ICAEW
TECHNICAL ADVISORY SERVICE

ANTI-MONEY LAUNDERING FOR SMALLER PRACTICES

Issued April 2019
Last Reviewed April 2020

INTRODUCTION

This helpsheet has been issued by ICAEW's Technical Advisory Service to help members comply with anti-money laundering (AML) legislation and guidance. It is aimed at sole practitioners and smaller practices.

Members may also wish to refer to the following related helpsheets and guidance:

- Anti-money laundering client due diligence
- Electronic client due diligence
- Anti-money laundering compliance review checklist
- Subcontracting accountancy services
- CCAB Anti-money laundering guidance for the accountancy sector

WHAT NEEDS TO BE PUT IN PLACE?

Appointments

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR17) require the appointment of:

- A nominated officer (NO) who must be responsible for receiving internal suspicious activity reports (SARs) and making external SARs to the National Crime Agency (NCA); **and**
- Where appropriate to the size and nature of the business, a board member or member of senior management who must be responsible for the business' compliance with the UK anti-money laundering regime. This individual is typically referred to as the money laundering compliance principal (MLCP).

In smaller practices, a money laundering reporting officer (MLRO) will generally fulfil both of these roles, with their responsibilities including internal controls and risk management around AML. The MLRO will:

- Be familiar with MLR17;
- Monitor and manage compliance with MLR17;
- Have oversight of, and be involved in, AML risk assessments;
- Create and maintain the business's risk based approach to preventing ML;
- Create and maintain AML documentation;

- Develop customer due diligence (CDD) policies and procedures;
- Receive internal SARs and make external SARs to the NCA; **and**
- Establish and maintain awareness and training.

A sole practitioner with no relevant employees need not make any of the appointments above as they will be solely responsible. An employee is relevant if his or her work is relevant to compliance with MLR17 or is otherwise capable of contributing to the business' identification, mitigation, prevention or detection of money laundering. This would include client service staff but possibly not a receptionist (depending on the scope of their role). This definition is important as it has a significant impact on responsibilities - no relevant employees means less to do.

Disclosure and Barring Service (DBS) check(s)

MLR17 requires that ICAEW approves all beneficial owners, officers and managers (BOOMs) of supervised firms. As part of this, ICAEW is expected to check that BOOMs do not have a relevant criminal conviction. BOOMs (including practitioners) must therefore obtain a DBS certificate. Further guidance is available on the Criminal records checks page of the website.

Training and assessment

The AML skills, knowledge, expertise, conduct and integrity of all relevant employees and agents (for example any subcontractors used) should be assessed. This may be included as part of recruitment, appraisal, and training procedures.

AML knowledge may, for example, be assessed via a test for which the results are recorded. Similarly, regular recorded ethics training (with test questions) may be useful in assessing integrity.

AML training must include making relevant employees and agents aware of the law relating to money laundering and terrorist financing, and of the requirements of data protection, which are relevant to the implementation of MLR17. Training should also include an explanation of how the law applies to the firm, the firm's policies and procedures (e.g. those around CDD, making SARs, record keeping and data protection). It should also include guidance on red flags and other matters to look out for.

Training records should be kept to demonstrate compliance with MLR17. As a minimum, they should show the content of the training (a summary), the date that the training was given, which individuals received it and the results of any assessments.

Quality procedures

Practices must introduce a system of regular, independent reviews to understand the adequacy and effectiveness of the AML systems and any weaknesses identified. Independent does not mean external, and firms considering their quality control systems should make AML a part of this. Existing monitoring programmes can be extended to include AML, proportionate to the size and nature of the business.

A sole practitioner with no relevant employees or agents need not implement regular, independent reviews unless requested by ICAEW.

Summary

A sole practitioner with no relevant employees or agents **must**:

- Make sure they are familiar with the requirements of MLR17 to ensure continuing compliance;
- Monitor and manage their own compliance with MLR17;
- Have a DBS check carried out;
- Risk assess the practice (see below).

A smaller practice with relevant employees or agents **must**:

- Appoint a NO and MLCP (this can be the same person, usually the MLRO);
- Assess the AML skills, knowledge, expertise, conduct and integrity of relevant employees and agents;
- Train relevant employees and agents;
- Regularly review AML systems;
- Carry out DBS checks on owners, officers and managers of the practice;
- Risk assess the practice (see below).

FIRM-WIDE RISK ASSESSMENT

MLR17 requires firms to take appropriate steps to identify and assess the risk of money laundering and terrorist financing to which they are subject.

Further information is available in Chapter 4 of the CCAB guidance and in the Firm-wide risk assessment methodology guidance.

CUSTOMER DUE DILIGENCE

Before entering into a business relationship

Customer or client due diligence (CDD) should be completed before entering into a business relationship. The purpose of CDD is to know and understand a client's identity and business activities and then using this knowledge and understanding, assess the risk that the client might be involved in money laundering, or want to use the firm to help it launder money. The process has three stages which should be formally documented:

1. **Identification** (information gathering)
   This stage involves gaining an understanding of who the client is. It requires the gathering of information about a client's identity and the purpose of the intended business relationship. Information may be gathered from a range of sources, including the client.

   For an individual, information gathered should include their full name, date of birth and address. For a body corporate (e.g. a company) information gathered should include the name of the body corporate, its company (or other) registration number, the address of its registered office, and if different, its principal place of business.

In the case of corporates and other organisations, identification also extends to establishing the identity of the directors and anyone who ultimately owns or controls the client (beneficial owners).

2. **Risk assessment**
   This stage involves performing a risk assessment to assess the AML risks associated with each client. For example:

   - Do they operate a cash-based business (and therefore may be at risk of income tax or corporate tax evasion)?
   - Do they operate in a location unfamiliar to the firm (this doesn't just mean an overseas location, a different part of the UK may still be unfamiliar)? If so, why have they chosen the firm to provide services rather than a firm more local to them?
   - Are they requesting services that present higher AML risk e.g. creating complex corporate structures, aggressive tax avoidance, or working from incomplete accounting records?

   The ICAEW guidance on Circumstances where there might be a high risk of money laundering or terrorist financing may assist in performing the risk assessment.

3. **Verification**
   This stage involves validating (with an independent, authoritative source), on a risk sensitive basis, that the identity is genuine and belongs to the claimed individual or entity.

   Where the client is a company, unregistered company, LLP or an eligible Scottish partnership, verification requires checking the information gathered against the register of people with significant control.. Any discrepancies should be reported to the registrar. Details on how to make a report are available in the Companies House guidance Report a discrepancy about a beneficial owner on the PSC register by an obliged entity.

Further guidance on CDD is available in Chapter 5 and Appendix C of the CCAB guidance and the helpsheets Anti-money laundering client due diligence (CDD) and Electronic client due diligence. The ICAEW Library & Information Service also offers a client screening service.

Ongoing CDD

Firms also have an obligation to carry out ongoing CDD on their clients. This involves the scrutiny of client activities (including sources of funds if necessary) to make sure they are consistent with your knowledge and understanding. Given how much existing information could already be held, ongoing CDD may require the collection of less new information than was required at the outset of the business relationship.

Ongoing CDD can be event driven or periodic. Events prompting a CDD update include:

- a change in beneficial ownership of the client or key office holders;
- a change in the service provided to the client*;*
- information that is inconsistent with the your knowledge of the client;
- a previously stalled engagement restarting;
- the participation of a politically exposed person (PEP) (see below);
- a significant change in the client's business activity (including operations in new countries); **and/or**
- causes for concern (for example where you doubt the accuracy of information provided).

There is no specific timeframe for when periodic reviews should be carried out*.* The frequency of up-dating should be based on the risk assessment and should reflect knowledge of the client and any changes in its circumstances or the services it requires.

Enhanced due diligence (EDD)

Higher risk engagements should be subject to EDD, for example where a client is established in a high-risk third country, the client is a PEP, or transactions are complex, unusual, or have no apparent economic or legal purpose.

All EDD **must** include:

- Examining the background and purpose of the engagement; and
- Increasing the degree and nature of monitoring of the business relationship, including greater scrutiny of transactions.

EDD on a PEP **must** include:

- Obtaining senior management approval for the relationship;
- Taking adequate measures to establish sources of wealth and funds; **and**
- Conducting enhanced monitoring of the ongoing relationship.

EDD in response to a client in a high-risk third country **must** include:

- Obtaining additional information on the client and beneficial owner;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining additional information on the source of funds and source of wealth of the client and the client's beneficial owner (see Source of wealth factsheet);
- Obtaining information on the reasons for transactions;
- Obtaining approval of senior management for establishing or continuing the business relationship; **and**
- Conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Further information can be found in Chapter 5 of the CCAB guidance and FCA guidance FG17/6: The treatment of politically exposed persons for anti-money laundering purposes.

EDD **may** also include:

- Seeking additional independent, reliable sources to verify information;
- Taking additional measures to understand better the background, ownership and financial situation of the client, and other parties relevant to the engagement; **and/or**
- Taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship.

It is possible to rely on CDD carried out by another firm with their written agreement. Further information can be found in Chapter 5 of the CCAB guidance.

CDD records must be kept for five years following the end of the business relationship and must be readily retrievable.

Summary

All practices **must**:

- Perform and document CDD when entering into business relationships with clients and on an ongoing basis;
- Perform EDD in certain circumstances including when dealing with a PEP and when dealing with a client established in a high-risk third country;
- Keep CDD records for five years following the end of the business relationship.

SUSPICIOUS ACTIVITY REPORTS (SARS)

Practices must have internal reporting procedures that enable relevant employees to disclose their knowledge or suspicions of money laundering or terrorist financing. Where appropriate, relevant employees make a SAR to the NO/MLRO. The NO/MLRO would then consider the SAR and the need to make an SAR externally to the National Crime Agency (NCA).

A SAR is usually required if information comes to you in the course of your business in a regulated sector that gives you a suspicion of a crime with proceeds (guidance is available in the helpsheet Suspicious activity reports (SARs) and Chapter 6 of the CCAB guidance). Suspicion is subjective. Only you can decide if you are suspicious or not. Suspicion fall short of actual knowledge or evidence, but is more than mere speculation.

If you have a valid basis for making a SAR, this would not be a breach of confidentiality or GDPR as there is legal obligation to make the report.

You must not tell the client that you are suspicious or that you will make or have made a SAR as this may constitute tipping off (see Anti-money laundering tipping off). No tipping off offence is committed when enquiries are made of a client regarding something that properly falls within the normal scope of the engagement or business relationship. For example, if a business discovers an invoice that has not been included on a client's tax return, then the client should be asked about it.

IF IN DOUBT SEEK ADVICE

ICAEW members, affiliates, ICAEW students and staff in eligible firms with member firm access can discuss their specific situation with the Ethics Advisory Service on +44 (0)1908 248 250 or e-mail ethics@icaew.com.

For further details members are invited to telephone the Technical Advisory Service **T** +44 (0)1908 248250. The Technical Advisory Service comprises the technical enquiries, ethics advice and anti-money laundering helplines. For further details visit icaew.com/tas