Directive lists criteria including: • unlisted companies: direct or indirect ownership or control of more than 25% of shares or voting rights; • listed companies: ability to exercise control over the company's management; • partnerships: ability to exercise control of the partnership or direct or indirect ownerships or control of more than 25% of capital, profits or voting rights; • trusts: ability to exercise control of the trust or having a vested interest in at least 25% of its capital.
Business Risk Assessment	The legislation requires designated bodies to formally identify and assess the risks of money laundering and terrorist financing involved in carrying on the designated person's business activities, considering the following risk factors at a minimum: • the type of customer that the designated person has; • the products and services that the designated person provides; • the countries or geographical areas in which the designated person operates; • the type of transactions that the designated person carries out; • the delivery channels that the designated person uses; • other prescribed additional risk factors. When carrying out a business risk assessment the designated person must consider the national risk assessment and any guidance issued by the relevant competent authority. A credit institution or financial institution must also consider guidelines issued by the European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority. The business risk assessment must be reviewed and kept up to date.
Competent Authority	Equivalent to a 'self-regulatory body' in EU law.

	Competent authorities monitor designated persons and secure compliance with legislative requirements. They comprise: • the Central Bank of Ireland for credit institutions or financial institutions; • the designated accountancy bodies for auditors, external accountants or tax advisers; • the Law Society of Ireland for solicitors; • the General Council of the Bar of Ireland for barristers; • the Minister for Justice and Equality for any other designated person under the Act, administered by the Anti-Money Laundering Compliance Unit. Competent Authorities do not investigate allegations of money laundering or terrorist financing within the State; this is the responsibility of the Financial Intelligence Unit within An Garda Síochána.
Correspondent Banking	A system that allows banks to offer services to customers in places (such as foreign countries) where the bank does not have branches. The bank (A) opens a correspondent account in another bank (B) that has a branch in the place where A's customers wish to do business. A's customers can use the correspondent account in B to lodge and withdraw money as if they were dealing with A.
Customer Due Diligence (CDD)	Steps that a designated person must take to verify the identity and affairs of a customer and, in appropriate circumstances, the ownership, control structure and beneficial ownership of any undertaking (such as a company, partnership or trust) connected with the customer or the service that the designated person is providing. When completing customer due diligence, the designated person must have regard to at a minimum: • the relevant business risk assessment; • the national risk assessment; • guidance issued by the relevant competent authority; • the nature of the transaction or relationship; • the regularity of transactions or duration of the relationship; • the presence of any factor that may suggest that the transaction or customer potentially poses either a lower or higher risk of money laundering or terrorist financing; any additional prescribed risk variables.
Designated Person	Equivalent to an 'obliged entity' under EU law. A person or undertaking required under AML/CFT legislation to conduct CDD (and, where appropriate, Enhanced Customer Due Diligence (ECDD)) on customers and to file Suspicious Transaction Reports (STRs) in the case of suspected money laundering or terrorist financing activity. Under current legislation (prior to this Bill), these include: • banks, credit unions, insurers and financial intermediaries;

	• external accountants, auditors and tax advisers; • relevant legal professionals; • estate agents and property service providers; • trust companies; • casinos and private gambling clubs; • traders in goods sold for cash worth €10,000 or more. The Bill proposes to include virtual currency platforms and custodian wallet providers, providers of tax-related services, and, when dealing with transactions of a total value of €10,000 or more, people storing, trading or acting as intermediaries in the trade of art and property letting agents.
Enhanced Customer Due Diligence (ECDD)	More detailed verification procedures that a designated person must carry out when beginning a business relationship with or providing services to customers where that customer and product/service combination is considered to pose a greater risk of money laundering or terrorist financing. Under current AML/CFT rules, ECDD is required in relation to: • politically-exposed persons, including their immediate family and close associates; • correspondent banking relationships; any circumstances that give a designated person reasonable grounds to suspect a heightened risk of money laundering or terrorist financing
Fiat Currency	A government-issued currency that is not backed by a physical commodity, such as gold or silver, but rather by the government that issued it. Examples of fiat currencies include the Euro, Pound Sterling, Australian Dollar and the US Dollar.
Financial Action Task Force (FATF)	An inter-governmental organisation closely linked to the OECD that was set up to develop policies for combatting international financial crime and to monitor states' implementation of the policies.
Financial Intelligence Unit (FIU)	An authority designated by a state as its centre for collecting, analysing and distributing (both domestically and internationally) information concerning money laundering or terrorist financing activity. Ireland's FIU is the Garda National Economic Crime Bureau (formerly the Garda Bureau of Fraud Investigation).
Money Laundering	In broad terms, techniques used by criminals to disguise the proceeds of crime and infiltrate them into the legitimate financial system in ways that allow the funds to be used freely. Common techniques include • false accounting by 'front businesses' to make funds appear to have been generated legitimately; • using shell companies to buy property and investments;

	buying high-value goods or properties and selling them to innocent buyers.
Occasional Transaction	Transactions where a designated person might not have a pre-existing business relationship with the other party, but where CDD (and possibly ECDD) is still required. Under current legislation, these include: • payments of €2,000 or more in private gambling clubs; • electronic funds transfers of €1,000 or more; other transactions (individual or linked) for €15,000 or more.
Politically-Exposed Persons (PEP)	People whose influential positions require designated persons who deal with them, their families or business connections to conduct ECDD. Under current legislation, this applies only to PEPs resident outside the State. PEPs include: • heads of State, ministers and members of parliament or a similar legislative body; • a member of the governing body of a political party; • senior judges; • Central Bank board members and senior state auditors; • ambassadors, *chargés d'affaires* and senior military officers; • senior officials of state-owned enterprises; • senior officials of the EU and international organisations. The Bill proposes to also include individuals performing a prescribed function.
Private Sector Consultative Forum (PSCF)	Irish AML/CFT policy is informed and assisted by the Private Sector Consultative Forum (PSCF), which provides an information-sharing framework for private-sector stakeholders and designated persons to regularly engage with public agencies on all AML/CFT issues. The PSCF is chaired in rotation on a half-yearly basis by members of the forum.
Relevant independent legal professional	This includes a barrister, solicitor or notary who acts for or on behalf of clients in financial transactions or transactions relating to land, or assists a transaction related to: • buying or selling land or business entities; • managing the money, securities or other assets of clients; • opening or managing bank, savings or securities accounts; • organising contributions necessary for the creation, operation or management of companies; creating, operating or managing trusts, companies or similar structures or arrangements.
Simplified Customer Due Diligence (SCDD)	The lowest level of due diligence that may be completed on a customer. SCDD is only appropriate where the designated person considers that the relationship or transaction presents a lower degree of risk and

	formally identifies the reasons for this determination in the relevant business risk assessment. A designated person assessing a customer under SCDD criteria is only required to identify the customer; there is no requirement to verify the identity of the customer as with CDD or ECDD. However, the business relationship must be continually monitored for trigger events that may create a requirement for further due diligence.
Suspicious Transaction Report (STR)	A report a designated person must submit to authorities (the Gardaí and Revenue Commissioners) if they know, suspect or have reasonable grounds to suspect a person is engaging in or has committed a money laundering or terrorist financing activity.
Terrorist Financing	In broad terms, techniques used to covertly channel funds (both legitimately sourced and the proceeds of crime) to terrorist organisations. Common techniques include: • the use of 'front businesses' and false charities; • smuggling of cash and high-value goods; • informal trust-based payment networks; • multiple small cash deposits for short terms in supporters' bank accounts; electronic funds transfers and the use of pre-paid credit and charge cards.
Virtual currencies[1]	A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically

[1] Hari Gupta, *L&RS Note: Virtual currencies – the regulatory challenges ahead*, June 2020.

Summary

On 10 August 2020, the Minister for Justice and Equality, Helen McEntee TD, received Cabinet approval for the publication of the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020. The Bill was officially published on 8 September 2020.

The Bill transposes the criminal justice elements of the Fifth EU Money Laundering Directive (EU 2018/843) and strengthens existing money laundering and terrorist financing legislation.

The Bill includes provisions to:[2]

- improve the safeguards for financial transactions to and from high-risk third countries, setting new limits on the use of anonymous pre-paid cards;
- bring a number of new 'designated bodies' under the existing legislation, including virtual currency providers and dealers and intermediaries in the art trade;
- prohibit credit and financial institutions from setting up anonymous safe-deposit boxes;
- enhance the customer due diligence requirements of the existing legislation; and
- provide for Ministerial guidance to clarify domestic 'prominent public functions' for the purpose of identifying politically exposed persons.

[2] See Merrion Street, 'Cabinet Approves publication of the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020', *Press Release*, 10 August 2020.

Table of Provisions

Table 1 below summarises the provisions in this Bill.

Section	Title	Effect
1.	Definitions	A standard provision setting out definitions to be used in the general interpretation of the Act. It contains 3 definitions: 'Act of 2010' refers to the principal Act – the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010* (as amended); 'Act of 2018' refers to the *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (transposing the 4AMLD); and 'Regulations of 2019' refers to the *European Union (Money Laundering and Terrorist Financing) Regulations 2019* (S.I. No 578 of 2019) (giving further effect to the 4ALMD).
2.	Amendment of section 2 of Act of 2010	This amends section 2 of the Act of 2010 to insert the definition of "Fifth Money Laundering Directive", which refers to Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018. This section also inserts a new subsection 2(3) into the Act of 2010 to clarify that references to the 'Appeal Tribunal' in that Act are to be understood as references to the Appeal Tribunal established under the new section 101A of the Act of 2010 (to be inserted by section 23 of this Act, see below).
3.	Amendment of section 24 of Act of 2010	This amends section 24 of the Act of 2010 to substitute a new definition of 'property service provider' into the section. The section also inserts definitions for 'custodian wallet provider', 'Electronic Identification Regulation', virtual currencies' and 'virtual currency service provider' into subsection 24(1) of the Act of 2010.
4.	Amendment of section 25 of Act of 2010	This amends section 25 of the Act of 2010 to expand the 'tax advisor' and 'property service provider' classes of designated person to include, respectively: • any other person whose principal business or professional activity is to provide, directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax matters; and • a property service provider acting as an intermediary in the letting of immovable property, but only in respect of transactions for which the monthly rent amounts to a total of at least €10,000. The section also adds three new classes of designated persons: • a provider engaged in exchange services between virtual currencies and fiat currencies;

		• a person trading or acting as an intermediary in the trade of works of art (including when carried out by an art gallery or an auction house) but only in respect of transaction(s) of a total value of at least €10,000; and • a person storing, trading or acting as an intermediary in the trade of works of art when this is carried out in a free port but only in respect of transaction(s) of a total value of at least €10,000.
5.	Amendment of section 33 of Act of 2010	This amends section 33 of the Act of 2010 to include a new trigger for performing CDD. A designated person will have to conduct CDD at any time where the designated person is obliged by law to contact the customer for the purpose of reviewing relevant information about beneficial ownership, including where obliged to do so to seek information for tax purposes. The section also provides that if the beneficial owner is a senior managing official, the designated person is also obliged to verify the his or her identity, keeping records of the actions taken in and any difficulties associated with the identification process.
6.	Amendment of section 33A of Act of 2010	This amends section 33A of the Act of 2010 to reduce the sums on low-value electronic money payments that allow for exemptions to the CDD process. An exemption from performing CDD will only apply in circumstances that indicate lower risk, where the issuer of the payment instrument carries out sufficient monitoring of the transaction(s)or business relationship to enable the detection of unusual or suspicious transactions, where the transaction is not a remote payment transaction of more than €50, and where the payment instrument: • can only electronically store up to €150; • can only be used to purchase goods and services; • cannot be funded with anonymous electronic money; • does not allow the user to redeem more than €50 in cash; and • is not reloadable or, where it cannot be used outside Ireland, it has a monthly transaction limit of €150. The section would also prohibit a credit or financial institution from accepting payment through an anonymous prepaid card issued in a non-EU state where that card does not meet the exemption criteria. A failure to adhere to this prohibition would result in an offence, punishable by a Class A fine (up to €5,000) or, on summary conviction, imprisonment for up to 12 months. The prison sentence may be for up to 5 years if the conviction is by indictment.

7.	Amendment of section 35 of Act of 2010	This amends section 35 of the Act of 2010 to require a designated person to ascertain that information concerning the beneficial ownership of the potential customer is entered on the relevant BOR, prior to the establishment of a business relationship with the customer. The relevant BOR for a customer who is a beneficial owner of a trust is the express trust (beneficial ownership) register; the relevant BOR for a person who is a beneficial owner of a corporation is the Central Register of Beneficial Ownership of Companies and Industrial Provident Societies; and the relevant BOR for a customer who is a beneficial owner of a financial vehicle, credit union or unit trust is the Central Register of Beneficial Ownership Irish Collection Asset-management Vehicles, Credit Unions and Unit Trusts. The section provides that a credit or financial institution may allow an account to be opened with it by a customer prior to the relevant BOR check so long as the designated person ensures that transactions on the account are not carried out by or on behalf of the customer prior to ascertaining the BOR information.
8.	Amendment of section 36A of the Act of 2010	This amends section 36A of the Act of 2010 to require a designated person to, as far as possible, examine the background and purpose of any transaction that is complex, unusually large, conducted in an unusual pattern or do not appear to have an economic or lawful purpose.
9.	Amendment of section 37 of the Act of 2010	This amends section 37 of the Act of 2010 to require a designated person to continue to treat a person as a politically exposed person for as long as is required to take into account the continuing risk posed by that person, until such time as that risk is deemed to be negligible. This section also expands the definition of a politically exposed person to include any individual performing a prescribed function, and it empowers the Minister for Justice and Equality, with the consent of the Minister for Finance, to issue guidelines to competent authorities in respect of functions in the State that may be considered to be prominent public functions. Competent authorities will be obliged to consider any such guidelines.
10.	Amendment of section 38 of the Act of 2010	This amends section 38 of the Act of 2010 to provide that only correspondent relationships involving the execution of payments need to be the subject of ECDD procedures.

11.	Amendment of section 38A of the Act of 2010	This substitutes a new subsection 38A(1) into the Act of 2010 to require designated persons, when dealing with a customer established or residing in a high-risk third country, to: • obtain additional information on the customer and on the beneficial owner; • obtain additional information on the intended nature of the business relationship; • obtain information on the source of funds and source of wealth of the customer and of the beneficial owner; • obtain information on the reasons for the intended or performed transactions; • obtain the approval of senior management to establish and/or continue the business relationship; • conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and by selecting patterns of transactions that need further examination.
12.	Amendment of section 40 of the Act of 2010	This amends section 40 of the Act of 2010 to further limit the extent to which a designated person may rely on a third party's CDD. If the designated person is relying on the third party to provide documents and information relating to the customer upon request, that information must include any information obtained by the third party from relevant trust services (as set out in the EU Electronic Identification Regulation).
13.	Amendment of section 42 of the Act of 2010	This inserts a new subsection into section 42 of the Act of 2010 to empower the FIU to provide timely feedback to a designated person who makes a STR on the effectiveness of any follow-up to the report.
14.	Amendment of section 51 of the Act of 2010	This amends section 51 of the Act of 2010 to further limit the defence for disclosure to those specified persons who can prove that the disclosure was made to either: • a credit institution or financial institution incorporated in a Member State, where both the institution making the disclosure, or on whose behalf the disclosure was made, and the institution to which it was made belonged to the same group, or • a majority-owned subsidiary or branch situated in a third country of a credit institution or financial institution incorporated in a Member State, where the subsidiary or branch was in compliance with prescribed group-wide policies and procedures, including procedures for sharing information within a group.

15.	Amendment of section 55 of the Act of 2010	This amends section 55 of the Act of 2010 to qualify that documents used to verify the identity of customers or beneficial owners includes any information derived from relevant trust services as set out in the EU Electronic Identification Regulation.
16.	Amendment of section 58 of the Act of 2010	This amends section 58 of the Act to prohibit credit or financial institutions from providing or keeping an anonymous safe deposit box for a customer.
17.	Amendment of section 60 of the Act of 2010	This amends section 60 of the Act of 2010 to identify the new competent authorities for certain designated persons: • the new competent authority for barristers is the Legal Services Regulatory Authority; • the competent authority for designated persons who is a provider engaged in exchange services between virtual currencies and fiat currencies or a custodian wallet provider is the Central Bank of Ireland; and • the competent authority for designated property service providers is the Property Services Regulatory Authority.
18.	Amendment of section 63B of the Act of 2010	This inserts a new subsection 63B(2A) into the Act of 2010. The new subsection qualifies that cooperation with Member State competent authorities may include the sharing of information where it is not prevented by law. It also provides that the provision of assistance must not be refused on the basis that: • the request for the sharing of information or the of provision assistance is also considered to involve tax matters; • the law of the State requires the competent authority to maintain secrecy or confidentiality except in those cases where the relevant information that is sought is protected by legal privilege; • there is an inquiry, investigation or proceeding underway in the State, unless the sharing of such information or the provision of assistance would impede the inquiry, investigation or proceeding; or • the nature or status of the requesting competent authority is different from that of the competent authority of whom the request is made.
19.	Amendment of section 63D of the Act of 2010	This amends section 63D of the Act of 2010 to ensure that competent authorities only employ those persons who maintain high professional standards, including standards addressing conflicts of interest.
20.	Reporting breaches to competent authority	This inserts a new section 63E into the Act of 2010. It would require competent authorities to establish effective and reliable mechanisms to encourage reporting of potential breaches. Competent authorities must also provide one or more secure

		communication channels to allow people to lodge STRs and report threats, or retaliatory or hostile actions, resulting from the report.
21.	Amendment of section 65 of the Act of 2010	This inserts a new subsection 65(2) into the Act of 2010 requiring competent authorities that are not State competent authorities to publish information in the authority's annual report regarding measures taken to monitor AML/CFT compliance by designated persons falling under its regulatory competence.
22.	Amendment of section 84 of the Act of 2010	This deletes the definition of the term "Appeal Tribunal" from section 84 of the Act of 2020.
23.	Appeal Tribunal	This inserts a new section 101A into the Act of 2020. The new section establishes a tribunal to be called the Appeal Tribunal. The new section outlines how the tribunal is to be constituted, how members are to be appointed and removed and the conditions of appointment. The provision makes the Appeal Tribunal independent in the exercise of its functions and empower the tribunal to regulate its own procedures.
24.	Amendment of Schedule 3 to the Act of 2010	This amends Schedule 3 of the Act of 2010 to qualify that the specified geographical risk factors (suggesting a lower risk of money laundering or terrorist financing) refer to the place of registration, establishment and/or residence.
25.	Amendment of Schedule 4 to the Act of 2010	This amends Schedule 4 of the Act of 2010 to include further specified red flags, for transactions that pose a higher risk of money laundering and/or terrorist financing. A higher risk is posed where: • a customer is a third-country national who applies for residence rights or citizenship in the State in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities in the State; • a product, service, transaction or delivery channel involves the use of non-face-to-face business relationships without the use of certain safeguards such as electronic identification means, relevant trust services or other secure, remote or electronic, identification processes that are officially regulated, recognised, approved or accepted; • a transaction relates to oil, arms, precious metals, tobacco products, cultural artefacts and items of archaeological, historical, cultural and religious importance, or of rare or scientific value, including ivory and protected species.
26.	Short title, commencement and collective citation	A standard provision setting out the short title of the Act, the collective citation, and commencement information. This Act will come into effect by order of the Minister. Different commencement days may be appointed for different provisions.

Source: L&RS analysis of the Bill

Background

Money laundering: a snapshot

Money laundering is the process by which criminals disguise the illicit origins of funds. It allows them to conceal the evidence of their crimes and to use the proceeds in legitimate financial systems and markets.

The global extent of money laundering is, by its nature, difficult to estimate. The United Nations Office on Drugs and Crime suggests that **dirty money worth between 2% and 5% of global GDP – that is, from US$800 billion to US$2 trillion – is laundered throughout the world every year**.[3] A 2015 report sponsored by the EU estimates that organised criminal activity in the EU generates revenues of at least €110 billion annually.[4]

The crimes that generate the funds to be laundered – known as 'predicate offences' – can vary between countries according to their economies, legal systems, social conditions and geography. The predominant ones include drug trafficking, human trafficking and exploitation, theft, smuggling, illegal firearms, gambling, counterfeiting, online crimes and tax fraud and evasion. The means used to launder the proceeds of crime are equally varied: common techniques involve investment in land and buildings, purchases of high-value goods (such as designer clothing, jewellery and art) that are easy to transport and sell, and the use of cash-centred 'front' businesses such as betting shops, retail outlets and pubs.

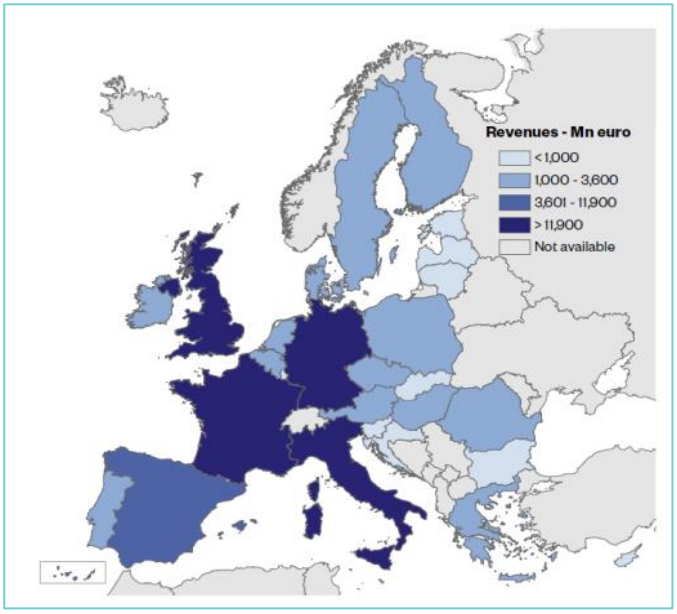

Figure 1: Estimated illicit revenues: selected EU markets

Source: Project OCP, Final Report (2015)

New technology has allowed criminals to exploit pre-paid credit cards, online betting, cash transfers and hard to trace 'cryptocurrencies', such as Bitcoin. Many criminals also take advantage of jurisdictions that are not tightly regulated or that permit the use of trusts, nominees and shell companies to obscure the beneficial ownership of money and property.[5]

---

[3] UNDOC, *Money Laundering and Globalisation*.

[4] Project OCP: Organised Crime Portfolio, *Final Report, From Illegal Markets to Legitimate Businesses: The Portfolio of Organised Crime in Europe* (2015) at pp. 34-35.

[5] 'Panama Papers' law firm partners arrested over money laundering claims, Irish Independent, 12 February 2017

Money laundering is considered to be essential for organised crime: the vast sums generated by crime can become much too large to be recycled entirely on a 'black market'. Without access to legitimate financial systems and markets, those funds would simply lose their value.[6] Significantly, money laundering does not only allow criminals to fund further criminal activities, it enables them to use their ill-gotten funds to influence markets and policy, to expand and diversify their activities and to spread corruption and instability through commercial, financial and political institutions.

Money laundering poses serious risks to Irish communities and businesses, and the State: the Government's National Risk Assessment in relation to money laundering and terrorist financing cites a 2015 study on financial aspects of organised crime in Europe which estimated that in 2010 money laundering transactions totalled €1.7 billion in the State.[7] The National Risk Assessment identifies money laundering risks arising from numerous types of crime including drug offences, financial crime, tobacco smuggling, tax evasion, prostitution, fuel laundering, cybercrime and corruption.

Terrorist financing

Terrorist financing is often conducted in a very similar manner to money laundering, in that terrorist groups frequently raise money using criminal means, such as robbery, fraud and extortion. They also encounter the same difficulties as 'ordinary' criminals in making use of the proceeds. However, in many cases, terrorist financing relies on ostensibly legitimate sources of income such as donations or contributions from what may at first appear to be charitable bodies. In those situations, terrorist financing may be seen as the opposite of money laundering – it involves moving 'legitimate' funds without detection into illegitimate channels. Studies suggest that terrorists use many of the same techniques as money launderers, such as the use of front businesses, cash smuggling, the purchase (or theft) and re-sale of high-value retail goods and multiple small cash transactions made through the accounts of supporters or by using pre-paid credit facilities.[8]

The role of the FATF

Policies and legislative approaches to money laundering and terrorist financing in the EU, USA and many Organisation for Economic Co-operation and Development (OECD) economies are significantly influenced by the recommendations of the Financial Action Task Force (FATF). The FATF is an inter-governmental body that was established in 1989 by the G-7 (as it then was) group of leading world economies, with the primary object of addressing financial crime. The FATF shares its headquarters with the OECD and works closely with that body. Members of the FATF

---

[6] The notorious drug boss Pablo Escobar is reported to have lost up to 10% of his annual turnover of more than US$20 billion to the effects of rats and mould on warehoused money. Business Insider (Australia), 11 September 2015.

[7] Savona Ernesto U. & Riccardi Michele (eds.) (2015) *Final Report of Project OCP*, cited in *National Risk Assessment for Ireland – Money Laundering and Terrorist Financing*, Departments of Finance and of Justice and Equality (2017), p. 24, fn. 63

[8] See for example the FATF's 2015 report *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*

include the European Commission as well as Ireland and most other EU Member States, the USA, Japan, Canada, China and Russia.

Since 1990, the FATF has issued and revised recommendations on policies to combat money laundering and terrorist financing. These recommendations act as a template to FATF members for anti-money laundering and counter-terrorist financing legislation (conventionally referred to as 'AML/CFT legislation'). The most recent edition comprises 40 recommendations; it was issued in 2012.[9]

The FATF conducts mutual evaluations of its members' levels of implementation of the FATF Recommendations on an ongoing basis. These are peer reviews, where members from different countries assess another country in accordance with the published methodology.[10]

Ireland was last evaluated by FATF in 2017. The report,[11] adopted at the FATF Plenary Meeting of June 2017, found:[12]

> "Generally, Ireland has a good understanding of the money laundering and terrorist financing risks it faces. It has broadened this understanding to relevant agencies and the private sector through effective national cooperation and coordination. Ireland's national risk assessment demonstrated an appreciation of the risks it could face from beyond its borders but, given its position as an important regional and international financial centre, it could further refine its understanding of international money laundering risks.
>
> Both the Central Bank of Ireland and the Department of Justice and Equality follow a risk-based approach in the supervision of their respective sectors and have established good cooperation with financial institutions and designated non-financial businesses and professions.
>
> Coordination, cooperation and the use of financial intelligence are strong points of the Irish AML/CFT framework. A range of competent agencies routinely access financial information on short notice to assist in their investigations. Irish authorities have also demonstrated that they cooperate internationally on money laundering and terrorist financing issues and are handling an increasing number of requests for assistance. **Ireland has sound laws to pursue money laundering and asset confiscation but has not yet achieved convictions after trial and has only been moderately successful in confiscating**

---

[9] FATF (2012) *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations*. This edition includes interpretative notes updated to November 2015.

[10] FATF (2013) *FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems*. This edition includes updates made in October 2019.

[11] FAFT (2017), *Anti-money laundering and counter-terrorist financing measures: Ireland – Mutual Evaluation Report*.

[12] FAFT (2017) *Ireland's measures to combat money laundering and the financing of terrorism and proliferation*.

> **criminal proceeds. Ireland prioritises counter-terrorism efforts and has secured terrorism-related convictions but it should more actively pursue the prosecution of terrorist financing.**
>
> **Ireland demonstrated that it has a generally sound AML/CFT framework but it must implement further measures, including additional resources to money laundering investigations.** Some of these measures are forthcoming and will further strengthen the effectiveness of Ireland's efforts to tackle money laundering and terrorist financing." (Emphasis added)

On 14 September 2020 the FATF published its latest report, Virtual Assets – Red Flag Indicators of Money Laundering and Terrorist Financing. This report covers 100 case studies, designed to help national authorities and financial institutions identify potential money laundering and terrorist financing activity involving virtual assets by highlighting the most important red flag indicators that could suggest criminal behaviour. The report aims to complement the June 2019 FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers which explains how to understand the money laundering and terrorist financing risks of virtual assets, how to license and register the sector, actions sectors need to take to know information about their customers, how to store this information securely, and how to detect and report suspicious transactions. These two reports will provide guidance on how the FIU will be expected to police the use of virtual assets as money laundering and terrorist financing tools.

EU Anti-Money Laundering Legislation and Policy

In 1991, the European Council legislated to combat money laundering, adopting the First Anti-Money Laundering Directive (1AMLD).[13] This legislation required Member States to prohibit money laundering and to oblige their respective financial sectors to identify their customers, guard against money laundering, and to report any suspicious activities to their competent authorities. The 1AMLD was primarily designed to target proceeds of the drugs trade.

The 1AMLD was succeeded by two further directives, the Second Anti-Money Laundering Directive (2AMLD)[14] and the Third Anti-Money Laundering Directive (3AMLD),[15] in 2001 and 2005 respectively.

The 2AMLD broadened the focus of European Anti-Money Laundering (AML) legislation to restrict financing of terrorist organisations (counter terrorist financing or CFT) and imposed requirements to identify customers and guard against money laundering on non-financial businesses, such as accountants and notaries.

The 3AMLD, went even further creating an obligation on institutions covered by the Directive to identify the beneficial owner of legal or corporate entities on whose behalf a transaction was conducted.

The 3AMLD was repealed with effect from 26 June 2017 and replaced with the Fourth Anti-Money Laundering Directive (4AMLD).[16] Member States were to have transposed all the mandatory provisions of the 4AMLD into national law by 26 June 2017.

In Ireland, art.30(1) of the 4AMLD was transposed early through the *European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2016* (S.I. No 560 of 2016) (revoked and replaced by *European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019* (S.I. No 110 of 2019)).

On 20 December 2016 the Government agreed upon the General Scheme for the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2016 with the aim of transposing the remainder of the 4AMLD. The 4AMLD was eventually transposed with the enactment of the

[13] See Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.

[14] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.

[15] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

[16] Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) 2012/648 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018 on 14 November 2018.[17]

On 16 July 2020, the Court of Justice of the EU (CJEU) ordered Ireland to pay a fine of €2 million to the Commission for its failure to fully transpose the 4ALMD on time, finding that the 4AMLD was not fully transposed into Irish law until 3 December 2019.[18]

Less than a year after the publication of the 4AMLD, the International Consortium of Investigative Journalists published the 'Panama Papers'. These were documents and correspondence from the archives of Mossack Fonseca – a law firm that operated in Panama, the British Virgin Islands and other offshore banking locations – that had been disclosed by a whistle blower. The documents disclosed financial transactions dating from the 1970s to 2015 worth billions of US Dollars, involving banks, high-worth individuals, politicians and – in some cases – persons of very dubious reputation. The reports indicated widespread disregard for regulatory and compliance procedures, tax evasion, money laundering and other criminal activities. In April 2016 the Panama Papers were published in newspapers around the world including *The Irish Times*, provoking a public outcry against tax evasion, the use of offshore banking structures and the abuse of international financial systems. The Panama Papers pointed to the widespread involvement of European residents, banks and professionals such as lawyers, accountants and tax advisers.

In July 2016, following terrorist attacks in Paris and Brussels and in light of the revelations of extensive multinational tax evasion listed in the Panama Papers,[19] the European Commission tabled a proposal for the Fifth Anti-Money Laundering Directive (5AMLD).[20] On 20 December 2017, the European Parliament and the Council agreed on amendments to the text of the 5AMLD, paving the way for the text of the Directive to be published on 19 June 2018. Member States had until 10 January 2020 to transpose the provisions of the 5AMLD.[21]

On 14 May 2020, the European Commission sent letters of formal notice to Ireland at the same time as Belgium, the Czech Republic, Estonia, Greece, Luxembourg, Austria, Poland and the United Kingdom for having only partially transposed 5AMLD. In February 2020, the Commission had previously also addressed letters of formal notice to Cyprus, Hungary, the Netherlands, Portugal, Romania, Slovakia, Slovenia and Spain because they had not communicated any transposition measures. The Commission stated that in the absence of a satisfactory response within four months of the date of the letter, the Commission may decide to send reasoned

---

[17] Michael O'Sullivan, *Bill Digest for the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2018*, Houses of the Oireachtas Service, Library and Research Service, 9 May 2018.

[18] Dillon Eustace, 'ECJ fines Ireland €2m over failure to transpose MLD4 on time', 21 July 2020. In deciding to impose a financial penalty of €2m on Ireland the CJEU considered the seriousness of Ireland's failure to fulfil its obligations, the length of time which the failure persisted (almost 2.5 years), and the ability of Ireland to pay a financial penalty, by reference to its GNP. The CJEU fined Romania €3m for a similar breach of its obligations to transpose the 4AMLD in time.

[19] See PANA Committee Report.

[20] See COM (2016) 450 (6 July 2016).

[21] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

opinions.[22] As shown by the decision of the CJEU to fine Ireland and Romania for their late transposition of the 4AMLD, the delay in fully transposing 5AMLD may have further financial consequences for the State.

As noted by Professor Demetriades and Dr Vassileva in a recent article, it is fundamentally important to deal with AML/CFT at the regional level:[23]

> "Once laundered money enters the euro area-or the single EU market-it creates risks for all the EU Member States. The risks are wide ranging. They include reputational costs not only to ESCB and ECB, but also possible financial instability since illicit financial flows can also result in bank failures, as in the ABLV case because of the actions taken by the US authorities. In addition, as argued above, these illicit financial flows may often be tied to corruption, rule of law decay, or malign activities undermining democracy, all of which underlie and promote European disintegration."

In an effort to strengthen criminal sanctions, to better coordinate the fight against money laundering across the EU and to allow for swifter cross-border cooperation between competent authorities, on 12 November 2018, the European Parliament published updated rules to further strengthen the fight against money laundering in the form of the Sixth Anti-Money Laundering Directive (6AMLD). The majority of Member States are required to transpose the 6AMLD into national law by 3 December 2020.[24] Although Ireland (together with the United Kingdom and Denmark) is not obliged to transpose 6AMLD, it has been reported that the government had indicated an intention to opt-in.[25]

The above should be read within the context of meetings of the European Union Council Economic and Financial Affairs Council on 10 October 2019 and 5 December 2019.[26] Among other things, ministers at the meeting discussed progress in the implementation of the anti-money laundering action plan set out in December 2018, as well as strategic priorities which will guide the European Commission's longer-term actions.[27] On 5 December 2019 the Council formally invited the Commission to explore possible further actions to enhance the existing AML rules, by considering:

- ways of ensuring a more robust and effective cooperation between the relevant authorities and bodies involved in anti-money laundering and terrorist financing, including through addressing impediments on exchange of information between them;
- whether some aspects could be better addressed through a regulation;

---

[22] European Commission, 'May infringements package: key decisions', *Press Release*, 14 May 2020.

[23] Professor P Demetriades and Dr R Vassileva, 'Money Laundering and Central Bank Governance in The European Union', (2020) *Journal of International Economic Law* 23(2), June 2020, 509 at 530-531

[24] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law.

[25] M. Adamberry and A. Pilcher, '5AMLD & 6AMLD: Is AML/CFT A Moving Target?', *IFC Media Review*, 2 April 2020.

[26] The Council of the European Union, Meeting of the Economic and Financial Affairs Council, 10 October 2019.

[27] Ibid.

- possibilities, advantages and disadvantages of conferring certain supervisory responsibilities and powers to an EU body.[28]

In response, on 7 May 2020, the Commission published a six-point Action Plan to help further strengthen the EU's fight against money laundering and terrorist financing. The aim of the Action Plan is to shut down any remaining loopholes and remove any weak links in the EU's AML/CFT rules. The Action Plan builds on six pillars:

- Ensuring the effective implementation of the existing EU AML/CFT framework;
- Establishing an EU single rule book on AML/CFT;
- Bringing about EU level AML/CFT supervision;
- Establishing a support and cooperation mechanism for FIUs;
- Enforcing Union-level criminal law provisions and information exchange;
- Strengthening the international dimension of the EU AML/CFT framework.[29]

Also, on 7 May 2020, the Commission published a new refined methodology to identify high-risk third countries that have strategic deficiencies in their AML/CFT regimes that pose significant threats to the EU's financial system. Part of this process included the adoption of an updated list of high-risk third countries.[30]

On 10 July 2020, the Parliament adopted a resolution welcoming the Commission's Action Plan, adding that MEPs want the Commission to address the persisting lack of quality data to identify ultimate beneficial owners, by setting up interconnected and high-quality registers within the EU, with high standards of data protection. The Parliament called on the Commission to widen the scope of supervised entities, to include new and disruptive market sectors such as crypto assets. MEPs also reiterated that non-cooperative jurisdictions and high-risk third countries must be immediately blacklisted, while creating clear benchmarks and cooperating with those undertaking reforms. In addition, the Parliament called for the mutual recognition of freezing and confiscation orders to be enforced, making criminal assets easier to recover across borders and enable swift cross-border cooperation. Finally, The Parliament called for the European Central Bank to be able to withdraw the licence of any bank operating in the euro area found to be in breach of AML/CTF obligations, independently of the assessment of national AML authorities.[31]

---

[28] The Council of the European Union, 'Money laundering: Council sets strategic priorities for further reforms' *Press Release*, 5 December 2019.

[29] European Commission, 'Commission steps up fight against money laundering and terrorist financing', *Press Release*, 7 May 2020.

[30] European Commission, 'Commission steps up fight against money laundering and terrorist financing', *Press Release*, 7 May 2020.

The list of high-risk third countries was amended by delegated legislation, which comes into force on 1 October 2020. The following countries will be added to the list: The Bahamas, Barbados, Botswana, Cambodia, Ghana, Jamaica, Mauritius, Mongolia, Myanmar, Nicaragua, Panama and Zimbabwe. The following countries will be removed from the list: Bosnia-Herzegovina, Ethiopia, Guyana, Lao People's Democratic Republic, Sri Lanka and Tunisia. A consolidated list of high-risk third countries and details of the new methodology may be found here.

[31] European Parliament, 'MEPs set out new measures to stop money laundering', *Press Release*, 10 July 2020.

In August 2020, Insurance Ireland published a response to the Commission's Action Plan. Among other comment, the organisation suggested that virtual asset service providers should be included within the scope of obliged entities, to ensure that legitimate innovations are not used to facilitate money laundering or terrorist finance activities, in particular the group pointed to crowd-funding platforms. Insurance Ireland noted:[32]

"As discussed in a 2015 FATF Report into Emerging Terrorist Financing Risks, 'crowdfunding is vulnerable to exploitation for illicit purposes, including instances where the true purpose of the funding campaign is masked. Individuals and organisations seeking to fundraise for terrorism and extremism support may claim to be engaging in legitimate charitable or humanitarian activities and may establish NPOs for these purposes. Several cases indicate that the end-use of funds collected through crowdfunding and social networks was not known to donors".

Insurance Ireland also requested that more information should be disseminated covering how to balance AML/CTF requirements with requirements set out under the GDPR, such as between the risk-based approach to the gathering, processing and retention of the personal data of customers (as well as of beneficial owners and other relevant related parties) as required under AML/CFT regulations versus GDPR rules around consent, excessive processing and the 'right to be forgotten'. The organisation suggested that an aligned approach between AML/CFT and GDPR regulations would help address these issues.[33]

[32] Insurance Ireland, *Response to Public consultation on an action plan for a comprehensive Union policy on preventing money laundering and terrorist financing*, August 2020 pp 12-15.

[33] Ibid p. 16.

A summary of 4AMLD

The 4AMLD, as amended, went much further than simply creating an obligation on relevant entities to identify beneficial owners. The directive also incorporated a risk-based approach that placed the onus on "obliged entities" ("designated persons" in the domestic legislation) to conduct risk assessments of their clients. Further, among other things, the 4AMLD made changes to the Simplified Customer Due Diligence (SCDD) procedures and the Enhanced Customer Due Diligence (ECDD) procedures applicable when dealing with specified categories of clients/customers. Each of these key changes are examined below.

A risk-based approach

As noted, the 4AMLD introduced a risk-based approach to AML, requiring obliged entities to take appropriate steps to identify and assess the risks of money laundering and terrorist financing in each of their individual business relationships and transactions while also obliging them to conduct an AML assessment, following a prescribed list of actions.

Obliged entities are now expected to maintain an awareness of policies, controls, and procedures that have been put in place by authorities to mitigate the risk of money laundering and then identify, understand, manage and mitigate their own risks by reference to these policies, controls, and procedures. The onus falls on obliged entities to apply customer due diligence (CDD) to transactions and report any suspicious activity to the authorities through suspicious transaction reports (STRs).

On 26 June 2017, the Joint Committee of the three European Supervisory Authorities (ESAs—European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA)) issued Guidelines aimed at promoting a common understanding of the risk-based approach to AML (the "Guidelines"), setting out how this approach should be applied. The Guidelines provided obliged entities with the tools they would need to make informed, risk-based decisions on the effective management of individual business relationships and occasional transactions for AML purposes. The guidelines have been applicable from 26 June 2018.[34]

Beneficial ownership of relevant entities and of express trusts

The 4AMLD required Member States to establish a central beneficial ownership register (BOR). This BOR must be made accessible to competent authorities, obliged entities (for the purposes of conducting CDD) and individuals who can demonstrate a "legitimate interest".

---

[34] Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions: see https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf.

The 4AMLD also obliges the trustees of any express trust governed by the law of the State, where the trust has "tax consequences" for the beneficiaries, to place information about the trust on a central BOR. The information must include: the identity of the settlor, the name(s) of the trustee(s), the name of the protector (if any), the names of the beneficiaries or class of beneficiaries; and the details of any other natural person exercising effective control over the trust. This trusts register will be accessible only to competent authorities and financial intelligence units.

Changes to SCDD and ECDD

The 3AMLD allowed obliged entities to apply SCDD procedures to transactions entered into by clients/customers who fell within specified categories. Although the use of SCDD procedures is still allowed under the 4AMLD, obliged entities may now only use these procedures to conduct CDD where the individual business relationship or transaction carries a lower degree of risk – obliged entities cannot simply assume that all transactions of a particular customer or class of customer may be assessed through a SCDD procedure.

The 4AMLD also extended the concept of politically-exposed persons (PEPs), who are subject to ECDD procedures. The 3AMLD only included foreign PEPs, while the 4AMLD includes both domestic and foreign PEPs. The 4AMLD expressly states that obliged entities must have appropriate risk management systems in place, including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is a PEP.

The 4AMLD allows the European Commission to identify third-country jurisdictions which are deemed to have strategic deficiencies in their national AML regimes ("high-risk third countries"). The European Commission applies a formal methodology to determine if a country should be listed. The Commission starts by considering Financial Action Task Force (FAFT) lists, complementing this by making an autonomous assessment of additional countries using the following approach:

- identify the risk profile and the level of threat to which the country is exposed;
- assess the legal framework and its effective application in 8 key areas – by analysing the countries measures on:
  - criminalisation of money laundering and terrorist financing;
  - CDD requirements, record keeping and reporting of suspicious transactions in the financial sector;
  - the same requirements in the non-financial sector;
  - the existence of dissuasive, proportionate and effective sanctions in case of breaches;
  - the powers and procedures of competent authorities;
  - their practice in international cooperation;
  - the availability and exchange of information on beneficial ownership of legal persons and legal arrangements;
  - implementation of targeted financial sanctions.[35]

The methodology was revised on 7 May 2020, to ensure an increased engagement with third countries by:

[35] European Commission, *EU Methodology for the identification of High-Risk Third Countries*.

- consulting third countries on preliminary findings;
- drafting country-specific 'EU benchmarks' to address each country's concerns (identified on a preliminary basis) in relation to the criteria set by the Anti-Money Laundering Directive;
- seeking third countries' commitment to implement specific corrective measures before a listing is considered;
- setting a deadline of 12 months for third countries to commit to addressing concerns.

A listing occurs where the third country fails to cooperate (i.e. refuses to express a commitment) or where it fails to implement the benchmarks within an agreed period.[36]

Under the 4AMLD, transactions made by persons or entities from high-risk third countries automatically trigger ECDD procedures, which include stricter monitoring of flows of money.

The ESA Guidelines published on 26 June 2017 provide advice on the risk factors to be taken into consideration when considering SCDD and ECDD procedures.

[36] European Commission, *EU Methodology for the identification of High-Risk Third Countries*.

A summary of 5AMLD

The 5AMLD proposed a number of amendments to the 4AMLD and some consequential amendments to the Company Law Directive[37] to better align the legislation with modern trends and technologies and to increase levels of transparency of financial transactions, of corporate and other legal entities, and of trusts and trust-like legal arrangements. The 5AMLD also aimed to improve the interconnectivity of national BORs.

Specifically, in relation to BORs, the 5AMLD amended 4AMLD to:

- set 10 January 2020 as the deadline to establish a BOR for companies;
- extend access to corporate BORs by requiring full access to be granted to competent authorities and Financial Intelligence Units (FIUs) and to obliged entities within the framework of customer due diligence (CDD); restricted access to corporate BORs must also be granted to 'any member of the general public', within the context of the limited 'security' exemption;
- set 10 March 2020 as the deadline to establish a BOR for trusts;
- extend access to trust BORs by requiring full access to be granted to competent authorities and FIUs, and to obliged entities (within the framework of CDD); restricted access to trust BORs must also be granted to any person that can demonstrate a legitimate interest in the subject trust and to any interested person who files a written request in relation to a trust holding or owning a controlling interest in a corporate or other legal entity;
- require Member States to implement mechanisms to ensure that information listed on the BORs is adequate, accurate and current; and
- create an obligation on obliged entities to consult BORs when performing CDD.

The amendments to 4AMLD made by 5ALMD also include:

- extends the scope of the AML/CFT rules to virtual currency platforms and wallet providers and providers of tax-related services, and, in prescribed circumstances, traders of art and property letting agents;
- prohibits financial institutions from providing anonymous bank and savings accounts, and safe-deposit box services;
- requires Member States to establish centralised bank, safe-deposit box and payment account registers or data retrieval systems by 10 September 2020;
- obliges Member States to issue a list of categories of domestic PEPs;
- introduces strict ECDD measures for high-risk third countries;
- provides protections for whistle blowers;
- lowers the thresholds for anonymous prepaid cards and e-money financial vehicles; and

[37] As to the Company Law Directive see Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent

- enhances the powers of FIUs, facilitating cooperation and information exchange among authorities.

Parts of the 5AMLD aim to increase the regulation of virtual currencies. Entities that hold, store or transfer virtual currencies would fall within the regulatory regime. When transposed, entities would need to identify customers and report any suspicious activity to the Financial Intelligence Unit of An Garda Síochána. New legislation would likely remove a level of anonymity from virtual currency transactions. This would make virtual currency exchanges, and their users, more transparent.

However, the regulatory regime may still have its limits. It can only regulate established virtual currency exchanges and wallets. This leaves entities that transact outside the regime unregulated. It is these entities that may pose the biggest risk of money laundering. Thus, it may be necessary to expand the category of entities subject to the anti-money laundering rules. Legislators could potentially amend the rules to include anyone who facilitates the creation and exchange of virtual currencies.[38]

[38] See further Hari Gupta, *L&RS Note: Virtual currencies – the regulatory challenges ahead*, June 2020.

Transposition of the 5AMLD in Ireland

Pre-legislative scrutiny

In January 2019, the Department of Justice and Equality published the General Scheme of the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2019. On 27 February 2019, the Committee on Justice and Equality confirmed to the Department that detailed scrutiny would not be required. No public consultation accompanied the publication of the General Scheme or the drafting of the related Statutory Instruments needed to transpose the elements of the 5AMLD related to beneficial ownership registers. In contrast, the United Kingdom Government, through HM Treasury, conducted a two-month public consultation process on the transposition of the 5AMLD from April to June 2019.[39]

Beneficial Ownership Registers

Elements of the amended 4AMLD relating to the corporate BOR and the trusts BOR have already been transposed through three separate Statutory Instruments, two of which came into effect in 2019 and the third came into effect on 25 June 2020:

- the *European Union (Anti-Money Laundering: Beneficial Ownership Of Trusts) Regulations 2019* (S.I. No 16 of 2019) (the 'Trusts BOR Regulations') require trustees to collect and keep up-to-date information on the beneficial ownership of trusts, and to make it available to authorised persons (such as An Garda Síochána, the Revenue Commissioners or other money-laundering authorities), as well as to persons (such as financial institutions) making routine enquiries under money-laundering legislation;
- the *European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019* (S.I. No 110 of 2019) (the 'Companies BOR Regulations') provide for companies to maintain their beneficial ownership details on an internal register and register details of beneficial owners with the Companies Registration Office (CRO; the CRO can then make some or all of the register available to members of the general public as well as to relevant authorities; and
- the European Union (Modifications of Statutory Instrument No. 110 of 2019) (Registration of Beneficial Ownership of Certain Financial Vehicles) Regulations 2020 (S.I. No 233 of 2020) (the 'Financial Vehicles BOR Regulations').

The Companies BOR Regulations appear to satisfy the transposition requirements of article 30 of 4AMLD (as amended by 5AMLD), but the Trusts BOR Regulations noticeably fall short of establishing a central beneficial ownership register and consequentially they cannot give requisite access to this register, as required by article 31 of the amended 4AMLD. Moreover, when the Companies BOR Regulations were given effect, the Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies did not extend to Applicable Financial Vehicles. On 6 March 2020 the Central Bank issued an information note confirming that it will be responsible for establishing a central BRO of credit unions and funds classified as ICAVs and Unit Trusts. According to the note, Common Contractual Funds and Investment Limited Partnerships will also

[39] HM Treasury of the United Kingdom of Great Britain and Northern Ireland (2019) *Transposition of the Fifth Money Laundering Directive: consultation*.

be included on the register in due course. This has been formalised with the introduction of the Financial Vehicles BOR Regulations. The Financial Vehicles BOR Regulations amend the Companies BOR Regulations to set out the beneficial ownership requirements for the following financial vehicles:

- Irish collective asset-management vehicles (ICAVs)
- credit unions; and
- unit trust schemes (within the meaning of the *Unit Trusts Act 1990* or an undertaking acting as a unit trust for collective investment in transferable securities, within the meaning of the European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations 2011 (S.I. No 352 of 2011) ('UCITS Regulations')).

The regulations appoint the Central Bank of Ireland as the Registrar of Beneficial Ownership of Irish collective asset-management vehicles, credit unions and unit trusts.

It is intended that a separate central register in respect of the beneficial ownership of trusts will be implemented by a separate authority in due course. At a meeting of the private sector consultative forum (PSCF) on 24 October 2019, it was confirmed that a new set of regulations for trusts was in the process of being developed, similar to the Companies BOR Regulations. However, work to implement a Trusts BOR continues. No formal decision has been made about the nature of the competent authority that will maintain the proposed Trusts BOR, but the assumption at present is that it will be based within the purview of the Revenue Commissioners. Until that time, trustees would be expected to hold this information on internal registers, as per their obligations under regulation 6(1) of the Trusts BOR Regulations.[40]

In response to a Parliamentary Question, in July 2019, the then Minister for Justice and Equality, Charles Flanagan T.D. stated:

> " … the Minister for Finance, has introduced, and will introduce further, legislation to deal with those elements of the Money Laundering Directives that fall within his policy remit. This includes the establishment of beneficial ownership registers and centralised bank account registers, etc."[41]

At the recent announcement of government approval for the publication of the Bill it was noted:[42]

> "… the Department of Finance is also engaged in giving effect to certain provisions of the Directive, including those relating to:
>
> - facilitating increasing transparency on who really owns corporate entities, financial vehicles and trusts by establishing beneficial ownership registers;

---

[40] Leonard Lavelle, 'Update - Central Register of Beneficial Ownership of Irish Collective Asset- management Vehicles, Credit Unions and Unit Trusts', *Beauchamps Publications*, 30 July 2020; McCann Fitzgerald, 'Recent Regulatory Updates for Fund Managers', *Knowledge*, 10 March 2020.

[41] Charles Flanagan T.D., Minister for Justice and Equality, Response to Parliamentary Question No. 342, 2 July 2019.

[42] See Merrion Street, 'Cabinet Approves publication of the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020', *Press Release*, 10 August 2020.

- ensure the creation of, and access to, centralised national bank and payment account registers or central data retrieval

The Minister for Finance has also secured Government Approval to bring forward amendments in respect of the regulation of Virtual Asset Service Providers (VASPs), that it is anticipated will be included in the Act. The amendments will ensure that the necessary registration and fitness and probity regime, required by 5AMLD for virtual asset service providers, become statutory requirements. Amendments will also address Ireland's international obligations, relating to a robust regulatory framework for new technologies, new products and new practices, as identified by the Financial Action Task Force (FATF)."

The General Scheme

The General Scheme of the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2019 was quite high-level, framing the provisions of the Bill, to give effect to elements of the 5AMLD by amending the principal legislation, the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010* (as amended) (the '2010 Act'). Heads 3, 15 and 22 were not incorporated into the Bill. They are summarised below.

Head 3: Appeal from Section 20 Order

This Head proposed to formally allow an appeal of an order of the District Court in the Circuit Court in relation to a direction or order not to carry out service or transaction on suspected grounds of money laundering or terrorist financing. This provision would not have transposed any part of the 5AMLD.

Head 15: Sanctions Screening

The Scheme proposed adding a new section 54A to the 2010 Act, empowering the Minister for Finance to make regulations on any matter in respect of screening requirements for International Financial Sanctions[43] by credit institutions and financial institutions. Breach of any such regulations would have been a criminal offence. This amendment was not expressly required by the 5AMLD.

Head 22: Additional Criminal Justice Measures

The Scheme proposed amendments to the *Criminal Assets Bureau Act 1996*, the *Criminal Justice Act 1994*, the *Criminal Justice (Theft and Fraud Offences) Act 2001* and the *Criminal Justice Act 2011*. These amendments were not required by the 5AMLD, but were included with the aim of supporting the Criminal Assets Bureau and An Garda Síochána in the administration of their AML/CFT functions, by improving access to bank records in electronic form.

---

[43] International Financial Sanctions emanate from the EU and the UN and are contained in sanctions lists. All natural and legal persons are obliged to comply with financial sanctions and can do so by monitoring the EU and UN lists and taking appropriate action as required. See further: Central Bank of Ireland, *Introduction to Financial Sanctions*.

Principal Provisions and Implications

New Designated Persons (sections 3 and 4)

Section 3 of the Bill[44] amends the definition of a 'property services provider' to refer to any person who provides a property service within the meaning of the *Property Services (Regulation) Act 2011*. Under section 2 of that Act, a 'property service' means "the provision, for consideration, in the State, in respect of property located within or outside the State, of any of the following—

> (a) the auction of property other than land,
> (b) the purchase or sale, by whatever means, of land,
> (c) the letting of land (including a letting in conacre or for the purposes of agistment), or
> (d) property management services."

The new definition covers a letting agent, effectively transposing art. 2(1)(d) of the amended 4AMLD.

New definitions of the terms 'custodian wallet provider' and 'virtual currencies' are included, transposing the definitions of art. 3(18) and (19) of the amended 4AMLD.

A definition of 'virtual currency service provider' is also included, referring to "an entity that provides services in respect of virtual currencies". It is unclear why this definition is included as the term has not been used in the Bill and it **appears to be redundant**. The Bill (see sections 4 and 17) refers to "a provider engaged in exchange services between virtual currencies and fiat currencies" – the same term as used in articles 2(3) and 47 of the 4AMLD as amended.

Section 4 of the Bill extends the list of 'designated persons' to include:

- a property service provider acting as an intermediary in the letting of immovable property, but only in respect of transactions for which the monthly rent amounts to a total of at least €10,000;
- a provider engaged in exchange services between virtual currencies and fiat currencies;
- a person trading, or acting as an intermediary in the trade, of works of art or providing storage services for art in a free port, where the total value of transactions is at least €10,000 (in one or more linked, or apparently linked, transactions).

The section also qualifies that the definition of 'tax advisor' includes "any other person whose principal business or professional activity is to provide, directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax matters."

Section 4 appears **to fall short of transposing** art. 2(3)(h) of the amended 4AMLD, in that custodian wallet providers have not been included in the list of designated persons. Section 17 of the Bill does make the Central Bank of Ireland the competent authority, regulating the activities of custodian wallet providers, but this would not have the effect of making custodian wallet providers designated persons under the Act of 2010 (as amended).

---

[44] There appears to be a small drafting error in paragraph (a) of section 3 in that the designation '(c)' is used before the definition of 'property service'. This designation appears to be redundant as the definition fits into a list of definitions in subsection (1), which contains no subparagraphs.

Triggers for conducting CDD extended (section 5)

Section 5 of the Bill requires a designated person to conduct CDD at any time that it is obliged by law to contact the customer for the purpose of reviewing relevant information about beneficial ownership, including where it is obliged to do so to seek information for tax purposes. If the beneficial owner is a senior managing official, the provision creates a new obligation on a designated person to verify the identity of the beneficial owner, maintaining formal records of actions taken and any difficulties encountered in the verification process. These amendments transpose amendments to articles 13 and 14(5) of the 4AMLD.

Electronic money (section 6)

Section 6 of the Bill[45] transposes the amendments made to art.12 of the 4AMLD.The section reduces the exemptions to CDD for low-value electronic money payments provided for in section 33A of the 2010 Act (as amended).

Electronic money payments are those which involve the use of pre-paid credit cards or equivalent online payment methods.

Under the existing legislation, an exemption from performing CDD applies in circumstances that indicate lower risk, where the issuer of the payment instrument concerned carries out sufficient monitoring of the transactions or business relationship concerned to enable the detection of unusual or suspicious transactions, and where the payment instrument:

- can only electronically store up to €250 (or €500 where limited to use within Ireland);
- can only be used to purchase goods and services;
- cannot be funded with anonymous electronic money;
- does not allow the user to redeem more than €100 in cash; and
- is either not reloadable or, where it cannot be used outside Ireland, has a monthly transaction limit of €250.

The exemption does not apply if the customer is based in a high-risk third country or if the customer is a PEP.

The new provision would reduce the €250 limits to €150, get rid of the €500 limit exemption for domestic electronic payment instruments, reduce the cash limit from €100 to €50 and add a new requirement that a transaction cannot exceed €50 if initiated via the internet or through a device that can be used for distance communication of an amount.

The section also creates an offence should a credit institution or financial institution acting as an acquirer accept a payment carried out with an anonymous prepaid card issued in a foreign state that does not fall within the exemptions.

[45] There appears to be a minor drafting error in this section, in that as subsection 33(2B) of the Act of 2010 as amended does not exist, subparagraph (a)(i) appears to be redundant. The error appears to stem from a difference in the numbering used in the General Scheme and the Bill.

Additional CDD Measures Prior to Establishing a Business Relationship (section 7)

Section 7 of the Bill imposes further CDD measures on designated persons for customers that are required to register their beneficial ownership information (corporate bodies, express trusts, financial vehicles, credit unions and unit trusts). The section requires that, prior to the establishment of a business relationship with a corporate or trust customer, a designated person must obtain ascertain that information concerning the beneficial ownership of the customer is entered on the relevant BOR. Although the expression used differs slightly from the amended art. 14 of the 4AMLD (requiring “proof of registration or an excerpt of the register”), the provision appears to adequately transpose the amendments in the 5AMLD.

Section 7 does allow for a limited exemption allowing a designated person that is a credit institution or financial institution to allow an account to be opened with it by the customer prior to conducting a BOR check so long as the designated person ensures that transactions in connection with the account are not carried out by or on behalf of the customer until the relevant BOR check is completed.

This provision would have the effect of prohibiting a designated person from acting on behalf of a company, express trust, financial vehicle, credit union or unit trust that has not registered its beneficial ownership information in the relevant BOR. This would limit the capacity of unregistered bodies to access legal services, accounting services and banking services among other things. Even the exemption implies that credit and financial institutions should freeze accounts of unregistered customers until they have been regularised.

Examination of Background and Purpose of Certain Transactions (section 8)

Section 8 of the Bill would soften the formerly strict requirement in section 36A of the Act of 2010 (as amended) for designated persons to examine the full background and purpose of all transactions which are complex, unusually large, follow an unusual pattern, or do not appear to have an economic or lawful purpose, by providing that this would only need to be done "as far as possible". Article 18 of the 4AMLD uses the phrase “as far as reasonably possible”.

Politically Exposed Persons (PEPs) and Enhanced Customer Due Diligence (ECDD) (sections 9, 10 and 11)

Section 9 of the Bill adds a new subsection requiring designated persons to continue to apply the prescribed measures to a PEP for as long as is reasonably required to consider the continuing risk posed by that person and until such time as that person is deemed to pose no further risk specific to PEPs. This requirement under art. 22 of the 4AMLD had not been included in Act of 2018.

Section 9 also expands the definition of a politically-exposed person to include any individual performing a prescribed function, and inserts a new subsection empowering the Minister for Justice and Equality to issue guidelines to competent authorities in respect of prominent public functions in the State, allowing for the transposition of art. 20a of the amended 4AMLD.

Section 10 proposes to clarify that, for the purpose of ECDD, correspondent relationships only include correspondent relationships involving the execution of payments by either a credit

institution or a financial institution, not all correspondent relationships entered into by a credit or financial institution.

Section 11 sets out several steps to be applied by designated persons in the context of ECDD on top of the other requirements specified in the Act of 2010. When dealing with a customer established or residing in a high-risk third country, a designated person must conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination. The designated person must also obtain the approval of senior management to establish or continue with a business relationship and obtain:

- additional information on the customer and the beneficial owner;
- additional information on the intended nature of the business relationship;
- information on the source of funds and source of wealth of the customer and of the beneficial owner; and
- information on the reasons for the intended or performed transactions.

Although section 11 of the Bill appears to transpose art. 18a(1) of the amended 4AMLD, it does not appear to transpose paragraph (2) and (3) of the article. The equivalent provision in the General Scheme made provision for secondary legislation to be introduced imposing additional ECDD and reporting obligations on designated persons doing business with third countries which pose a high money-laundering and/or terrorist-financing risk. Such a provision would have allowed for the transposition of the remaining part of art. 18a of the amended 4AMLD. However, these provisions were not replicated in the Bill.

Reliance on third parties to carry out Customer Due Diligence (CDD) and keep records (sections 12 and 15)

Section 12 of the Bill proposes to add a requirement that a designated person may only rely on a third party's CDD if the information includes any information from relevant trust services as set out in the Electronic Identification Regulation.

Section 15 proposes that, as part of the duty to keep records of procedures used in CDD, a designated person should keep a copy of any information obtained from relevant trust services as set out in the Electronic Identification Regulation.

Feedback from Financial Intelligence Unit (FIU) (section 13)

Section 13 of the Bill requires the FIU, where practicable, to provide timely feedback to a designated person who has lodged a STR on how the STR was treated. This provision appears to transpose art. 46(3) of the 4AMLD, which appears not to have been transposed by the Act of 2018.

The 'tipping off' defence (section 14)

Section 14 of the Bill proposes some tweaks to the tipping-off defence found in section 51 of the 2010 Act. The disclosure of information relating to suspicious transactions can only be made between credit institutions and financial institutions incorporated in the same Member State and belonging to the same group, or between institutions incorporated in a Member State and a

subsidiary or branch situated in a third country where the disclosure is made in adherence to group-wide AML/CFT policies and procedures adopted in accordance with the relevant domestic and EU legislation.

Anonymous safe-deposit boxes (section 16)

Section 16 has the effect of prohibiting credit institutions and financial institutions from keeping an anonymous safe-deposit box for a customer, transposing art. 10(1) of the amended 4AMLD.

Remits of certain competent authorities (section 17)

Section 17 expands the remit of the Central Bank of Ireland as a State competent authority to make it the competent authority for providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers. It also expands the remit of the Property Services Regulatory Authority (PRSA) to act as the competent authority of all property services providers; this seems to pull the provisions of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority and State Competent Authority) Regulations 2016* (S.I. No 453 of 2016) into the Act of 2010 – which made the PRSA the State competent authority for all property service providers. Finally, the section changes the competent authority for barristers from the General Council of the Bar to the Legal Services Regulatory Authority.

Cooperation with Member State competent authorities (section 18)

Section 18 of the Bill appears to transpose art. 50a of the amended 4AMLD by inserting a new subsection into section 63B of the Act of 2010. The new subsection confirms that cooperation between Member State competent authorities should be facilitated through the sharing of any information where it is not prevented by law. Information sharing must not be refused on any of the specified grounds.

Employment standards of competent authorities (section 19)

Section 19 of the Bill adds a new employment standard to which competent authorities must adhere. Competent authorities may only employ a person who maintains high professional standards with regard to conflicts of interest. This provision appears to transpose art 48(2) of the amended 4AMLD.

Mechanisms for reporting to competent authority (section 20)

Section 20 of the Bill requires a competent authority to establish and maintain effective and reliable mechanisms to encourage reporting of suspicious activities by designated persons falling under its remit. This includes the provision of one or more secure communication channels which can be used by designated persons for lodging reports of potential and actual breaches of the Act of 2010 and for lodging reports of threats or retaliatory or hostile actions resulting from a report. This provision appears to transpose art. 61(1) of the amended 4AMLD.

Annual reporting by competent authorities (section 21)

Section 21 requires non-State competent authorities (designated accountancy bodies and the Law Society of Ireland), when acting in their capacity as a competent authority, to include in their annual reports a statement of information regarding the measures taken by the authorities to monitor compliance with the provisions of the 2010 Act by designated persons falling under their remit.

Appeal Tribunal (section 23)

Section 23 of the Bill repeals section 101 and inserts a new section 101A into the 2010 Act, to establish a new 'Appeal Tribunal'. The Tribunal will hear appeals against certain decisions by the Minister made under the money laundering Acts. The section outlines how the tribunal is to be constituted, how members are to be appointed and the conditions of appointment. The section also provides that the new tribunal is empowered to regulate its own activities.

There is a potential **drafting anomaly** in this section. Paragraph (b) of the section provides that the new section 101A is to be inserted after section 101. However, as section 101 is repealed by the preceding paragraph some confusion may result unless the words 'section 101' are replaced with 'section 100'.

Low-Risk Factors (section 24)

Section 24 qualifies the heading 'geographical risk factors' confirming that the list of risk factors pertains to the place of registration, establishment and/or residence of customers.

High-Risk Factors (section 25)

Section 25 provides that a higher risk of money laundering and/or terrorist financing exists where:

- a customer is a third-country national who applies for residence rights or citizenship in the State in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities in the State;
- a product, service, transaction or delivery channel involves the use of non-face-to-face business relationships without the use of certain safeguards such as electronic identification means, relevant trust services or other secure, remote or electronic, identification processes that are officially regulated, recognised, approved or accepted; and
- a transaction is related to oil, arms, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare or scientific value, as well as ivory and protected species.

Contact:

Houses of the Oireachtas
Leinster House
Kildare Street
Dublin 2
D02 XR20

www.oireachtas.ie
Tel: +353 (0)1 6183000 or 076 1001700
Twitter: @OireachtasNews

Library & Research Service
Tel: +353 (0)1 6184701
Email: library.and.research@oireachtas.ie