Insolvency Practitioners Association

AUGUST 2019

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
2. Nominated Officer(s)
3. Firm risk assessment
4. Case risk assessment – Client Due Diligence ('CDD')
5. Case risk assessment – Enhanced Due Diligence ('EDD')
6. Politically Exposed Persons ('PEPs')
7. Client risk assessment – Simplified Due Diligence ('SDD')
8. Policies, procedures and controls
9. Reporting suspicions of Money Laundering or Terrorist Financing and Tipping-Off
10. Training
11. Record Keeping
12. Insolvency Specific Matters

1. INTRODUCTION

The Money Laundering, Terrorist Financing & Transfer of Funds (Information on the Payer) Regulations 2017 ('MLR17') were introduced in March 2017.

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 Insolvency Practitioner ('IP') but the IPA does not act as your PBS. As part of the work in registering and approving beneficial owners, officers, managers ('BOOMs') in June 2018, you would have been advised as to whether the IPA acts as your SA.

As part of the IPA's role as an SA, the Secretariat have provided a strategy on how the IPA will deal with our role as an SA. This has been published on the IPA website.

Updates on Anti-Money Laundering ('AML') issues will be circulated to members via the IPA newsletter and the usual platforms.

The IPA has also set up dedicated e-mail addresses to deal with AML queries from our members – amlhelpline@ipa.uk.com. To raise any AML specific complaints, email amlcomplaints@ipa.uk.com.

Complaints will be treated confidentially and in line with the IPA Whistleblowing Policy.

This guidance is designed to assist IPs and members with details of what is expected under MLR17 and is to support the upcoming appendix to the CCAB guidance which will highlight 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.

The first 11 chapters cover general matters which apply to all members. Chapter 12 looks specifically at issues that arise in relation to insolvency matters and looks to assist members who deal with insolvency assignments whilst the CCAB appendix is finalised.

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

The guidance will provide some detail on what is expected from IPs and members under MLR17 and also provides guidance on matters that may assist with applying MLR17 to insolvency work.

A separate guide will be published to provide information on what members can expect to be reviewed by our Inspectors when they undertake regulatory visits, both in cases where the IPA is your SA and where the IPA is not your SA.

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, have 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 PBS 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 clear job description and responsibilities expected of the 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.

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.

A risk assessment of your business will assist in:

- Developing policies and procedures for your firm and work that you undertake
- Helping consider and apply a risk-based approach to detecting and preventing Money Laundering
- 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 undertaken 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.

4. CASE RISK ASSESSMENTS – CLIENT DUE DILIGENCE

Regulation 27 of MLR17 requires Client Due Diligence ('CDD') 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.

CDD details were more commonly known as the 'Know Your Client' ('KYC') requirement, but these have been enhanced under Regulation 33.

You should identify and verify all new clients. To identify the client, obtain proof of their identity (passport, driving licence as well as current utility bill for example).

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.

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.

You should also utilise Regulation 43, which imposes a duty on a corporate body which is not listed on a regulated market to provide you with the information you require to allow the client to be identified and verified.

CDD must be undertaken before the establishment of a business relationship. Whilst Regulation 30(3) allows verification to be completed after contact is first established, this should be in very limited circumstances. This is possibly only where there is a hostile appointment, or an emergency

appointment is requested.

It is recommended that CDD is completed prior to signing any letter of engagement or taking on an appointment. Initial client identification with an initial assessment as to the risk of the assignment should be undertaken, reviewed and updated subsequent to the appointment.

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
- The business relationship or a transaction is with a person in a high-risk third country (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
- Transactions appear to have little economic or legal purpose

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.

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. POLICIES, PROCEDURES & CONTROLS

It is important that you have established written policies, written procedures and controls in place in order 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 what is required by them and the firm in dealing with the risks of Money Laundering and Terrorist Financing, and 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 and you should consider focusing resource and work on where your firm's risk assessment indicates that the greatest threat from Money Laundering and Terrorist Financing would occur.

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.

9. 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') and 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 who to report suspicions of Money Laundering or Terrorist Financing to.

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 SAR' ('DAML SAR').

A DAML SAR 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 SAR 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), so 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 DAML SARs reported to the NCA and that access to those details is limited.

It is also important that if a SAR or DAML SAR 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.

10. 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, as well as 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 and who received the training.

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. However, it is recommended that training is made mandatory.

11. 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.

12. INSOLVENCY SPECIFIC MATTERS

The previous information provided general guidance on MLR17 to assist with your work managing and mitigating general risks from Money Laundering and Terrorist Financing. While we have written it from an insolvency perspective, much of it could also be applied to other businesses operating in a financial setting.

The checklist below lists points for Money Laundering matters as they may impact specifically on insolvency-only work and engagements. This guidance is being issued as the Insolvency Appendix to the CCAB guidance is being finalised and is yet to be released. This part of the guidance will be reviewed when the Appendix has been approved and published.

The CCAB Appendix will be published and details released to members as soon as the guidance has HM Treasury approval. Members should be aware that a draft has been finalised by the RPBs and Insolvency Service and is undergoing a legal review prior to being sent to HM Treasury for approval. It is hoped the CCAB appendix will be issued by the end of 2019. Updates will be provided to members on the progress of publication.

This guidance will be designed to assist you with your work regarding Money Laundering risks and considerations in respect of insolvency work. It is not formal regulation and you should continue to review and consider matters with your MLRO/MLCO, your compliance officers/agents and team members to ensure that your policies and procedures deal with the risks from Money Laundering and Terrorist Financing that you have identified in your firm's risk assessment.

As this is not formal regulation and is not subject to agreement with the other RPBs, this guidance, whilst designed to assist members with consideration as to the risks and issues that arise from MLR17, should not be treated as such formal regulation/legal guidance or advice.

This part of the guidance should be read in conjunction with the published general CCAB Guidance, which is available on the IPA website.

It is expected to see CDD documents in relation to the following appointments/matters:

- Agreeing to act as a Liquidator in a solvent or insolvent company or LLP
- Agreeing to act as provisional Liquidator of a solvent or insolvency company or LLP
- Agreeing to an appointment as Administrator or Special Administrator
- Agreeing to accept the appointment as Administrative Receiver
- Agreeing to accept an appointment as a Receiver in Scotland
- Agreeing to act as a Nominee or Supervisor in an IVA
- Agreeing to act as a Nominee of Supervisor in a CVA where the CVA is not preceded by another insolvency appointment
- Agreeing to act as a Trustee or Interim Trustee in a Bankruptcy, Sequestration or a Trust Deed
- Accepting an instruction to prepare, or assist in the preparation of a proposal for a CVA or IVA where appointment as Nominee is to be sought

- Agreeing to act as Liquidator, Provisional Liquidator or Administrator of an insolvent partnership
- Agreeing to act as Trustee of a Partnership under Article 11 of the Insolvent Partnerships Order 1994
- Agreeing to act as Nominee or Supervisor in relation to a Partnership Voluntary Arrangement ('PVA')

It is paramount that IPs must consider each case over which an appointment is to be made individually on its own terms as to the assessed risk of Money Laundering/Terrorist Financing and ensure that sufficient checks to consider that risk are carried out.

File notes to confirm the case risk assessment and the work carried out to arrive at the case assessment are highly recommended to be made and held on the case file. It is also important that the case risk is reviewed throughout the appointment.

Further details on CDD

Where CDD cannot be completed before taking office, sufficient information should be gathered to enable you to form a general opinion and understanding of the entity over which the appointment is to be made. This can include details from on-line sources for example – but you should ensure that the information is reliable and current.

It is understood that CDD could not be completed in cases such as where an appointment is made at a decision procedure where an alternate IP is nominated or by a creditor's petition. It is recommended that CDD is completed as soon as practicable after appointment, and this would be expected to be within five working days of appointment. Information may be obtained again from on-line sources or prior office-holders.

Appointments from Court, Accountant in Bankruptcy ('AiB') or Secretary of State

As these appointments tend to be with no prior involvement with the insolvent, reliance can be placed, in part, on the order of appointment or initial Court Order to identify the insolvent.

This will not remove the requirement to consider the identity of the beneficial owner of the entity or the need to consider whether Money Laundering activity has taken place prior to your appointment. You should therefore take appropriate steps to ensure that you are confident that the identity of the individual, corporate entity and/or beneficial owner is, or can be, adequately confirmed and that there is sufficient information to be able to carry out a case risk assessment.

It should also be noted that whilst MLR17 places no requirement on the Official Receiver to carry out CDD checks on a bankrupt, in respect of a debtor's petition, the adjudicator does undertake enquiries to confirm the identity of the applicant. Unless you can obtain copies of the verification work undertaken by the adjudicator, you may want to consider undertaking your own CDD checks to confirm that you are content that you hold sufficient detail to verify identity and to complete a case risk assessment.

The requirement to keep the risk under review throughout the appointment will also remain in place.

If you undertake an appointment as a Receiver in Scotland, or as an Administrative Receiver or Administrator under an appointment from a bank or institution itself subject to MLR17, you may be able to obtain the CDD undertaken by the institution for use in your own CDD checks. This should be obtained as soon as reasonably practicable.

You must satisfy yourself that the details you obtain provide sufficient detail and evidence of identity to assess the Money Laundering risk for the assignment, and you must carry out further CDD checks as necessary to allow the risk to be fully considered and evidenced.

Asset sales

In Bankruptcy, Sequestration and Trust Deed appointments, assets of an insolvent vest in the IP and asset sales are conducted by the IP as principal. As an IP is a relevant person within a regulated sector, the occasional transaction provision should be applied and CDD conducted on purchasers of assets for transactions amounting to €15k or more.

For appointments as Liquidator, Administrator, Administrator or other Receiver, or Supervisor of an IVA or CVA, your business relationship is with the debtor or entity over which you have been appointed and not the purchaser of assets.

Any appointment over an unregulated entity does not change the nature of the business of the debtor or entity. This means that if the insolvent entity was not regulated prior to the appointment, they are not a regulated entity due to the appointment of an IP. This means that the routine CDD checks of asset purchasers is not required.

However, you are reminded that where the transaction on an asset sale exceeds the high-value dealer threshold of €10k in cash, this may turn the entity into a 'High Value Dealer' and require HMRC supervision. HMRC advise that no-one should accept or make high value cash payments until they are registered as a high value dealer.

Use of Agents for Asset Sales

Where you use an agent or agency to sell assets and where CDD is required to be carried out on the purchaser of assets, you should ensure that your obligations for CDD requirements are able to be carried out effectively.

You should be carrying out CDD prior to any binding contract regarding the sale of assets being completed.

An agent may be a regulated entity – such as an estate agent – and reliance may be placed on the CDD the agent has undertaken subject to satisfying yourself that the details provided are adequate and enable an assessment of any risk to be undertaken.

Whilst you may ask the agent to undertake CDD on your behalf, any such arrangements should be formalised in writing, and the responsibility for completing CDD and ensuring that any checks are compliant will remain with the IP.

Third Party Funds

If funds are received from a third party – such as in an IVA or bankruptcy, you should carry out CDD on the third party and the source of funds, and assess the Money Laundering risk.

CDD on recipients of dividends/distributions

A dividend or distribution payment does not form a business relationship and CDD is not usually required to be undertaken. However, a risk-based approach should be considered and consideration made to check the Office of Financial Sanctions Implementation lists to ensure payments are not made to parties subject to sanctions.

Regulated Entity Appointments

Appointments do occur over entities that are in a regulated sector. If this happens, the entity remains in the Money Laundering regime and you should inform their PBS of your appointment.

It is noted that there would then be more than one PBS with interest in the appointment (your PBS and the entity's PBS) and you should take your own appropriate advice on who the relevant PBS would be for activities in relation to the insolvent entity.

Such an appointment would not make you a BOOM of the entity for Money Laundering purposes.

Further Considerations of Reporting Suspicions of Money Laundering or Terrorist Financing

Where assets are to be sold or distributed (including in specie), or payments are to be made from an entity for which a suspicion exists, consideration must be made about whether to submit a Defence Against Money Laundering SAR ('DAML SAR') to the NCA. If a DAML SAR is approved, this will provide you with consent to continue with the transaction.

If the suspicion involves cash in a bank account, any funds that are suspected of being the proceeds of crime will taint all funds in an account and distributions, and other payments may require consent to protect you from committing an offence under POCA 2002.

Where you form a suspicion of Money Laundering or Terrorist Financing, you should report such suspicions via your MLRO and subject to your firm's written policy.

Tipping-Off

As well as the usual care that should be taking regarding tipping-off, care should also be taken to ensure that reports to creditors or other parties which may be liable to disclosure do not contain any information that may be considered to constitute tipping-off.

You will not be tipping-off by providing access to case files to your RPB in the course of usual monitoring and inspection activity. You should exercise care in ensuring that working papers and

other records required to be maintained under insolvency legislation and regulation do not contain copies of reports made under MLR17.

If you have any concerns about tipping-off, due to the potential seriousness of any breach that is found against you, you should discuss this with your firm's MLRO or MLCO and check your internal guidance.