Anti-Money Laundering: 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.[1]

[1] Economic Crime Plan 2019-22

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 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[2], 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

[2] 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.'

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.

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.[3] 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.

[3] 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 there have been cashflow issues in the business, the IP should consider the possibility of fraud.
- 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[4] 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

[4] 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[5] 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[6] 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.

[5] National Audit Office Investigation into the Bounce Back Loan Scheme (nao.org.uk)
[6] 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[7]. 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.

[7] CPS Money Laundering Offences

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.