Insolvency Practitioners Association

1961 60 2021 LEADING PROFESSIONAL INSOLVENCY STANDARDS FOR SIXTY YEARS

Anti-Money Laundering Annual Report

2020/21

Contents

Introduction from the CEO

Paul Smith

This report will define the work undertaken by the Insolvency Practitioners Association (IPA) in performing our Anti-Money Laundering (AML) supervisory functions in accordance with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR17).

In an environment where financial crime has become part of our daily lives, and the increasing use of tech platforms for all forms of financial transactions has given rise to a significant increase in the range of methods by which fraud is perpetrated, the IPA are more than ever focused on ensuring that our Insolvency Practitioners (IPs) are equipped with the tools, knowledge and processes that will enable them to be compliant, be alive to the emerging risks of money laundering, and uphold the highest professional standards in their work across all areas of regulated activity.

I believe that this requires regulatory and supervisory processes and procedures that are effective, robust, sustainable, fit for purpose, and transparent.

The IPA's role as a Professional Body Supervisor is a key part of the UK's defence against money laundering. It sits alongside the IPA's overall Regulatory Objective to protect and promote the public interest. The pace of innovation in financial crime shows no sign of reducing. Consequently, encouraging strong knowledge of AML risks and having robust policies and procedures is at the heart of our supervisory responsibilities. The IPA regards

AML supervisory work as being of equal importance to our 'traditional' regulatory work in insolvency practice.

The IPA is the only regulatory body which is solely dedicated to the regulation and representation of IPs. As part of our roles to regulate and represent IPs, the IPA is pleased to be a member of two AML Supervisor Groups and is in regular communication with other insolvency Recognised Professional Bodies on AML matters.

This report covers the period to 5 April 2021. During 2020/21, the IPA was subject to an oversight visit from the Office for Professional Body AML Supervision (OPBAS), which identified ways in which the IPA's supervision role could be made more robust. Since the OPBAS review, the IPA has undertaken a risk profiling exercise of all IPs whom we supervise for AML purposes. The risk profile assists the IPA in planning AML specific visits and AML compliance reviews, as well as highlighting areas that should be notified to members as potential high-risk indicators for AML activity. Wherever we refer to AML, this includes money laundering and terrorist financing activity.

The IPA is also pleased to have provided AML-specific briefings (held at lunchtimes) to highlight what the IPA expects from members in respect of AML compliance and highlighting areas that the IPA considers may indicate a higher risk of money laundering. It was pleasing to see so many members attend these free briefings, and the IPA will be repeating them in 2022, reflecting the latest trends apparent from our supervisory work, and providing updates on emerging AML risks.

As CEO I am committed to ensuring that the IPA leads the way in relation to AML supervision of IPs, and I welcome the oversight and support of OPBAS in assisting the IPA in this endeavour. This report sets out how we fulfil our AML commitments in accordance with the MLR17, and how we shall continue to do so.

Paul Smith

The IPA's role as an AML supervisor

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR17) lists the IPA as one of 22 Professional Body Supervisors (PBSs). As a PBS it is the IPA's key function to ensure that the licensed IPs it regulates comply with MLR17 and the amendments[1] which came into force on 10 January 2020. The amendments further widened the scope of regulation to different sectors, which will impact a wide range of insolvency appointments. The IPA directly supervises 260 of our licensed IPs across 157 firms. The remaining IPs licensed by the IPA work at firms supervised by other PBSs. The IPA works collaboratively with the other PBSs to ensure that all IPs and firms who are Relevant Persons (as defined in MLR17) are appropriately and effectively supervised.

In our role as a PBS we monitor the compliance of our supervised population with MLR17 when carrying out insolvency and related work. This is achieved by:

- Undertaking targeted AML compliance monitoring by way of desk-based reviews and onsite inspections.
- Checking new licence holder applications to confirm identity and ability to act as an IP
- BOOM[2] verification and approval
- Reviewing firms' Regulation 18 AML risk assessments as part of the annual renewals process
- Reviewing AML compliance as part of all insolvency monitoring visits
- Investigations initiated from complaints and other intelligence received
- Robust and dissuasive enforcement measures where members' AML policies and procedures are deemed ineffective or non-compliant.

Our role as a PBS also involves working to promote best practice in AML compliance. We achieve this by:

- Being an active member of external AML-related groups;
- Regular communications and intelligence sharing with other PBSs, in particular where the PBS licenses IPs;

[1] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019

- Providing AML training via webinars, as part of roadshows and at our conferences;
- Regularly reviewing the AML risks most relevant to the insolvency sector and issuing guidance and technical updates on AML matters to members; and
- Supporting our members in adopting a risk-based approach via guidance, training and direct support via the IPA's dedicated AML email address (aml@ipa.uk.com) and telephone support where required.

AML Subcommittee

In January 2020, the IPA set up a Subcommittee to assist the IPA in achieving compliance with MLR17, reviewing IPA policies, procedures and guidance to ensure these are fit for purpose, and receive and challenge the IPA on its AML supervisory work.

The Subcommittee meets approximately 5 times a year and, since May 2021, has included lay membership.

IPA Board

The Chair of the AML Subcommittee is also a member of the IPA's Board, and the Board receives papers on AML at each Board meeting which update the Board on the IPA's AML operational and supervision work.

The IPA's approach to AML supervision

As required under regulation 17 of MLR17, the IPA adopts a risk-based approach to AML supervision. Further details on AML risk are provided in the IPA Sector Risk Assessment below. Thus, the IPA's supervisory efforts are focused on where the money laundering risks are highest. This helps to identify situations where additional measures and controls may be appropriate to reduce money laundering, while seeking to ensure that such measures are proportionate to the assessed risk. To help achieve this, the IPA maintains a risk profile of its supervised population. This helps to determine the frequency and intensity of onsite and desk-based supervision.

Types of Supervision

Compliance reviews

These are often conducted offsite and will typically involve elements of both insolvency and AML compliance. A firm's AML policies, procedures and controls (including SARs policies) are reviewed, and a selection of insolvency cases is reviewed. The effectiveness of these policies and procedures and the extent to which they are applied in practice are reviewed. This includes a review of the CDD measures. Training records are also reviewed to identify whether there are any deficiencies in the training of relevant employees, including the nominated officer for the purposes of regulation 21(3) (often referred to as the Money Laundering Reporting Officer, or 'MLRO') and other BOOMs.[2] The scope of compliance reviews will vary according to the assessed risk and may include interviews of relevant employees.

AML specific visits

These will mostly be undertaken onsite, but an offsite visit can also be accommodated if circumstances require. AML specific visits review and assess a firm's AML policies, procedures and controls (including a review of a selection of cases). As part of the visit, interviews will be undertaken of not only a firm's appointed MLRO, but also members of staff to assess the general understanding around the risks of money laundering, the firm's AML policies and procedures, the employees' role in AML matters and how employees spot and deal with suspicions of money laundering. Training logs will also be reviewed to identify whether there are any shortfalls in the training of staff, including the MLRO. Record keeping will be assessed along with the adherence to policies and procedures. The effectiveness and quality of suspicious activity reporting will also be reviewed.

Insolvency monitoring visits

When monitoring the insolvency work of an IPA Member, regardless of the firm's PBS, insolvency case files are reviewed for adequate written risk assessments, effective customer due diligence, record keeping and, where suspicious activity has been seen, whether this has been appropriately reported.

[2] Beneficial Owner, Officer or Manager

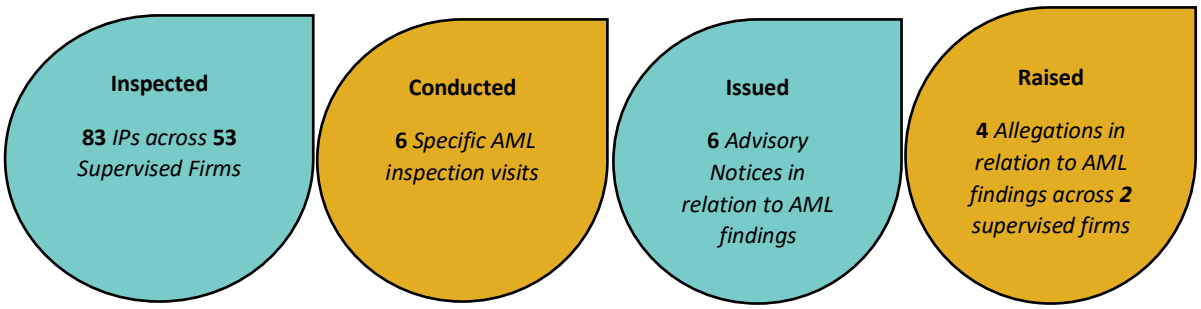
Results from monitoring activity

Overview and key themes

This report covers the period from 6 April 2020 to 5 April 2021. All inspection visits have included a check on an individual IP's compliance with their firm's AML policies, procedures and controls, as well as checks to ensure that the firm's policies are being adhered to and are effective irrespective of whether the IPA directly supervises the firm for AML purposes.

2020/2021 in numbers

Across our supervised population we have:



For more than two years, Advisory Notices (ANs) have been issued by Inspectors as a result of findings from routine inspections and AML-targeted inspections. An AN is often issued in circumstances which fall below the disciplinary standard but where the change proposed will assist the member in stronger compliance with regulation. A member's response to the issue of an AN is monitored subsequently.

Allegations of misconduct in respect of insolvency appointments can be issued and considered by the IPA's disciplinary process where the alleged breach or failure reached the level of serious misconduct.

Findings are published on the IPA website and the Insolvency Service website. These details are publicised to assist members in their compliance with MLR17.

Key themes, which have led to the issue of Allegations and ANs have been:

- Failure to undertake a risk assessment on Court appointed work;
- Failure to continually monitor AML risks through the lifetime of a case; and

- Failure to document considerations/additional work undertaken following electronic verification red flags.

IPs are reminded to ensure that:

- There is a firm-specific and regularly reviewed Reregulation 18 risk assessment, that identifies and assesses the risks of money laundering and terrorist financing to which the business is subject to;
- Each appointment has an assessment of the money laundering risk relating to that specific case and that the risk is monitored throughout the appointment;
- CDD/EDD work is, wherever possible, completed prior to the establishment of a business relationship; and
- Where electronic verification is used, 'red flags' from the electronic checks are reviewed and considered and extra checks undertaken are properly documented.

The IPA undertook six specific AML inspection visits, which were either flagged from prior findings in inspection visits or as a result of intelligence received.

Going Forward

The IPA continues to refine its risk-based approach to AML supervision. We have recently undertaken an exercise to ask MLROs about types of appointment held, training undertaken etc. The information has assisted in the risk profiling of firms and, with the use of information gained from past monitoring and intelligence received, the IPA expects to be able to better target resource in monitoring compliance with MLR17.

Improvements have been made to the 2022 licence renewal process to highlight to members the importance of AML issues. The renewal process requests greater up to date detail on AML matters to help refine the risk profiling of members, and members must also provide a copy of the firm's current regulation 18 risk assessment.

The consideration of effectiveness of policies and procedures will continue to be a key feature of AML specific visits. As part of these visits, the interviews of staff members will be seeking to ensure that policies are not only in place but are effectively communicated and utilised by staff.

There will also be an increased review of SARs records and policies, and a review of the quality of SARs submitted to the NCA. The IPA is aware that overall in the accountancy sector (which includes insolvency as outlined in the National Risk Assessment), the number of SARs submitted is only 0.93% of the total submitted SARs, and more frequent relevant reporting will be encouraged.

Members will see an increase in AML specific visits and compliance reviews in the coming 12 months in order to respond to the changing landscape of AML risks in insolvency work and from the consideration of information from risk profiling. With the UK starting to open up from the rollout of the COVID vaccination programme, more of the AML specific visits will be undertaken onsite. The IPA will also continue to provide guidance and information to members regarding new and increasing risks to businesses from potential money laundering and financial crime.

What is required of relevant persons supervised by the IPA?

The IPA requires its supervised population to comply with:

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended by The Money Laundering and Terrorist Financing (Amendment) Regulations 2019); and
- the Proceeds of Crime Act 2002 (as amended by the Serious Organised Crime and Police Act 2005).

IPA members are expected to be familiar with the AML/CTF Guidance for the Accountancy Sector, published by the CCAB[3]. This includes a new Appendix F (still pending Treasury approval) providing supplementary AML guidance for IPs.

To address the risks of money laundering and terrorist financing, the IPA must robustly supervise its members for AML compliance, and regulation 76 requires the IPA to impose effective sanctions on Members where the IPA is satisfied that a person has contravened a

[3] Consultative Committee of Accountancy Bodies

'relevant requirement'. The relevant requirements are set out in Schedule 6 to MLR17. Therefore, the IPA's supervisory procedures are designed to establish (among other things) whether relevant persons are:

- carrying out firm-wide risk assessments that demonstrate a clear understanding of the money laundering and terrorist financing risks faced by their firms;
- establishing, maintaining and regularly reviewing policies, controls and procedures to mitigate and effectively manage the AML risks identified;
- carrying out effective customer due diligence measures on clients, which include a risk assessment of the money laundering risks of the client and verifying the client's identity and sources of funds (as appropriate). The extent and nature of the verification procedures should reflect the risk rating of each client;
- training all relevant employees to be able to identify money laundering and terrorist financing risks, recognise red flag indicators and know how to report suspicious activities; and
- appointing a nominated officer to receive internal reports of suspicious activity and make external suspicious activity reports[4] (where appropriate) to the National Crime Agency (NCA).

IPA Members are expected to be familiar with the detailed requirements in these areas. Although the IPA provides AML training, in various forms, it is for individual Members to determine their training needs and how best to acquire relevant training. Nevertheless, the IPA provides information, guidance and other resources on its website through the Anti-Money Laundering Hub and in the Members' area.

[4] SAR reporting requirements and guidance links

IPA Sector Risk Assessment

Introduction

The impact of money laundering is devastating – it enables serious organised crime such as modern slavery, drugs trafficking, fraud, corruption and terrorism. A comprehensive system of risk assessment is key to understanding the money laundering and terrorist financing risks to which a business is exposed.

According to regulation 18 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR17), an insolvency practitioner (IP) licensed by the IPA must take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which their business is subject, taking into account:

- information made available to them by the IPA (including this sectoral risk assessment required by regulation 17(1)), and
- risk factors relating to its clients, services, transactions and delivery channels, and the countries or geographic areas in which they operate.

An IP must, on request, provide their risk assessment to the IPA. They must also establish and maintain policies, controls and procedures to mitigate and effectively manage the risks of money laundering and terrorist financing identified in the risk assessment undertaken under regulation 18. Those policies, controls and procedures must include (among other things) risk management practices and customer due diligence (CDD).

CDD procedures undertaken will vary according to the assessed risk and may also suggest that client risk should be reassessed. But CDD itself should not be confused with the risk assessment. This document explores the relevant AML risks relating to insolvency practice. But first, let us be clear about what we mean by AML risk:

What is AML risk?

Regulation 16 of MLR17 states that the Treasury and the Home Office must make arrangements for a risk assessment to 'identify, assess, understand and mitigate the risks of money laundering and terrorist financing affecting the United Kingdom', and they must report

on that risk assessment. That report has become known as the National Risk Assessment (NRA).

According to regulation 17, the IPA must identify and assess the risks (of money laundering and terrorist financing) to which its Members are subject (The IPA must also develop and record risk profiles for each of its practising IPs). Similarly, as we have seen, regulation 18 also requires the IP to identify and assess the risks of money laundering and terrorist financing to which their business is subject. To be clear, it is the public who are most vulnerable to the risks of money laundering and terrorist financing. An IP is subject to the risk that they will fail to comply with MLR17, but the wider public bear the risk that money laundering or terrorist financing will take place and might even go undetected.

The IP's risk of noncompliance with MLR17 includes the risk that they may be subject to exploitation for money laundering purposes. In fact, MLR17 refers to a relevant person's responsibility to mitigate the risks, which can only be done through avoiding involvement in the money laundering process. Therefore, when we talk about an IP's AML risk in this sectoral risk assessment, we are referring to both the IP's risk of exploitation for money laundering and the risk that the IP may fail to identify (or reasonably suspect) money laundering where it has taken place.

The overall risk of money laundering and terrorist financing in the accountancy sector

The Economic Crime Plan identifies economic crime as a significant threat to the security and the prosperity of the UK. Its impact is felt across our society. Fraud is now one of the most common crimes in the UK, with one in fifteen people falling victim each year. Money laundering enables criminals to profit from some of the most damaging crimes. Bribery and corruption undermine fair competition and are barriers to economic growth.[5]

HM Government, law enforcement, and the professional body supervisors work together to ensure that criminals find it difficult to exploit accountancy services. Members of the Accountancy AML Supervisors Group (AASG) have been able to set out the key risks, and red-flag indicators, that they consider are relevant to the accountancy sector. The AASG (of which

[5] Economic Crime Plan 2019-22

the IPA is a member) will update this 'Risk Outlook' on a regular basis, reflecting the UK's latest NRA and other emerging threats and trends.

The AASG's Risk Outlook is available to assist accountants and IPs in assessing AML risk with reference to the services they provide and the types of client they have. The firm's written risk assessment will identify the areas of the business that are most at risk and this will enable the accountant (or IP) and their firm to focus resources on the areas of greatest risk. It is the responsibility of the firm's senior management to approve and document the policies, controls and procedures that address and mitigate the risks. The firm must also provide training to staff on the risks and how the firm mitigates those risks (including through CDD).

The NRA states that accountancy services remain attractive to criminals due to the ability to use accountants to help their funds gain legitimacy and respectability, as implied by the accountant's professionally qualified status. Although the accountancy services considered most at risk of exploitation continue to be:

- company formation and termination,
- mainstream accounting; and
- payroll,

insolvency practice still provides the legitimacy and respectability of the accountancy professional, as well as carrying specific risks relating to the different types of insolvency practice.

The NRA says little about insolvency practice specifically[6], but it concludes that accountancy services generally are at highest risk of being exploited or abused by criminals when the accountant does not fully understand the money laundering risks and does not implement appropriate risk-based controls. This would apply to IPs too. These risks can be well-managed through effective AML policies and procedures, in line with the AML Guidance for the Accountancy Sector (AMLGAS). Firms should tailor their AML policies and procedures to address the risks present in particular service lines or clients.

[6] Paragraph 9.11 states: 'There continues to be a risk that criminals will exploit company liquidation and associated services (including insolvency practice, which may be conducted by certain accountancy professionals) to mask the audit trail of money laundered through a company.'

Key risks relevant to the insolvency sector

The remainder of this document is intended to help IPs to better understand their exposure to risk, and so equip them to apply appropriate procedures to mitigate that exposure. Therefore, IPs are expected to consider this document when assessing the risks they and their firms face relating to money laundering. It must be seen to impact IPs' and firms' own risk assessments, and so inform their AML policies and procedures, including CDD. Sectoral and firm-wide risk assessments should also be incorporated into staff training, to help mitigate the risks of money laundering taking place unnoticed, or even being unwittingly enabled.

The UK's first NRA published in October 2015 highlighted that:

"*Criminals can use accountants to conceal the origins of criminal funds and/or legitimise accounts in a variety of ways, such as the creation of companies, trusts and offshore corporate structures; providing false accounts; preparation or audit of businesses' annual accounts; insolvency malpractice; and providing advice*."

Key threats and vulnerabilities within the professional advisor sector were identified, and remain relevant still. For clarity of understanding, those money laundering risks may be categorised between:

- active assistance in money laundering,
- unwitting exploitation for money laundering, and
- the risk that money laundering will go undetected.

The IPA believes that these risks remain present and can, to some extent, be mitigated by IPs evidencing compliance with the Insolvency Code of Ethics and with SIP 1. The latter states that IPs should 'ensure that their acts, dealings and decision making processes are transparent, understandable and readily identifiable, where to do so does not conflict with any legal or professional obligation. An insolvency practitioner should inform creditors at the earliest opportunity that they are bound by the Insolvency Code of Ethics …'.

The NRA was updated in October 2017 and again in December 2020. Accountancy services generally remain a high risk area for money laundering (but low risk in respect of terrorist financing) and, in the 2020 update, the following was noted in respect of insolvency work:

'There continues to be a risk that criminals will exploit company liquidation and associated services (including insolvency practice, which may be conducted by certain accountancy professionals) to mask the audit trail of money laundered through a company. Regulatory guidance, increased supervision and strict legislative requirements on ASPs go some way to mitigate the risks of providing these services.'

The IPA is also required to make its Members aware of the CCAB's Anti-Money Laundering Guidance for the Accountancy Sector 2020 and specifically it is recommended best practice that IPs follow the draft CCAB insolvency specific appendix.[7] Aspects of the CCAB's AMLGAS have been incorporated into the guidance below. It recognises that trust or company services providers (TCSPs) are relevant persons according to MLR17, but that an IP acting in their capacity as an office holder is understood to be a relevant person only in their capacity as an IP and not as a TCSP, notwithstanding that the registered office of the entity in respect of which they have been appointed has been changed to that of the IP.

Relevant risks relate broadly to the client entity type, the nature of the service being provided, the location of assets or trading activities (including customers, suppliers and the control of the business), the nature of the client's business, and risks associated with the interface between the business and its client where the client is more remote than normal. IPs should consider the extent to which these categories of risks apply in a particular insolvency appointment and their work in general.

Examples of higher risk factors that may be encountered in the context of insolvency appointments may include the following:

Client risk factors

- Where the debtor, company officers or beneficial owners of the insolvent entity are the subject of a criminal investigation or civil recovery proceedings.
- Where there have been cashflow issues in the business, the IP should consider the possibility of fraud.

[7] This version of the guidance, including the insolvency appendix, is currently in draft pending approval from HM Treasury. It was published in September 2020.

- Where the debtor or the insolvent entity is a 'relevant person' within the definition of regulation 8 of MLR17, particularly when it has not recognised this.

Service risk factors

- Where the insolvency proceedings will involve the realisation or distribution of assets of the insolvent entity.
- Where the IP cannot withdraw once appointment has been made.

Geographical risk factors

Where any of the following are within a country or countries identified as presenting high risk factors:

- the country of incorporation or residence of the client;
- the location of the beneficial owner;
- the location of assets or trading activities conducted;
- the location into which payments may be made.

Channel risk factors

- Where there is no personal contact with the debtor or the directors or beneficial owners of the insolvent entity.

Appointment

Where an IP is appointed by court order, by a decision or deemed consent procedure convened by the official receiver, the Accountant in Bankruptcy, or directly by the Secretary of State, without any prior involvement with the insolvent, some reliance can be placed on the order of appointment or the initial bankruptcy or winding-up order to evidence the identity of the insolvent as part of risk based procedures. This would apply to the following cases:

- Appointment as provisional liquidator by order of the court;

- Appointment as liquidator in a winding up by the court (whether by court order following an administration, via a decision procedure or deemed consent procedure convened by the official receiver or directly by the Secretary of State);
- Appointment as administrator or special administrator by order of the court;
- Appointment as administrative receiver (in Scotland, receiver) or special manager by order of the court;
- Appointment as trustee in bankruptcy (whether via a decision procedure or deemed consent procedure or meeting convened by the official receiver, the Accountant in Bankruptcy or directly by the Secretary of State).

Any such reliance on the court order, the notice of appointment or the initial bankruptcy or winding-up order does not remove the need to consider the identity of the beneficial ownership of the entity, or remove the need to consider whether money laundering activity may have taken place. The IP will also need to consider and assess AML risks that may become apparent during the course of the appointment.

Having documented the firm's (or IP's) risk assessment, a client risk assessment and CDD must take place before the establishment of a business relationship, for example prior to:

- agreeing to act as liquidator or provisional liquidator of a solvent or insolvent company or LLP;
- agreeing to act as nominee in a company voluntary arrangement not preceded by another insolvency procedure;
- agreeing to accept an appointment as administrator or special administrator;
- agreeing to accept appointment as an administrative receiver (in Scotland, receiver);
- agreeing to act as nominee or supervisor in an individual voluntary arrangement;
- agreeing to act as a trustee (including interim trustee) in a bankruptcy, a sequestration or under a trust deed;
- accepting instructions to prepare, or assist in preparing, a proposal for a company or individual voluntary arrangement where appointment as nominee will 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.

In very limited circumstances (for example a hostile appointment), it may not be possible to have completed the risk assessment and CDD before taking office. But an initial client identification and assessment of risk must be completed before consenting to act and reviewed as soon as is practicable following appointment (within five working days is considered reasonable). IPs should also be mindful that the circumstances in which legislation permits an office holder to resign do not include an inability to complete CDD procedures.

Where it is not possible to complete the CDD before taking office, IPs should nevertheless have gathered sufficient information to allow them to form a general understanding of the identity of the debtor, company officers or beneficial owners of the entity, including information about what the business did and where it traded, in order to be able to assess AML risk.

Under certain circumstances, IPs are permitted to rely on CDD conducted by third parties. Where an IP is appointed administrative receiver (in Scotland, receiver) or administrator by a bank or other institution which is itself subject to MLR17, the IP may be able to rely on CDD undertaken by that institution. But it is the IP's responsibility to ensure they have sufficient information to be able to assess AML risk.

MLR17 require ongoing monitoring of business relationships. In a formal insolvency where trading has ceased, it is likely that further CDD would only be required where the office holder becomes aware of suspicious activity or is concerned about the veracity of previous CDD information.

In the case of an appointment where the IP becomes vested of the assets of the debtor, (bankruptcy in England & Wales and Northern Ireland and sequestration and trust deeds in Scotland), asset sales are conducted by the IP as principal. In such cases, the IP, being

themselves a relevant person within the regulated sector, should apply the occasional transaction provisions and conduct CDD on the purchasers of assets for transactions amounting to 15,000 euros or more. (When appointed as a liquidator, administrator, administrative or other receiver, or supervisor of an IVA or CVA, an IP's business relationship is with the debtor or the entity over which they have been appointed, not with the purchasers of their assets.)

After appointment

Where an IP receives other funds from a third party, for example a third party contribution in an IVA or a bankruptcy, the IP should assess the associated AML risk. In an insolvency context, examples of factors which may be considered as part of the risk assessment would include:

- the relationship between the third party and the insolvent;
- the rationale for the third party contributing to the insolvent estate;
- the source of funds to the third party.

The payment of a distribution or dividend is not a business relationship for the purposes of MLR17. However, the IP should consider whether they should check the Office of Financial Sanctions Implementation lists to ensure they are not making payments to any parties subject to financial sanctions.

It is generally understood, among IPs, that members' voluntary liquidations (MVLs) of solvent companies present the highest risk. This is because the IP is presented with a company that has a cash balance to be distributed and they are unlikely to know the business or owners. Therefore, it is essential that the IP can demonstrate robust CDD in respect of the MVL.

Recently emerging risks

The IPA's annual renewals process now requires all its IPs to supply copies of their firms' AML risk assessments under regulation 18 of MLR17. The media sent to IPA Members has made it clear that firms' risk assessments must be evidenced as having been updated and reviewed, at least on an annual basis. It is expected that the impact of recent events and the widely publicised COVID-related frauds should feature heavily in risk assessments.

According to Insolvency Statistics published recently, the number of company insolvencies in June 2021 was 63% higher than in the same month in the previous year and 18% lower than in June 2019. Personal insolvency numbers still greatly exceed corporate figures. The number of Debt Relief Orders in June 2021 was 21% lower than in June 2020 and 33% lower than in June 2019. Bankruptcies were 17% lower than in June 2020 and 44% lower than in June 2019. The sustained reduction in work levels across both corporate and personal insolvency appointments means that there is increased risk of IPs being under financial pressure if they are not utilising the furlough scheme and other support measures.

Corporate Appointments

Criminals continue to use UK and overseas corporate vehicles to move and conceal illicit funds. A range of vulnerabilities are exploited to circumvent controls, with continued use by offenders of nominee directors, shell companies and trusts to conceal beneficial ownership. This poses a potential threat to IPs who may unwittingly become involved in corporate insolvencies that may have previously been involved in illegal activities or may be purchased out of insolvency with the proceeds of crime.

IPs must maintain records that demonstrate compliance with their AML responsibilities, as well as compliance with the Insolvency Act, Statements of Insolvency Practice, and the Code of Ethics. IPs must be able to demonstrate their assessment of risks, appropriate CDD and an appropriate level of scepticism in respect of corporate insolvencies.

As appropriate to each firm's business profile, their firmwide risk assessment should incorporate all relevant risks that reflect current appointments and industry exposure. 2020 and 2021 have seen a significant rise in warnings via *Dear IP*, published by the Insolvency Service, and these should be considered for all risk assessments. A key notification is Dear IP 117[8] which highlighted 'Suspicious or fraudulent redundancy payment claims – A reminder of an Insolvency Practitioner's responsibilities', with the key being robust CDD measures to check all directorships.

The Bounce Back Loan Scheme (BBLS), which closed on 31 March 2021, was set up in April 2020 to help small and medium sized businesses struggling as a result of the COVID-19

[8] DEAR INSOLVENCY PRACTITIONER Issue 117 – December 2020

emergency. Businesses could borrow up to a maximum of £50,000. In total 1.2 million loans were given, totalling £36.9 billion. The National Audit Office report of October 2020[9] estimated '*total credit and fraud losses of between 35% and 60%*,'. The Insolvency profession will continue to see the fallout of this in insolvency appointments over the next few years. IPs are also likely to see abuse of other COVID-19 support measures such as the furlough scheme. If the actions result in criminal property then they should be reported accordingly. IPs and their staff need to understand the risks and potential indicators, and how to make a SAR (as well as reporting under section 218[10] of the Insolvency Act).

Personal Insolvency

The AML risk relating to personal insolvency is inherently low, especially in the IVA market. But, due to the very large number of cases each year, IPs must be mindful of the risks and be able to identify red flags (i.e. risk indicators). The National Strategic Assessment of Serious and Organised Crime report also highlighted concerns about individuals being recruited as money mules. Given the vulnerability and pressures of insolvency it is possible that insolvent individuals may be more susceptible to engaging in such activities. Money mules may be:

- asked to receive and transfer money into and out of their bank accounts, offering a cut in return,
- provided with cash and paid a fee to purchase goods for shipment overseas, to minimise traceability, or
- conned into becoming mules unwittingly, by asking for bank details via seemingly genuine job adverts.

Scotland and Northern Ireland appointments

The vast majority of IPA Members deal predominately with England and Wales appointments, although all IPs with full authorisation have the ability to take appointments in Scotland and Northern Ireland. IPs must be aware of the legislative differences, although there is no evidence to suggest AML risks are very different. The one exception for Scotland is that of Scottish Limited partnerships (SLPs). It has been reported by the BBC that SLPs had been used to move $80bn from Russia in just four years.

[9] National Audit Office Investigation into the Bounce Back Loan Scheme (nao.org.uk)
[10] S218 (4) of the Insolvency Act 1986

Action on risk

The IPA issues to Members the regular updates from the NCA and other authorities to highlight the impact of fraud on AML risk, including the continued fallout from the COVID pandemic. IPs must be able to demonstrate that they regularly review the emerging risks from fraud, embezzlement, exploitation of furlough and other COVID support measures, along with medicrime, corruption and cybercrime. The IPA's roadshow series has raised awareness of these issues.

IPs must be aware of the red flags, including the most common red flags across all professions, and be on alert to them when dealing with both new and existing clients.

Transactions: Are transactions unusual because of their size, frequency, or the manner of their execution, in relation to the client's known business type?

Structures: Do activities involve complex or illogical business structures that make it unclear who is conducting a transaction or purchase?

Assets: Does it appear that a client's assets are inconsistent with their known legitimate income?

Resources: Are a client's funds made up of a disproportionate amount of private funding, bearer's cheques, or cash, in relation to their socioeconomic profile?

Identity: Has a client taken steps to hide their identity, or is the beneficial owner difficult to identify?

Behaviour: Is the client unusually anxious to complete a transaction or are they unable to justify why they need completion to be undertaken quickly?

Political Status: Is the client engaged in unusual private business given that they hold a prominent public title or function? Or do they have ties to an individual of this nature?

Documents: Are information or documents being withheld by the client or their representative, or do they appear to be falsified?

Geographical Area: Is the collateral provided, such as property, located in a high-risk country, or are the client or parties to the transaction native to or resident in a high-risk country?

Choice of Professional: Have you been instructed from a distance, asked to act outside of your usual speciality, or offered an unusually high fee?

The Financial Action Task Force (FATF) website has more information on potential indicators of money laundering, as well as up to date information on high-risk jurisdictions.

The COVID pandemic has increased the potential for fraud and the IPA has seen that there is a tendency to approach IPs through website referrals as opposed to traditional referrals from local accountants and legal firms. We therefore regard IPs with web-based referral business as high risk. However, the statutory obligations an IP undertakes (performed diligently) in investigating how a business was conducted, its prior transactions and its assets should flag any suspicions for reporting. The implications of failing to report suspicions are set out in the Crown Prosecution Service guidance[11]. A professional will be prosecuted for failure to disclose, which is an offence under Section 330, where a person:

- receives information in the course of a business in the regulated sector, as defined in Schedule 9, and
- thereby knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering, and
- can identify that other person or the whereabouts of any of the laundered property or believes, or it is reasonable for them to believe, that the information will or may assist in identifying that person or whereabouts of any of the laundered property; and
- fails to disclose to a nominated officer (see sections 338(5), 336(11) and 340(12)), or a person authorised for the purposes of Part 7 by the Director General of the NCA, the information on which his knowledge or suspicion is based as soon as is practicable after the information comes to him.

[11] CPS Money Laundering Offences

Working with others to share information

Under regulation 50 of the MLR17, the IPA is required to take appropriate steps to co-operate and share intelligence with other supervisory authorities (including the other PBSs), HM Treasury and law enforcement agencies.

To support a strong supervisory framework, the IPA shares information and intelligence by participating in the following groups:

Anti-Money Laundering Supervisors Forum (AMLSF)

The Forum aims to share and develop the consistent application of best practice across all AML/CTF supervisory bodies. Through it, the PBSs liaise with the NCA, HM Treasury, the Home Office, HMRC, the FCA, the Gambling Commission and other government agencies involved in the prevention and reduction of economic crime. Further information on the purpose of the group is available in its terms of reference.

Accountancy AML Supervisors' Group (AASG)

The AASG (formerly known as the Accountancy Affinity Group (AAG)) is a sub-committee of the UK's AMLSF consisting of PBSs listed in Schedule 1 to MLR17. It is a forum in which professional accountancy bodies (including the IPA) work collaboratively to develop a sector-appropriate supervisory policy to promote consistency in standards and best practice. Further information on the purpose of the group is available in its terms of reference.

Accountancy Sector Intelligence Sharing Expert Working Group (Accountancy ISEWG)

The purpose of the Accountancy ISEWG is to advance and improve intelligence and intelligence-related information sharing between accountancy sector PBSs, AML statutory supervisors and law enforcement agencies. Further information on the purpose of the group is available in its terms of reference.

Financial Conduct Authority Shared Intelligence Service (SIS)

The IPA is a member of the SIS which is owned by the Financial Conduct Authority. Membership enables the IPA to participate in information sharing between PBSs and law

enforcement agencies on AML/CTF matters. As a member of SIS, the IPA must respond to intelligence sharing enquiries from other SIS members and pro-actively input its own intelligence into the SIS.

Other intelligence sharing

Regulation 46(5) of MLR17 requires a PBS which, in the course of carrying out its supervisory functions or otherwise, knows or suspects, or has reasonable ground for suspecting, that a person is or has engaged in money laundering or terrorist financing, must as soon as practicable inform the NCA.

The IPA made 3 Suspicious Activity Reports (SARs) to the NCA during the 2020/21 financial year, which was an increase on the 2 reports made for the 2019/20 financial year. SARs are reported when we identify a suspicion of money laundering through our work.

The IPA is committed to providing members with information to assist in reviewing their firms' AML policies and procedures and to highlight new and increasing risk issues. We look to publish a relevant AML article in each IPA Newsletter, which may include information from the NCA on new risk areas and updates to the SAR reporting regime.

We have also updated the AML Hub – accessible from the regulatory pages of the IPA website – with useful guidance for members to assist with AML compliance. This has been expanded to include guidance on high-risk indicators for IPs in insolvency work.

The IPA seeks to ensure that AML is considered and discussed at all IPA Conferences and Roadshows.

Whistleblowing

IPs have a duty under SIP 1 to report any IP who is not complying with, or has not complied with, any relevant laws and regulations. A report must be made either to the Complaints Gateway or to the relevant Recognised Professional Body. IPs also have a duty under MLR17 to report an IP who is not complying with, or may have breached their AML obligations under MLR17 or IPA requirements. The IPA's updated policy on whistleblowing can be found here.

Agile money laundering personas

The NRA for 2020 highlights that 'There continues to be a risk that criminals will exploit company liquidation and associated services (including insolvency practice, which may be conducted by certain accountancy professionals) to mask the audit trail of money laundered through a company.'

Insolvency Practitioners should be aware of the constantly evolving risks of money laundering and terrorist financing. IPs may find it useful to consider the various fictional examples which can be found here.

IPA resources - support and guidance

Further guidance can be found on the IPA website and, in particular, on its Anti-Money Laundering Hub pages.

Details on the Hub include:

- The IPA's AML strategy
- An AML guide and a checklist for members
- Guidance for members on emergency DAML requests
- Agile Personas and AML case studies
- NCA guidance on submitting better SARs
- IPA's policies on whistleblowing, conflicts and complaints
- Links to the Money Laundering Regulations, CCAB Guidance, 5th Money Laundering Directive
- Information provided to members regarding COVID and AML

The website also provides copies of the IPA Newsletter where articles relating to AML matters are published each month and details of conferences and roadshows where the IPA will include sessions on AML.

Further AML and CFT support for Members can be sought through the AML email address – **aml@ipa.uk.com**. Calls can also be made to the IPA office and one of the members of the IPA Secretariat who deal with AML matters will return your call. Details from a call will be treated confidentially. Advice requested and given via the AML 'help-desk' email is confidential and is provided to assist members with their compliance with the Money Laundering Regulations.