Insolvency Practitioners Association

APRIL 2024

Anti-Money Laundering and Counter-Terrorism Financing:

Guidance for IPA Members on requirements under The Money Laundering, Terrorist Financing & Transfer of Funds (Information on the Payer) Regulations 2010 ('MLR17') and specific matters relating to insolvency

Contents

1. INTRODUCTION

The Money Laundering, Terrorist Financing & Transfer of Funds (Information on the Payer) Regulations 2017 ('MLR17') were introduced in March 2017 and have been subject to regular amendments.

MLR17 applies to persons who carry on business in the 'regulated sector'. This includes acting as an Insolvency Practitioner ('IP') as per S388 of the Insolvency Act 1986 and Article 3 of the Insolvency (Northern Ireland) Order 1989.

Under MLR17, the IPA is listed as a Supervisory Authority ('SA') to monitor compliance with MLR17. You may be regulated by the IPA as an IP but the IPA does not act as your SA. As part of the IPA's licence renewal work each year, IPs are asked to confirm who it is considered supervises your firm for AML purposes. The IPA reviews the information and liaises with the other SA's to confirm the position.

As part of the IPA's role as a SA, the Secretariat has a dedicated section of the IPA website which provides members with guidance, resources to assist with AML work, detail on AML risk and information on reporting money laundering suspicions. The 'AML Hub' can be reached on the IPA website.

Updates on Anti-Money Laundering ('AML') issues will be circulated to members via the IPA newsletter, as well as the AML specific newsletter the IPA publishes three times a year and the usual platforms. The IPA also ran our first AML & Fraud Conference for IPs in September 2023, and this will be held annually.

The IPA has also set up a dedicated e-mail address to deal with AML queries from our members. The email is aml@ipa.uk.com.

This guidance is designed to assist IPs and members with details of what is expected under MLR17 and is to support the appendix to the CCAB guidance which highlights specific AML issues in relation to insolvency matters. This guidance is issued by the IPA as a supplement to the CCAB appendix and is not to be treated as formal regulatory and/or legal guidance or advice.

Members should also continue to seek assistance from their own compliance teams and colleagues who deal with AML matters (where applicable).

2. NOMINATED OFFICER(S)

Under Regulation 21 of MLR17, you must have a nominated officer who acts for the firm in relation to Money Laundering matters. The Nominated Officer is more commonly known as the Money Laundering Reporting Officer ('MLRO').

The MLRO should have sufficient seniority, a sound understanding of MLR17 and be able to access all relevant information to assist in their role and with disclosures to the National Crime Agency ('NCA').

The MLRO should have their appointment confirmed in writing, and notification of the identity of the MLRO should be sent to your SA within 14 days of their appointment.

It is recommended that a deputy MLRO should also be appointed to ensure continuity in the role and that there is a clear job description and responsibilities expected of the MLRO/Deputy MLRO.

Depending on the size of your organisation, the board/partners/managers must create a culture that promotes, supports and resources the MLRO and Money Laundering work.

Dependent on the size of your organisation, Regulation 21 states that a member of the Board or equivalent management body must be appointed to work with the MLRO, ensure that the board/managers/partners are provided with reports on Money Laundering issues and help embed good compliance with the MLR17 in your firm. This person is commonly known as the Money Laundering Compliance Officer ('MLCO').

Again, should an MLCO be appointed, their details should be provided to your SA within 14 days of appointment.

Specific training for the MLRO (and appointed deputy and MLCO) which outlines their role and responsibilities should be provided and details included on the AML training log for the firm (see section 10 for further details on AML training).

3. FIRM RISK ASSESSMENT

Under Regulation 18 of MLR17, you are required to produce a written risk assessment which identifies and assesses the risk to your business from Money Laundering and Terrorist Financing.

Members should note that insolvency was highlighted as a high-risk environment by the Financial Action Task Force ('FATF'), and OPBAS have stated that they also consider insolvency as having a high risk and this should be considered when setting-up or reviewing the written risk assessment.

You should consider and account for:

- Your clients and client base
- Any geographical areas in which you operate
- What products/services you are offering and to whom
- How you conduct transactions
- Size and nature of your business

This will require an understanding by your MLRO and/or MLCO as to your business, i.e. what types of appointment you seek (is it purely corporate insolvency, for example), whether you also act in turnaround and restructuring or general debt advice.

An understanding will also be required of whom you act for – do you act for clearing banks, directors, debtors, creditors, asset finance companies, factors etc.

You should also understand where your client, or potential clients, are based. Do you have any clients who live overseas? Is the beneficial owner of a corporate client based overseas – which may lead you to consider that there is a higher risk in respect of those aspects of your work.

Also consider any potential clients who are based or trade at a distance from your firm's offices. Is there a reason why they are seeking the appointment of an IP who is not more local to their operations?

A risk assessment of your business will assist in:

- Developing effective policies and procedures for your firm and work that you undertake
- Helping consider and apply an effective risk-based approach to detecting and preventing Money Laundering and managing and mitigating risks from appointments
- Helping to ensure that training is provided which explains and deals with areas of risk notified
- Inform your assessment of risk associated with certain areas of work, or with clients for which you undertake work and to take an informed risk-based approach on client engagement

You should ensure that you keep an up-to-date record of the steps you have taken to produce your risk assessment and consider any steps that you may take to mitigate the risks of Money Laundering

and Terrorist Financing for your firm.

You should also keep the risk assessment under regular review and be prepared to provide a copy to your SA on request.

Members should also identify and assess the risks to your business from proliferation financing as outlined under Reg 18A.

Proliferation Financing is 'the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.'

The matters to be considered are the same as required for the general assessment of risk under Reg 18 – customers, countries/geographic areas, products or services, transactions and delivery channels.

The IPA undertake an annual review of a random sample of Reg 18/18A firm risk assessments where the IPA is the relevant SA. If any issues are noted, urgent corrective action will be required to be undertaken to ensure that your risk assessment is compliant with Regulation 18/18A.

4. CASE RISK ASSESSMENTS – CUSTOMER DUE DILIGENCE

Regulation 27 of MLR17 requires Customer Due Diligence ('CDD') to be undertaken when you are establishing a business relationship, carrying out an occasional transaction, suspect Money Laundering or Terrorist Financing, or doubt the veracity or adequacy of documents or information provided for CDD purposes.

Regulation 28 requires you to assess and obtain information on a prospective client and in relation to the work that is to be undertaken.

You should consider the purpose and nature of any engagement as well as the assets and proposed transactions and consider the risk in respect of each engagement with reference to your firm's risk assessment.

Regulation 28 advises that CDD is a three-stage process and that a relevant person (i.e. an IP) must:

- Identify the client - including taking reasonable steps to identify beneficial owners
- Verify their identity by obtaining documents – you should obtain photographic identification and proof of address dated within the last three months. Where appropriate, you should request additional documentation
- Assess, and where appropriate obtain information on, the purpose and intended nature of the business relationship

The third part of CDD is where the IPA finds there is a shortfall in compliance. CDD should be considered in light of information obtained as part of the information gathering process and also should take into account the high-risk indicators from the firms Reg 18 firm-wide risk assessment.

You must be able to evidence an understanding of the 'worth' of the company/individual. Are you satisfied you understand how major assets were funded? This is of particular importance in MVL cases where the main asset is usually cash at bank. Ensure that you understand where the funds in the account originated from. Are you satisfied the funds were from legitimate trading or asset sales?

For a corporate client, or where you are acting in relation to a corporate insolvency, you should obtain and verify the name of corporate body, company number and registered office address and principal place of business.

Obtain a copy of the Persons of Significant Control ('PSC') Register – remember under the 5th Money Laundering Directive where the information held on Companies House as to the PSC differs from the details that you have obtained or been provided with, you have a duty to report any material discrepancy to Companies House.

Businesses may choose electronic identification processes either on their own, or in conjunction with other paper-based evidence to assist in CDD work. Firms must understand the basis of the systems they intend to use and gain assurance that the information provided to them is reliable,

comprehensive and accurate.

Where the corporate body is not listed on a regulated market you should also be taking steps to determine and verify:

- The constitution of the corporate entity (articles of association etc.)
- Law under which it operates
- Full names of the board of directors and senior people who are responsible for operations
- Confirm and identify the name of the beneficial owner and ensure that their identity is verified
- If the beneficial owner is another company or a trust etc., ensure that you understand the ownership and control structure
- If the corporate body is owned by another person, you must identify the owner(s) and take reasonable measures to verify their identity, so you are satisfied as to the ownership structure.

If an IP is appointed over a corporate body which is not listed on a regulated market Regulation 43 allows you to request that the corporation provides you with the information required to verify their identity.

CDD must be undertaken before the establishment of a business relationship. It is recommended that CDD is completed prior to signing any letter of engagement or taking on an appointment and must be completed prior to accepting funds.

Whilst Regulation 30(3) allows verification to be completed after contact is first established, this should be in very limited circumstances. The Appendix – Guidance for Insolvency Practitioners from CCAB advises at p F.3.5 that the circumstances would be a hostile/emergency appointment.

The guidance is also clear that an initial client identification and assessment of risk must be completed before consenting to act and reviewed subsequent to appointment. Sufficient information should be gathered to allow a general understanding of the identity of the debtor, company officers and beneficial owners of the entity including information about what the business did and where it traded. The information will allow for the risk of money laundering to be assessed before the completion of full CDD.

The guidance advises that in these circumstances and other relevant cases – such as appointments obtained via a decision procedure where you were the alternative IP nominated – that CDD should be completed as soon as reasonably practicable on appointment and the measure of five working days is advised a reasonable.

Instances where assets are dealt with, or funds are held prior to the completion of due diligence work must be avoided.

You should ensure that all staff are aware of the policy on CDD and able to complete the required identification and verification.

If MLR17 does not apply, it is recommended that CDD checks are still undertaken.

5. CASE RISK ASSESSMENT – ENHANCED DUE DILIGENCE

Regulation 33 deals with Enhanced Due Diligence ('EDD') requirements and when EDD is required.

EDD is required when:

- You identify a high risk of Money Laundering or Terrorist Financing from the risks highlighted in your firms Reg 18 firm-wide risk assessment
- The proposed appointment relates to a high-risk indicator as provided in guidance from your SA
- The business relationship or a transaction is with a person in a high-risk third country as per Sch3ZA MRL17. (You should ensure that you review the guidance issued on countries with unsatisfactory AML controls from FATF – www.fatf-gafi.org as well as the HM Treasury Sanctions List if there are concerns)
- If there are concerns regarding a client or potential client being a Politically Exposed Person ('PEP') (see 6 below for further information)
- A transaction is unusually large or complex – this can be in relation to a transaction that you uncover during your SIP2 enquiries that is outside the usual business of the company for example

There are further details on when EDD is required and steps to take at Regulation 33(6), which should be reviewed if the circumstances require.

In relation to insolvency work, EDD should be undertaken:

- Where a debtor, company or beneficial owners are subject to criminal or civil proceedings
- If cashflow issues with the business indicate the possibility of fraud or dishonesty
- Where the debtor, company or beneficial owners are in a high-risk country or area
- Where the location of assets is in a high-risk area
- When payments are being asked to be made to a location that is a high-risk area
- Where there is no personal contact or personal contact is being avoided

These lists are not exhaustive and you should consider where you believe EDD is required depending on your firm's risk assessment and the nature of the engagement.

6. POLITICALLY EXPOSED PERSONS ('PEPS')

PEPs not only include a politically exposed person, but a family member or close known associate of a PEP.

You are required to ensure that your risk systems and checks are able to determine if a potential client or beneficial owner is a PEP and if so, that you are able to assess the level of risk and what EDD measures are required to be applied to that client. For example, you should ensure that if you use electronic verification that the system is able to search for and flag potential PEP matches for review.

Regulation 35 provides for further measures to undertake if there is a PEP in place and these include:

- Approval from Senior Management for establishing and/or continuing the relationship
- Establishing the source of wealth/funds involved with the PEP and in relation to any transaction
- Continuing EDD with the PEP and the relationship

7. CASE RISK ASSESSMENT – SIMPLIFIED DUE DILIGENCE

There are occasions when you may apply Simplified Due Diligence ('SDD'). This is where you determine that there is a low risk of Money Laundering or Terrorist Financing in relation to a business relationship or transaction.

You must still consider the CDD requirements under Regulation 28 and ensure that you keep the matter under review.

Regulation 37(3) provides matters to take into account, and consider to assess, whether there is a lower risk of Money Laundering or Terrorist Financing. However, one or more of the points listed is not indicative or proof that a lower risk applies, and a written assessment and conclusion of any decision must still be held on file.

8. RELIANCE

A relevant person (i.e. an IP) may rely on another relevant person to apply any CDD measures required under MRL17.

Reg 39 advises that if you are to rely on a third party to complete CDD, you remain liable for any failure to apply proper CDD measures. This may be important if there is reliance on your solicitor to complete CDD on the sale of a significant/valuable asset. Are you satisfied that proper CDD was undertaken on the purchaser/origin of funds?

If you are going to rely on another relevant person to apply CDD you must:

- Immediately obtain from the third party all the information needed to satisfy the CDD requirements, and,
- Must enter into arrangements with the third party which enable you to obtain immediately on request copies of any ID & verification date and other relevant CDD documentation and require the third party to retain copies of the documents for a period of 5 years from when the business relationship has come to an end

Where there is reliance on another relevant person, you must still carry out a risk assessment and perform ongoing monitoring.

IPs should proceed with caution if asked to perform CDD for another party and ensure that your client and any other relevant third parties are aware that disclosure may be made to another party and has no objection to disclosure.

9. POLICIES, PROCEDURES & CONTROLS

It is important that you have established written policies, written procedures and controls in place to effectively manage the Money Laundering and Terrorist Financing risks identified in your risk assessment and that the policies, procedures and controls can effectively mitigate such risks.

Any policies, procedures and controls should be proportionate to the size of your business and the nature of work that you undertake but must be approved by the senior management of your firm as set out under Regulation 19.

You should ensure that all policies and procedures are communicated effectively around your teams so that they are aware of the firm's requirement in dealing with the risks of Money Laundering and Terrorist Financing. In addition, all policies and procedures should be subject to regular review, with any updates effectively communicated to all team members.

Regulation 19 advises what should be covered by any policies, procedures and controls, but these must cover:

- Risk management practices
- Regulation 21-24 controls (see further detail below)
- How CDD is carried out
- Reporting and record-keeping
- How Suspicious Activity Reports ('SAR') and disclosures to the National Crime Agency ('NCA') are dealt with
- Monitoring, communicating and managing compliance with internal policies
- Identification and EDD for large, complex and high-risk areas of work

It is recommended that a risk-based approach is taken. You should focus resource and work on where your firm's risk assessment indicates that the greatest threat from Money Laundering and Terrorist Financing may occur.

Regulation 19A has now been introduced. This requires the consideration of having the policies and procedures to also manage, and mitigate effectively, the risks of proliferation financing identified in any risk assessment undertaken under Reg 18A (see above for details).

Controls as per Regulation 21 are internal controls, which allow for an audit of your Money Laundering policies and procedures to test and consider their effectiveness. The audit does not have to be external, but it should be independent of the function being reviewed (where possible).

The appointment of an MLCO (as per part 2 of this guidance) may be an effective internal control – should the size of your firm allow an appointment to be made.

An internal control is also the screening of relevant employees appointed before and during the appointment.

10. REPORTING SUSPICIONS OF MONEY LAUNDERING OR TERRORIST FINANCING & TIPPING-OFF

SARs are the main defence to involvement in a potential Money Laundering offence under the Proceeds of Crime Act 2002 ('POCA'). It is therefore of high importance to you and your staff that you should have internal policies and procedures which provide all staff with the process for how to raise and report suspicions of Money Laundering or Terrorist Financing.

It is recommended that your MLRO familiarize themselves with the NCA's guide to SARS submission and remember including Glossary Codes as part of any SAR to assist the NCA with their review of the intelligence provided.

It is important to ensure that all staff are aware of the requirement and that if they fail to report suspicions, there is the potential for them personally to be subject to action which could lead to a fine or imprisonment, or both.

Staff should also be advised about the ability for your MLRO to request a 'Defence Against Money Laundering' ('DAML') as part of any SAR report.

A DAML is a request made to the NCA for consent to proceed with a transaction or course of action for which the SAR has been lodged. If consent is granted by the NCA, or there has been no response to a DAML within seven working days of receipt by the NCA of the request, the transaction can then proceed.

If consent is withheld, you may be prevented from completing the transaction for up to 31 calendar days (and the NCA can extend this by a further five 31 calendar day periods). It is important that your MLRO has a policy in place for how to deal with such an eventuality, which avoids tipping-off the subject of the SAR.

You should also ensure that your MLRO is able to securely hold details of SARs or DAMLs reported to the NCA and that access to those details is limited.

It is also important that if a SAR or DAML is lodged with the NCA, a copy of the details provided to the NCA is not kept on the case file, nor should any note that a SAR has been lodged with the NCA be kept on the case file as this could result in a third party inadvertently tipping-off the person, or persons, that a SAR has been submitted.

Again, it is recommended that your internal policies highlight to all staff the importance to avoid tipping-off due to the potential personal penalties that could be levied against someone for tipping-off.

11. TRAINING

Training continues the requirement from the 2007 Regulations to ensure that appropriate measures are made to ensure that staff are made aware of the law and regulations relating to Money Laundering and Terrorist Financing. It also demonstrates how they can recognise and deal with transactions and other areas where Money Laundering and Terrorist Financing may occur.

All staff should also receive training that ensures that they are aware of internal policies and procedures and where they can obtain copies of any policies and procedures.

You should ensure that a written record is kept of all training provided – particularly when the training was provided, the type of training, who received the training and any test score (where this is relevant).

There is no recommendation of what training should be given, but you should consider the size of your business and nature of the work undertaken and whether seminars, on-line sessions, conferences etc. work best to communicate and provide all staff with the appropriate information to comply with the Regulations and internal policies and procedures.

As advised at part 2 above, specific training on the role and responsibilities of the MLRO, any appointed deputy and any appointed MLCO should also be provided to the individuals who hold these roles and included as part of the firm's AML training log.

The IPA also recommends that training provided is tested for its effectiveness and to consider if there are any gaps in knowledge where further training may be required.

12. RECORD KEEPING

You are required to keep records for a period of five years from the date that the business relationship is considered to be complete and/or the transaction which applies to records kept has been completed.

At the end of the five-year period, you must ensure that all personal data obtained for the purposes of MLR17 is destroyed unless you are required to maintain such records (under any enactment of Court proceedings) or you have specific consent to retain the data.

Regulation 41 has further details regarding data protection and MLR17.

You should have a written policy regarding records to be kept in respect of physical and electronic records and who would be able to have access to such records.

Records that you may wish to keep and cover in your policy are:

- Appointment of an MLRO and where relevant an MLCO
- PEP form
- MLRO query log
- SARs – internal reporting form
- Training records and log
- Compliance monitoring forms
- Enhanced compliance monitoring forms
- Annual and other reports to senior management

This list is not exhaustive and the records you wish to keep will depend on your internal policy and the size and nature of your business.

These records can form the basis of a defence against accusations of failing to carry out duties under POCA and the 2017 Regulations. Businesses should consider their retention policies taking into account both data protection and the potential for law enforcement contact.