Managing your AML Obligations

by Emer Kelly

"Gatekeepers particularly solicitors, accountants, and tax advisors who provide services such as advisory on tax and other complicated financial advisory and company and trust formation could be exploited by criminals who seek to launder the proceeds of crime or evade tax. The risks are higher in situations where these professionals do not apply comprehensive CDD procedures to identify the beneficial owner and the source of funds."

This is an extract from Ireland's Mutual Evaluation Report by FATF from 2017 and it highlights the role of the accountancy sector within the Irish Anti-Money Laundering (AML) framework. The Irish National risk Assessment listed the potentially vulnerable services provided by the sector as follows;

- Company and trust formations;
- Insolvency services;
- Providing financial advice;
- Providing tax advice;
- Handling client money;
- Managing client assets and financial accounts;
- Investment business services;
- Auditing financial statements; and
- Company secretarial services.

It also identified potentially higher risk clients as

- High net worth clients;
- Politically exposed persons (PEPs); and
- Other known potential higher risk clients, e.g. cash intensive businesses, construction or real estate transactions, suspected criminals etc.

The report states that the involvement of accountancy service providers can provide a veneer of legitimacy to illicit transactions.

In this role as gatekeeper, accountants have a vital role to play to prevent their services being used for criminal purposes including the funding of terrorism. In doing so it is essential that all accountancy firms have robust policies and procedures in place regarding money laundering and terrorist financing (MLTF). The role of the accountant, auditor and tax advisor regarding MLTF obligations is provided for by the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010. This was recently amended by the Criminal Justice (Money Laundering and Terrorist Financing) Act 2018, which gave effect to certain provisions of the Fourth Money Laundering Directive. In this article, the '2010 Act' refers to the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended by the Criminal Justice Act 2013 and the Criminal Justice (Money Laundering and Terrorist Financing (Amendment) Act 2018.

Key Changes

The key changes introduced by the 2018 legislation were as follows;

- Greater emphasis on identification of beneficial owners of businesses
- Wider definition of politically exposed persons (PEPs) to those resident in this jurisdiction. Previously under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, designated persons must carry out enhanced measures where a customer was a "politically exposed person", meaning persons holding certain political, judicial or other offices abroad. These measures must now be applied nationally.
- A requirement to apply procedures based on an enhanced risk-based approach to assess and respond to potential money laundering or terrorist financing
- Lowering the threshold for determining whether a high-value goods dealer falls under the Act from €15,000 to €10,000

Newly Published Guidance

Earlier this year CPA Ireland through CCAB-I, published guidance on the changes introduced by the 2018 legislation. This guidance is an important part of the MLTF framework to ensure that accountants remain vigilant in their dealings with clients.

If firms have not already updated their policies and procedures in this area, this guidance is a good place to start.

Key areas for developing policies and procedures

Firms must ensure that they have written and communicated policies and procedures that deal with the following areas;

Responsibility and oversight

The legislation explicitly requires firms to:

- Monitor and manage their own compliance with the 2010 Act; and
- Ensure that policies, controls and procedures adopted in accordance with the 2010 Act are approved by senior management and that such policies, controls and procedures are kept under review, in particular when there are changes to the business profile or risk profile of the firm.

In deciding what systems to install, a firm will need to consider the type,

scale and complexity of its services.

The systems should be capable of assessing the risk of a client, performing appropriate customer due diligence (CDD), monitoring clients, keeping appropriate records and enabling staff to make an internal Suspicious Transaction Report (STR) where appropriate.

The legislation requires that the business risk assessment and the firm's policies and procedures are approved by senior management.

A Money Laundering Reporting Officer ("MLRO") or other nominated officer may be appointed by the accountancy firm to manage its internal reporting procedures, taking responsibility for receiving internal STRs and making external STRs to the State Financial Intelligence Unit (FIU Ireland) and the Revenue Commissioners.

Risk based approach

An accountancy firm must have policies and procedures in place that provide for a risk-based approach to MLTF risks. A risk-based approach recognises that the risks posed by MLTF activity will not be the same in every case and so allows a firm to tailor its responses accordingly.

Risk assessment procedures must now be applied at both the client level and at the firm level and certain specified criteria must be considered.

A firm risk assessment must be conducted to identify and assess the risks of MLTF involved in the firm's business activities. The legislation requires that a firm consider at a minimum the risk factors outlined in S.30(A), Schedule 3 and Schedule 4 of the 2010 Act, e.g. the types of customers, the products and services that are provided etc. This firm risk assessment must be approved by senior management. MLTF risks at a firm level may include the possibility that the firm might:

- Be used to launder money (e.g. by holding criminal proceeds in a fund or a client money account, or by becoming involved in an arrangement that disguises the beneficial ownership of criminal proceeds);
- Be used to facilitate MLTF by another person (e.g. by creating a corporate vehicle to be used for money laundering or by introducing a money launderer to another regulated entity);
- Suffer consequential legal, regulatory or reputational damage because a client (or one or more of its associates) is involved in money laundering;
- Fail to report a suspicion of MLTF

An accountancy firm with a simple client base and a limited portfolio of services may result in a simple risk assessment for the firm – and in such circumstances a single set of policies and procedures may suffice. The risk profile of the firm should show where particular risks are likely to arise, and so where certain procedures will be needed to tackle them.

As part of the risk assessment the following should be considered;

a. the type of customer that the designated person has;

b. the products and services that the designated person provides;

c. the countries or geographical areas in which the designated person operates;

d. the type of transactions that the designated person carries out;

e. the delivery channels that the designated person uses;

f. other prescribed additional risk factors.

A risk assessment of individual clients must also be conducted and must provide for different risk categories such as: low, normal and high. Low and high-risk factors such as those set out in Schedule 3 and 4 of the Act, which include customer and geographical risk factors, must be considered.

The client risk assessment should be conducted at the start of a new business relationship and the outcome of the assessment will determine the required level of CDD required.

Customer Due Diligence

Customer Due Diligence procedures must be applied at the start of a new business relationship, at appropriate times during the lifetime of the relationship and when an occasional transaction is to be undertaken.

The components of CDD are;

- Identifying the client and then verifying their identity (i.e. confirming that identity is valid by obtaining documents or other information from sources which are independent and reliable).
- Identifying beneficial owner(s) so that the ownership and control structure can be understood and the identities of any individuals who are the owners or controllers can be known and, on a risk sensitive basis, reasonable measures should be taken to verify their identity; and
- Gathering information, reasonably warranted by the risk of money laundering or terrorist financing on the intended purpose and nature of the business relationship.

The legislation prescribes the level of CDD that should be applied in certain situations (i.e. simplified or enhanced) and a firm's risk assessment should flow through into client acceptance and ID procedures. A firm's policies should clearly identify the situations where enhanced due diligence must be applied, for example where a client is identified as a PEP.

Such procedures must consider the risk factors set out in Schedule 3 and 4 of the legislation.

Suspicious transaction reporting

An accountancy firm must make a suspicious transaction report where the firm or individual has knowledge, suspicion or reasonable grounds for suspicion of money laundering or terrorist financing arising from the firm's normal course of business.

The external reporting obligation under the legislation is to the FIU

and to the Revenue Commissioners. The report to the FIU is made via the online GoAML portal.

It is essential that firms have written and communicated internal reporting lines for such reports.

Firms and their staff should be aware of the offence of prejudicing an investigation (tipping off).

Record keeping

It is important that all records created as part of the CDD process and the business relationship are retained for five years after the client relationship ends.

Firms should also be aware of the interaction between MLTF requirements and those relating to GDPR.

Training and awareness

The Act requires that ongoing training is provided.

Training programmes should be tailored to each business area and cover the firm's procedures so that individuals understand the MLTF risks posed by the specific services and types of client they deal with.

Records should be kept detailing the attendees, dates and the topics covered.

Monitoring and supervision

The CPA quality assurance regime will monitor a CPA firm's AML compliance and will assess the adequacy of a firm's risk assessment, policies and procedures, customer due diligence processes and training. Breaches of MLTF requirements may result in regulatory action for a CPA member or firm.

Members who provide services such as book-keeping services which do not necessarily require the provider to hold a practising certificate must register separately with CPA Ireland for the purposes of the legislation.

5th AML Directive

The world of MLTF is fast paced and continues to become more complex. Legislation in this area continues to evolve to keep up. The 5th AML Directive is now due to be transposed by EU Member States by January 2020.

The areas for change include the following;

- Interconnection of national Beneficial Ownership registers
- Extension of the requirement to apply CDD at times to also include "when there is a legal duty to contact the client in the relevant calendar year to review any relevant information relating to the beneficial owners".
- Introduction of an EU list to identify PEPs
- Response to the increased use of virtual currencies
- Introduces stricter measures in relation to anonymous prepaid cards
- Requirement for Member States to establish bank and real estate registers to identify bank accounts, safe deposit boxes and the legal persons owning real estate.

Such changes will require further changes to the internal policies and procedures of accountancy firms.

Emer Kelly,
Quality Assurance Manager, CPA Ireland

As part of her role she is involved in the supervision of CPA firms for AML purposes. She has also lectured on this topic and was part of the CCAB-I working group that developed AML guidance for accountancy firms.

"formerly **mystrikeoff.ie**"

- Voluntary strike-off advertisements for only €99 plus Vat per company
- Full strike-off service for only €199 plus CRO fees (includes Vat and advert)
- Discounted rates on liquidation advertisements

Call us today for more information!
Tel: 041 981 0541
Email: info@closedforbusiness.ie