

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

by Patrick D'Arcy

In this article, Patrick D'Arcy gives an overview of some of the changes introduced in the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018 that may affect professional accountants.

"The important thing is not to stop questioning"

Albert Einstein

The adage of Albert Einstein could be a very simplified way of summarising a key element of the Fourth Money Laundering Directive (MLD4) following its transposition into law under the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018 in November 2018.

The 2018 Act amends existing AML/CTF legislation (i.e. the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 and requires accountants, and other designated persons under the Act to implement business risk assessments. To include a record of the risk assessment undertaken and further

enhanced customer due diligence to include an understanding of the services, transaction types, delivery and operating channels, etc, and more importantly the nature and source of a customer's funds as well as identifying risks inherent in the sector or market within which the customer trades.

Report of Financial Action Task Force

In September 2017, the Financial Action Task Force (FATF) published their evaluation of the anti-money laundering and counter-terrorist financing ("AML/CTF") measures in place in Ireland arising from their on-site visit during the period 3 to 17 November 2016. The findings contained in the executive summary of the FATF Report in relation to preventative measures of designated non-financial businesses and professionals (DNFBP) and Trust or Company Service Providers (TCPS) are outlined in Chapter 5 of the FATF Report state as follows:

24. DNFBPs' understanding of their ML/TF risks are largely domestically focused. Accountants



who perform auditing services and some of the larger TCSPs have shown a better understanding of their ML/TF risks including cross-border ML/TF risks. Overall, the AML/CFT controls and process in place for DNFBPs were less sophisticated in nature and in many cases, the CDD and monitoring process are manual (although this could be appropriate in some cases where the business and customer profile are less complex).

25. The implementation of CDD (e.g. collection of beneficial ownership information and existing clients) measures by FIs and DNFBPs could be further strengthened. There are also concerns on their ability to identify, in a timely and accurate manner, relationships/transactions in relation to PEPs and designated entities in relation to TFS.

26. For some FIs and DNFBPs, there is indication that there is strong reliance on local community networks and knowledge. While this is a useful source, and could enrich customer understanding when used appropriately, it could also be subject to preconceived notions, and not always adequately supported by objective analysis. Further, such strong reliance may reduce the incentive to give adequate focus to external and cross-border factors.

27. The level of STR reporting, particularly by DNFBPs (e.g. TCSPs, PSMDs etc.), is also low.¹

The FATF Report acknowledges in the case of Ireland the understanding that designated non-financial businesses and professionals (e.g. accountants) have knowledge of a customer's business through local community networks, but this knowledge may not necessarily facilitate a similar understanding of cross-border money laundering and terrorist financing risks.

Introduction of Business Risk Assessment

One of the main aims of MLD4 is to eliminate some of this inherent risk with the introduction of a "Business Risk Assessment", which reflects the "risk-based approach" of MLD4 for Member States and designated persons to better understand and identify the type of risks that are in existence nationally and internationally.

In addition, to conducting a Business Risk Assessment, the business risk assessment must be fully documented and available to the relevant competent authority, upon request. The business risk assessment is managed and controlled by a designated person within the organisation, at pre-defined periods, and must be approved by senior management. The business risk assessment processes are in addition to the normal take-on and identification requirements and are required to assess the potential level of risk of money laundering and/or terrorist financing that may be involved in the customer's business or sector.

A designated person may be required to demonstrate compliance with the regulations as set out in the Act, and where necessary, this may include consultation with the Department of Finance's National Risk Assessment (NRA) or other guidelines issued by the European Central Bank in the case of credit and financial institutions.

Customer Due Diligence

Designated persons can carry out simplified Customer Due Diligence (CDD) where a customer or business carries a lower degree of risk of money laundering and/or terrorist financing. The litmus test for applying simplified CDD is whether a "reasonable person" would make a similar assessment of the risk. The designated person must, if requested

by a competent authority, set out its reason(s) for applying a simplified CDD to its customer or its business operations. Where necessary, the appended schedules to the 2010 Act setting out potential risk factors, the National Risk Assessment and in the case of case of credit and financial institutions, the guidelines issued by the relevant European Supervisory Authorities (i.e. EBA, EIOPA and ESMA - ESAs) should be consulted to ensure a proper assessment of potential risk(s) are understood.

There is now an obligation to carry out enhanced CDD in the case of politically exposed persons (PEPs) that are resident in Ireland as well as PEPs that are outside of Ireland. In addition, specific steps are required to be undertaken where the PEP is also a beneficiary of a life assurance policy. The threshold for making such an assessment is whether a "reasonable person" would make a similar assessment of the risk.

A designated person is required to conduct enhanced CDD when dealing with a customer or business residing in a high-risk third country, or where a relationship or transaction presents a higher degree of risk.

Monitoring and Reporting

The 2018 Act requires a designated person to monitor on an ongoing basis and to review transactions and the source of funds of such transactions in order to determine whether transactions are consistent with the designated person's knowledge of its:

- customer;
- customer's business/pattern of transactions; and
- customer's risk profile as determined by the business risk assessment.

The Act also requires the designated person to examine all unusually large or complex transactions, and unusual pattern of transactions for which

¹ FATF Mutual Evaluation Report - Anti-money laundering and counter-terrorist financing measures in Ireland – 2017, page 8



there appears to be no apparent lawful, business or economic purpose. Where such transactions are identified the designated person must increase the degree and level of monitoring to determine whether such transactions appear suspicious. A failure to do so is an offence under the Act.

The level of suspicious transaction reports (STRs) received from designated non-financial businesses and professionals is identified in the September 2017 FATF Report (extract above) as low. The Central Bank of Ireland has also identified the low level of reporting as one of its key AML/CFT priorities for 2019 and has advised firms that it would like greater importance placed on recognising the need to file STRs promptly with both An Garda Síochána's Financial Intelligence Unit (FIU) and the Irish Revenue Commissioners.

In Summary

The requirements introduced by the 2018 Act clearly enhance the existing risk-based approach to AML & CFT. The new additional requirements do not represent a significant change to the existing framework and the Central Bank of Ireland has stated that it expects firms to reflect the changes in their risk management frameworks and bring their risk assessments and

policies and procedures in line with the requirements, as outlined in the 2018 Act.

All professional accountants and designated persons should:

- review their existing AML/CFT policy to ensure it is updated to meet the requirements of the 2018 Act;
- establish and conduct business risk assessment processes with a focus and regard for published guidelines, including the NRA for Ireland;
- fully document any decision to use simplified CDD;
- introduce internal processes to assist with monitoring customer and business relationships on an ongoing basis; and
- undertake an assessment of the revised AML & CFT policies and procedures to ensure alignment with the requirements.

As stated at the beginning of this article, the important thing is not to stop questioning and this appears to be the one of the key mantras contained in the MLD4 in relation to the requirement of a designated person to monitor on an ongoing basis and to review transactions and the source of funds of its customers and of their businesses.

Footnote: This article is merely a general overview of some of the changes introduced in the 2018 Act that may affect professional accountants and should not be interpreted as legal advice. Readers of this article should consult the 2018 Act to identify the key changes introduced for all regulated financial service providers and other designated persons operating in the financial services industry.



Patrick D'Arcy,

Forensic Accountant and Director with Grant Thornton Corporate Finance Limited,

With significant experience, having led and conducted a number of high profile and complex money laundering investigations with both a national and international dimension to them.