

# IPA Sector Risk Assessment 2022/2023

The purpose of this section is to set out the sector risks in respect of money laundering (ML) and terrorist financing (TF) that the IPA considers to be of relevance to the insolvency practitioners (IPs) and firms the IPA supervise. The aim is to inform our supervised population of current or emerging risks they might face. IPs should review this document and ensure they evaluate the relevant risks they face and incorporate these firstly into their own firm's risk assessment<sup>1</sup> and Customer Due Diligence (CDD)<sup>1</sup> risk assessments and also ongoing monitoring, policies, procedures. This should also be incorporated into staff training to help mitigate the risks of assisting ML and TF.

IPs<sup>2</sup> that are licenced by the IPA are automatically supervised by the IPA. Where IPs work at firms that have an alternative PBS<sup>3</sup> supervisor the IPA collaborates with them to agree supervision on a firm by firm basis. The IPA will take regulatory action for AML or Counter Terrorist financing /(CTF) compliance failings in respect of any insolvency appointment, irrespective of an IPA regulated IPs PBS. Given the interaction of accountants, IPs and the legal sectors it is vitally important that IPs are fully aware of their duties and the requirements placed upon them by all relevant AML and CTF legislation. The regulations have continued to evolve. On 10 January 2020 changes to the Government's Money Laundering Regulations came into force The Money Laundering and Terrorist Financing (Amendment) Regulations 2019<sup>4</sup> set out the amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR17). This legislation extended the scope of regulated industries and changed the way customer due diligence and enhanced due diligence is conducted.

The IPA has a duty to uphold professional standards and ensure that IPs are aware of the duties and requirements to ensure that they fully understand the threats, vulnerabilities,

---

<sup>1</sup> [The Money Laundering, Terrorist Financing and Transfer of Funds \(Information on the Payer\) Regulations 2017 Risk assessment Reg 18 & CDD regulation 28](#) -

<sup>2</sup> [Insolvency Practitioner as defined under section 388 of the Insolvency Act 1986](#)

<sup>3</sup> [As per Schedule 1 The Money Laundering, Terrorist Financing and Transfer of Funds \(Information on the Payer\) Regulations 2017](#)

<sup>4</sup> [The Money Laundering and Terrorist Financing \(Amendment\) Regulations 2019](#)

consequences, and risk that they may face from different appointments and also by interacting with other regulated professionals and those that are unregulated. To assist IPs comply with their obligations under UK legislation to prevent, recognise and report money laundering it is advised that they follow the updated CCAB guidance on [Anti-Money Laundering and Counter-Terrorist Financing Guidance for the Accountancy Sector 2022](#) and specifically it is recommended best practice that IPs follow the draft [CCAB insolvency specific appendix](#).

### **Threats and vulnerabilities**

The UK's first [National Risk Assessment \(NRA\)](#) 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. Many of the vulnerabilities set out below also leave accountants open to being used, wittingly or unwittingly, to assist the financing of terrorism.”*

The key threats and vulnerabilities within the professional advisor sector were identified through this risk assessment as:

- complicit professionals facilitating money laundering
- collusion with other elements of regulated sector
- coerced professionals targeted by criminals
- creation of structures and vehicles that enable money laundering
- the provision of false accounts
- failure to identify suspicion and submit SARs
- low barriers to entry and mixed standards of compliance with the regulators across the sector
- ASPs not registered under the regulations facilitating money laundering or terrorist financing (wittingly or unwittingly)
- inconsistencies in the supervisory framework, and the potential for poor communication between supervisors

The IPA considers these risks remain present and can be mitigated by education and IPs evidencing compliance with the [Insolvency code of ethics](#) and ensuring compliance with [SIP 1](#)

of ensuring that acts dealings and decisions making are readily identifiable and that any act that discredits the profession is reported.

The NRA was updated in October 2017<sup>5</sup>. Insolvency remained a high risk area and the following was noted:

*'Company liquidation and associated services (including insolvency practice, which may be conducted by certain accountancy professionals) also pose a risk of criminals masking the audit trail of money laundered through a company and transferring the proceeds of crime. The scope for abuse of insolvency services is mitigated to some extent by the licensing of practitioners, the strict set of obligations through the Insolvency Act and recent changes through the Small Business, Enterprise, and Employment Act 2015. However, there remains evidence of insolvency and wider company liquidation services being abused.'*

An example of the abuse by an Organised Crime Group ('OCG') was provided by the following case study:

*'A substantial food manufacturing company was acquired by individuals connected to an OCG through abuse of insolvency procedures. The company was acquired, through the assistance of a professional body supervised accountant, using funds from suspicious sources involving creditor write-offs exceeding £1 million. Once acquired, the company was suspected of being used to launder criminal cash. There was evidence indicating that the company was managing large sums of cash on-site using two distinct safes in a manner that supported this suspicion. The accountant was subsequently expelled as a member by the relevant professional body supervisor in respect of matters arising from this acquisition. '*

The case example remains a potential threat that the supervised population should be aware of.

The third NRA was published in December 2020. Money laundering risk remain higher than terrorist financing and whilst insolvency only gets two mentions, the key message on risk is a shared one:

*'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*

---

<sup>5</sup> NRA [2017 National Risk Assessment](#) & [2020 National Risk Assessment](#)

*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 report highlights the continued development and evolution of money laundering methodologies.

### **Impact of Russia's invasion of Ukraine, COVID, FinCEN files, Panama, and Paradise papers**

The 2022 IPA renewals will once again require all IPs to supply copies of their firm's AML risk assessment under [reg 18](#). All members are required to ensure that risks are evidenced as updated and reviewed, at least on an annual basis. Risk assessments should be clearly dated and record maintained of previous versions. It was expected that the impact of recent events in Ukraine and the widely publicised Covid frauds should continue to feature heavily in risk assessments along with the impact of [OFSI](#) sanctions and potentially EU Sanctions and for any US\$ transaction Office of Foreign Assets Control (OFAC).

The complex techniques some individuals and organizations employ to avoid sanctions regulations often make headlines. Although criminals intentionally evade sanctions, financial institutions and professional services providers may unintentionally facilitate sanctions evasion—resulting in not only financial and reputational risk. The risks arise when an entity does not understand potential sanctions evasion schemes and how to implement tailored, risk-based sanctions programs to mitigate those risks. Sanctions enforcement is increasingly a primary focus area. IPs need to update their knowledge of their domestic regulatory requirements and other global programs regularly to prevent and detect sanctions evasion techniques.

The use of shell companies is a well known technique to disguise ownership. Those wishing to avoid sanctions are increasingly using shell companies to funnel money to sanctioned entities, to sanctioned jurisdictions and/or for the purchase of sanctioned goods. Shell companies are relatively quick and simple to set up. They allow sanctioned countries and individuals the ability—and a level of anonymity—to conduct business for a brief period, moving money in a short burst of activity. IPs need to be able to demonstrate knowledge of the firms they are appointed over.

## **Risk by IP services**

The [Insolvency Service insolvency statistics to September 2022](#) continue to highlight very little historical difference in the ratio of corporate insolvencies. Creditor Voluntary Liquidations (CVLs) remain the highest in terms of numbers at around 3,000 per quarter, and normally compulsory liquidations are around 1,000 per quarter, although the impact of Covid provisions on the ability to issue court action to recover debts has dramatically reduced these number for the last 12 months. Administrations and CVAs continue to make up less than 1,000.

The majority of firm risk assessments reviewed as part of the IPA's supervision have tended to show that solvent liquidations (MVLs) present the highest risk. This is usually because the IP is only presented with a company that has a cash balance to be distributed and the IP is unlikely to know the business or owners. It is therefore imperative that IPs can demonstrate both a robust understanding of the inherent risks and full customer due diligence in respect of MVLs. This is a primary risk for 2022/23 especially due to the sanctions evasion techniques.

The latest [Insolvency Statistics](#) show: In September 2022 there was a total of 1,679 registered company insolvencies, comprised of 1,379 CVLs, 204 compulsory liquidations, 39 administrations and 11 CVAs. There were no receivership appointments.

The personal insolvency numbers greatly exceed corporate figures. There were 1,812 Debt Relief Orders (DROs) in September 2022, which was 16% lower than September 2021 and 26% lower than the pre-pandemic comparison month (September 2019).

There were, on average, 7,188 Individual Voluntary Arrangements (IVAs) registered per month in the three-month period ending September 2022, which is 5% higher than the three-month period ending September 2021, but 4% lower than the three-month period ending September 2019. IVA numbers have ranged from around 6,300 to 7,800 per month over the past year. The previous two years showed sustained reductions in the work levels across both corporate and personal insolvency appointments, numbers are recovering and the continued threat of a formal recession and the cost of living pressures mean that numbers are likely to pick up and it is important that AML policies remain effective with increased volumes.

## Risks to IPs

### *a) Corporate Appointments*

[The National Strategic Assessment of Serious Organised Crime](#) report published in 2020 estimated that serious organised crime (SOC) costs the UK economy £37Billion and there are estimated to be 4,772 organised crime groups in the UK. The networks are well established and continue use new technologies to exploit and commit offenses so it is important that IPs are aware of these developments. The report also highlights that Money Laundering represents in excess of £100Billion in the UK annually. 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.

Accountants and solicitors continue to be used to facilitate the movement and concealment of illicit funds, as seen in many high-value illicit finance and proactive asset denial investigations in the past year. A growing number of professional money launderers have been observed working outside of or in combination with international controller networks.

This poses a potential threat to IPs who either willingly or unwittingly become involved in corporate insolvencies that may have previously been involved in illegal activities or maybe purchased out of insolvency with proceeds of crime.

The IPA must ensure that IPs maintain records that show the checks undertaken in respect of their AML duties and also the insolvency profession requirements of compliance with the Insolvency Act, Statements of Insolvency Practice, and the Code of Ethics. IPs should be able to demonstrate clear assessment of risks, appropriate customer due diligence and a proportionate level of investigations undertaken in respect of corporate insolvencies.

As appropriate to each firm's business profile, their [regulation 18](#) risk assessment should incorporate all relevant risks that reflect current appointments and industry exposure. This is highlighted in AASG alerts as might be relevant to the risks the firm may face such as published in the last 12 months. 2020 and 2021 has seen a significant rise in warning via Dear IP notifications published by the Insolvency Service and these should be considered for all risk

assessments. A key notification is Dear IP 117<sup>6</sup> 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.

#### *Abuse of Bounce Back Loan Scheme (BBLs) and other Covid Support measures*

The BBLs, which closed on 31 March 2021, was originally set up in April 2020 to help small and medium sized businesses struggling as a result of the Covid-19 emergency. Businesses could borrow between £2,500 and up to 25% of their turnover, up to a maximum of £50,000. In total 1.2million loans were given totalling £36.9Billion. The National Audit Office report of October 2020<sup>7</sup> estimated that ‘total credit and fraud losses of between 35% and 60%,’ The Insolvency profession will continue to see the fall out of this in insolvency appointments over the next few years. IPs and their staff need to understand the risks and potential indicators and need appropriate reporting methods including SAR and S218<sup>8</sup> report requirements. IPs are likely to see abuse of other Covid -19 support measures such as abuse of the furlough scheme. If the actions result in criminal property, then they should be reported accordingly. The IPA expects to see robust CDD and compliance with [SIP2](#).

#### *b) Personal Insolvency*

The risk from personal insolvencies are inherently low especially in the IVA market but due to the number of cases involved (circa 260,000 open IVA cases during the year) there is a higher risk of occurrence and IPs should be mindful of the risks and have strategies to minimize risk and be able to identify any [reg flags](#).

[The National Strategic Assessment of Serious Organised Crime](#) report also highlighted potential concerns from members of the public being recruited as money mules. Given the vulnerability and pressures of insolvency it is likely that insolvent individuals may be more susceptible to engaging in such activities. Offenders may seek to recruit mules by:

- Asking people, in person or online, to receive or transfer money into or from their bank accounts, offering a cut in return. Alternatively, providing people with cash and paying them a nominal fee to purchase goods for shipment overseas, to minimise traceability.

---

<sup>6</sup> [DEAR INSOLVENCY PRACTITIONER Issue 117 – December 2020](#)

<sup>7</sup> National Audit Office [Investigation into the Bounce Back Loan Scheme \(nao.org.uk\)](#)

<sup>8</sup> [S218 \(4\) of the Insolvency Act 1986](#)

- Conning people into becoming mules unwittingly, by asking for bank details via seemingly genuine job adverts. Signs of recruitment include adverts proclaiming, 'easy job; work from home; big cash pay-outs' or 'instant money; minimal hours.'

Identified mules may have their accounts closed, be unable to obtain new accounts, phone contracts or credit, and can face prison terms of up to 14 years. The website [www.moneymules.co.uk](http://www.moneymules.co.uk) contains further advice. The report on [Chinese underground banking](#) has potential for links to be identified in both personal and corporate accounts being compromised. These risks were highlighted to members in correspondence, VPR meetings and the IPA Annual conference 2022.

### **Scotland and Northern Ireland appointments**

This risk assessment has focused on the UK as a whole but there are important jurisdictional differences that are expected to be presented by IPs in their AML and CTF obligations. By number the vast majority of the IPA members deal predominately with England and Wales appointments. All IPs with full authorisation have the ability to take appointments in Scotland and Northern Ireland. They need to be aware of the legislative differences and review if there are different AML and CFT risks. The personal insolvency legislation for Scotland is dramatically different but there is no evidence to suggest the ML and CF risks are any different. Corporate appointments are regarded as having the same risks across the UK. 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. A separate [report](#) in June 2021 highlighted the risks posed of failing to understand or identify Mini-umbrella fraud where companies have been set up with Philippine directors to take advantage of the employment allowances. This continues to be an area of high risk. Typically, organised criminals create multiple umbrella companies, each of which artificially employs a small number of temporary workers rather than through one umbrella company.

These are set up to pretend to be small employers and fraudulently claim National Insurance Contribution and VAT reliefs that are only available to genuine small employers.

Businesses need to ensure they are not enabling such schemes.



Members based in Scotland and Northern Ireland are expected to undertake their own risk assessment and consider the market in which they operate.

### **Action on risk**

As insolvency appointments are disseminated across the full range of sectors, it is imperative that an IP can demonstrate they have appreciated the risk of working in any specific sector and that the supervised firm will 'Know the signs, report the crime.'

The IPA have issued to members the regular updates from the NCA and other authorities to highlight the impact of fraud in light of the recession and continued fallout from the Covid pandemic. IPs need to be able to demonstrate that they regularly review the emerging risks from fraud, embezzlement, exploitation of furlough and other Covid support measures along with medicine, corruption and cybercrime. The 2020 roadshow series raised awareness of these issues.

IPs should be aware of the [red flags](#) (risk indicators) of potential money laundering activity, such as some of the most common red flags across all professions, and make sure they are familiar with the indicators, and be on alert for 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, or other professionals involved been instructed at 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](#).

#### **Key risk aims for IPA supervised individuals and firms**

The IPA expects its supervised population to have processes and procedures in place that limit the risk of IPs and firms facilitating ML and TF. They should demonstrate full consideration of the following 6 principles of compliance:

- **risk assessment**
- **proportionality of procedures**
- **top level commitment**
- **due diligence**
- **communication and training**
- **monitoring and review**

IP's need to ensure that the firms risk assessment fully demonstrates knowledge of the risks associated with the IP services provided and there is a full assessment of:

- **Assets**
- **Identity**
- **Geographical Area**
- **Political Status**
- **Regular review of [emerging risks](#)**

IPs and their firms need to demonstrate contemporary knowledge of sector risks, ML and TF typologies and emerging risks. 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 as the advantage of regional based knowledge is reduced and IPs need to be reliant on more robust due diligence procedures. IPs need to consider how individuals and companies can be utilised to facilitate ML and TF and what the warning signs could look like. IPs should develop knowledge of potential areas of risk and keep track of emerging trends and this should be regularly reflected in updated risk assessment, policies and training. IPs and firms should regularly review published material by the [NCA](#), and government bodies and also an awareness of reported cases using free services such as [KYC 360](#), [transparency international](#), [RUSI](#) and [International Consortium of Investigative Journalists](#).

The biggest risk to the IPA's supervised population continues to be that they are not fully aware of the warning signs, developing techniques and emerging risks. If performed diligently the statutory obligations an IP undertakes in terms of investigation into the way in which a business was conducted, prior transactions and company/individuals assets should flag suspicions for reporting performance. The prospect of IP or their staff not seeing or suspecting "*criminal property*". [Section 340](#) of the Proceeds of Crime Act 2002 during the course of their careers is virtually impossible. The implications of failing to report suspicions are defined in the Crown Prosecution Service guidance<sup>9</sup> that they will prosecute professional for failure to disclose which is an offence is committed 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

---

<sup>9</sup> [CPS Money Laundering Offences11 June 2021 Updated: 2 June 2021](#)

information on which his knowledge or suspicion is based as soon as is practicable after the information comes to him.

### **Supervisory Risks**

The [FATF assessment of Risk-based supervision](#) which was published in March 2021 is a useful reference point and defined some supervisors as just using AML supervision as a tick box exercise. The IPAs continual improvement in risk-based supervision is starting to return results with SAR numbers increasing, technical queries increasing and increased feedback from training material and events to raise awareness of risks. Published sanctions also assist in delivering the key messages.

Education and information sharing with the supervised population is a key strategy for the IPA. Raising awareness of risks in the sector is seen as a key drive to improve the effectiveness of identifying and reporting suspicious activity

*IPA Sector Risk Assessment October 2022*