Legal Sector Affinity Group
Anti-Money Laundering Guidance for the Legal Sector
2021

Contents:

Contents

1. The Status of this Guidance and Terminology Used

1.1 Status

This draft guidance replaces previous guidance and good practice information on complying with AML/CTF obligations.

This guidance is issued by the Legal Sector Affinity Group, which comprises the AML Supervisors for the legal sector.

The authors will aim to keep this guidance up to date with new legislation as it comes into force, but this guidance cannot be regarded as a definitive statement of the law or of the effect of the law, and does not comprise, and should not be relied on as giving, legal advice. It has been prepared in good faith, but neither the Legal Sector Supervisors nor any of the individuals responsible for or involved in its preparation accept any legal responsibility or liability for anything done in reliance on it.

Practice Units are not required to follow this guidance, however legal sector supervisors will consider whether a legal professional has complied with this guidance when undertaking its role as regulator of professional conduct, and as a supervisory authority for the purposes of the Regulations. You may be asked by your regulatory body to justify a decision to deviate from this guidance.

Some independent legal professionals are authorised and regulated by the FCA because they are involved in mainstream regulated activities, e.g., advising clients directly on investments such as stocks and shares. Those professionals should also consider the Joint Money Laundering Steering Group's guidance.

This guidance has been submitted to HMT for approval. In accordance with sections 330(8) and 331(7) of the Proceeds of Crime Act 2002, section 21A(6) of the Terrorism Act 2000, and Regulation 86(2)(b) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, the court is required to consider compliance with this guidance in assessing whether a person committed an offence or took all reasonable steps and exercised all due diligence to avoid committing the offence.

1.2 Terminology

This guidance uses “must,” “should” and “may” throughout to contextualise how to understand the various directions.

The terms have the below meanings:

Must – a requirement in legislation or a requirement of a regulation or other mandatory provision. You must comply, unless there are specific exemptions or defences provided for in relevant legislation or regulations.

Should – good practice for most situations. These may not be the only means of complying with the requirements and there may be situations where the suggested route is not the best option.

If you do not follow the suggested route, you should be able to justify to supervisors why your alternative approach is appropriate, either for your practice, or in the particular instance.

May – an option for meeting your obligations or running your practice. Other options may be available and which option you choose is determined by the nature of the individual practice, client or matter. You may be required to justify why this was an appropriate option to your supervisor.

2. Background

This guidance has been written both as a result of the changes made to The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 by The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 that came into force on 10 January 2020 and an extensive review of the previous guidance by the Legal Sector Affinity Group.

These iterative pieces of legislation will be referred to collectively as “the Regulations” throughout this guidance.

This guidance has been submitted to HMT for approval.

The guidance has two over-arching goals:

- First, it intends to provide practical information for legal practices in scope of the Regulations to aid their compliance and to effectively protect against Money Laundering and Terrorist Financing risks; and,
- Second, it aims to communicate supervisors’ expectations for those they supervise.

It is not the intention of this document to cover every eventuality. In reviewing it, we have aimed to strike a balance between specificity where helpful and providing the tools that legal practices need in order to deal with any given scenario. The risk-based approach (RBA), which is a long-established principle within Anti- Money Laundering (AML), acknowledges that every situation is different and that the legal practitioners and practices themselves are best placed to understand the risks and deal with them proportionately.

The guidance is separated into two parts:

- **Part 1** includes the guidance, generally applicable for legal practices; and,
- **Part 2** includes guidance for particular sectors (including barristers).

The guidance for barristers in Part 2 has been written recognising the specific nature of the Bars and the risks to which they are exposed. In particular, it recognises that most barristers are self-employed, do not engage directly with the lay client and are limited by their regulation in the scope of practice, which means that they do not hold client money or manage their clients’ affairs. Barristers should read Part 2 in the first instance, drawing on Part 1 for further detail where relevant.

Likewise, the Part 2 guidance makes clear that most work undertaken by notaries *(or in Scotland, solicitors acting solely in a notarial capacity)* in their core role as public certifying officers will fall outside the scope of the Regulations.

3. High-Level Compliance Principles

3.1 Introduction and context

The Regulations set out requirements which must be adhered to. These, in addition to the compliance principles below, should be viewed as the "building blocks" for creating robust AML policies, controls and procedures.

The guidance in Part 1 and Part 2 provides additional information and support to help in adhering to these principles.
All legal practices must consider whether their business brings them into scope of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) ("the Regulations"), through any of the qualifying activities but particularly those stated in R12.

If a legal practice deems itself to be in scope, it is a "relevant person" for the purposes of the Regulations. We will generally refer to a relevant person as a "practice" throughout the guidance.

All Relevant Persons must demonstrate to their supervisor that they have adopted a risk-based approach to the management of Money Laundering (ML) and Terrorist Financing (TF) risk within their businesses.

This guidance is intended to address issues faced by relevant persons that are drawn into scope of the Regulations

3.2 Compliance Principles

The following compliance principles are the key areas to address when trying to ensure a practice is compliant with the Regulations .

<u>AML Governance:</u>

1. All current beneficial owners, officers and managers must be approved by their supervisory authority in accordance with R26.
2. Practices must appoint a MLRO (Money Laundering Reporting Officer) who is responsible for receiving disclosures from staff of suspected money laundering and determining whether they warrant the submission of a suspicious activity report (SAR) to the National Crime Agency (NCA). This individual is responsible for the submission of SARs to the NCA where appropriate. The practice must notify its supervisory authority of this appointment within 14 days of the date of the appointment.
3. Where appropriate to the size and nature of the practice a member of the board (or equivalent) or of senior management must be appointed to be responsible for compliance of the practice with the Regulations. This position is referred to as the Money Laundering Compliance Officer (MLCO). The practice must notify its supervisory authority of this appointment within 14 days of the date of the appointment
4. The Board Level Person may delegate the operational day to day AML compliance work of the practice to the MLRO though cannot delegate responsibility/accountability. This delegation must be documented

5. The AML duties/responsibilities of all partners and employees of the practice should be adequately documented
6. The AML policies, controls and procedures (PCPs) of the practice must be approved by the practice's senior management (and/or board). This approval must be documented
7. The Board (or equivalent) must monitor and manage compliance with AML PCPs. Board discussions and decisions regarding AML compliance must be documented
8. All practices must allocate adequate and competent resource to the management of AML/TF risks
9. Procedures (including robust, easily accessible record keeping) must be in place to ensure comprehensive and timely reporting and submissions to relevant supervisory authorities

Practice-Wide Risk Assessment:

10. Practices must have a written, up-to-date practice-level risk assessment in place, in line with R18 requirements.
11. Practices must use this to directly inform their AML PCPs.

Client/Matter Level Risk Assessment:

Practices must have:

12. Client and matter level ML/TF risk assessment procedures that include a requirement to undertake a written risk assessment on each new client and matter/retainer particularly where the matter is non-repetitive.
13. A documented procedure for the application of client/matter level risk assessment outcomes to the due diligence undertaken on any particular client/matter.

AML Policies, Controls and Procedures:

The practice must have clearly documented PCPs based on their practice-wide risk assessment which include:

14. The AML governance arrangements of the practice

Client Due Diligence:

The practice must have clearly documented PCPs based on their practice-wide risk assessment which include:

15. Client Due Diligence procedures (including procedures to identify the ownership and control structures of non-natural persons)
16. Identification and verification (ID&V) procedures relating to natural persons (this includes ID&V procedures in relation to the ultimate beneficial owners of non-natural clients, and those purporting to act on behalf of a client)
17. Procedures to facilitate a clear understanding of the client's source of wealth and funds in relation to a transaction, and the level of evidence required, in line with the risk profile of the client/matter.
18. Procedures to facilitate reporting of discrepancies between Beneficial Ownership information obtained through due diligence checks and what is held on the Companies House register
19. Enhanced Due Diligence procedures – including the provision of adequate controls to manage higher risk clients/transactions, and measures to establish Source of Funds/Source of Wealth where appropriate
20. The practice's position on the use and application of Simplified Due Diligence.
21. The timing of any due diligence procedures

22. The practice's position on the use of R39 Reliance and any related procedures
23. The ongoing monitoring of clients and their matters
24. The identification of instances where it is required or appropriate to re-apply or renew CDD or EDD on a client
25. Dealing with the return of un-solicited or apparently accidentally deposited funds
26. Identification and scrutiny of any complex or unusually large transactions, or an unusual pattern of transactions, or those which serve no apparent economic or legal purpose
27. Any additional measures to prevent products/transactions that support anonymity being used for ML/TF
28. Identification of Politically Exposed Persons (PEPs), their relatives or close associates and the control of any associated risks

Suspicious Activity Reporting:

29. The practice must have procedures setting out how, and in what circumstances an internal disclosure should be submitted to the Nominated Officer (MLRO)

Technology:

The practice must have clearly documented PCPs based on their practice-wide risk assessment which include:

30. Measures taken when new technology is adopted to protect against ML or TF risks
31. Where practices use electronic identification and verification (EID&V) tools they should document the role of the tool, the data sources it uses, and in what circumstances (clients/matters) it is appropriate to use the solution

Training

The practice must have clearly documented PCPs based on their practice-wide risk assessment which include:

32. Measures deployed to ensure AML relevant training of partners, staff and agents, including the maintenance of records relating to such training. This training must include awareness of MLR, Proceeds of Crime Act Part 7 and Terrorism Act Part 3 reporting requirements, legal professional privilege and data protection requirements. Training should also cover recognition of red flags/risk indicators as relevant to their duties and responsibilities, along with other relevant laws
33. Procedures for the communication of PCPs to partners and staff

Internal Controls

Where appropriate to the size and nature of the practice:

34. The practice must conduct an independent audit of the adequacy and effectiveness of its AML policies, controls and procedures
35. The practice must undertake screening of relevant employees – both at pre-employment stage and on an ongoing basis

Record Keeping

36. The practice must have procedures relating to records keeping and related data protection matters

4. AML Governance and Policies, Controls and Procedures

4.1 Overview

This section outlines the Anti- Money Laundering (AML) roles, responsibilities, and appointment of senior individuals in a practice including the Money Laundering Reporting Officer (MLRO), Money Laundering Compliance Officer (MLCO), and beneficial owners, officers, and managers (BOOMs), as well as some of the structures that practices must or should put in place (e.g., training and independent audit.)

Note that sole practitioners will fulfil the responsibilities of all role holders mentioned in this section, but rather than having any duty to report matters internally within their practice, they must instead record such information in writing (e.g., records of SARs).

Relevant Compliance Principles

1. All current beneficial owners, officers and managers must be approved by their supervisory authority in accordance with R26.
2. Relevant Persons must appoint a MLRO (Money Laundering Reporting Officer) who is responsible for receiving disclosures from staff of suspected money laundering and determining whether they warrant the submission of a suspicious activity report (SAR) to the National Crime Agency (NCA). This individual is responsible for the submission of SARs to the NCA where appropriate. The practice must notify its supervisory authority of this appointment within 14 days of the date of the appointment.
3. Where appropriate to the size and nature of the practice a member of the board (or equivalent) or of senior management must be appointed to be responsible for compliance of the practice with the Regulations. This position is referred to as the "Board Level Person" or Money Laundering Compliance Officer (MLCO). The practice must notify its supervisory authority of this appointment within 14 days of the date of the appointment
4. The Board Level Person may delegate the operational day to day AML compliance work of the practice to the MLRO though cannot delegate responsibility/accountability. This delegation must be documented
5. The AML duties/responsibilities of all partners and employees of the practice should be adequately documented
6. The AML policies, controls and procedures (PCPs) of the practice must be approved by the Relevant Person's senior management (and/or board). This approval must be documented
7. The Board (or equivalent) must monitor and manage compliance with AML Policies, Controls & Procedures (PCPs). Board discussions and decisions regarding AML compliance must be documented
8. All Relevant Persons must allocate adequate and competent resource to the management of AML/TF risks
9. Procedures (including robust, easily accessible record keeping) must be in place to ensure comprehensive and timely reporting and submissions to relevant supervisory authorities

4.2 Approvals, Roles and Positions

The Regulations specify the roles and responsibilities of certain individuals in a practice. These are the:

- Beneficial Owners.
- Officers.
- Managers.
- MLRO; and,
- MLCO or "Board Level Person".

4.2.1 Beneficial Owners, Officers and Managers

Under R26, you must gain approval from your supervisor for all BOOMs at your practice before the practice can undertake any of the activities that fall under the Regulations.

Those acting as BOOMs without approval, could be subject to summary conviction and a prison term of up to three months or a conviction on indictment and a prison term of up to two years.

Definition of a BOOM

Beneficial Owner (R5)

(1) In these Regulations, "beneficial owner", in relation to a body corporate which is not a company whose securities are listed on a regulated market, means:

a) any individual who exercises ultimate control over the management of the body corporate;
b) (any individual who ultimately owns or controls (in each case whether directly or indirectly), including through bearer share holdings or by other means, more than 25% of the shares or voting rights in the body corporate; or
c) any individual who controls the body corporate.

(2) For the purposes of paragraph (1)(c), an individual controls a body corporate if:

a. the body corporate is a company or a limited liability partnership and that individual satisfies one or more of the conditions set out in Part 1 of Schedule 1A to the Companies Act 2006 (people with significant control over a company); or
b. the body corporate would be a subsidiary undertaking of the individual (if the individual were an undertaking) under section 1162 (parent and subsidiary undertakings) of the Companies Act 2006 read with Schedule 7 to that Act.

(3) In these Regulations, "beneficial owner", in relation to a partnership (other than a limited liability partnership), means any individual who:

a) ultimately is entitled to or controls (in each case whether directly or indirectly) more than 25% share of the capital or profits of the partnership or more than 25% of the voting rights in the partnership;

b) satisfies one or more the conditions set out in Part 1 of Schedule 1 to the Scottish Partnerships (Register of People with Significant Control) Regulations 2017 (references to people with significant control over an eligible Scottish partnership); or
c) otherwise exercises ultimate control over the management of the partnership.

(4) In this regulation "limited liability partnership" has the meaning given by the Limited Liability Partnerships Act 2000.

"Officer" (R3)

(a) in relation to a body corporate (including LLPs), means:

i. a director, secretary, chief executive, member of the committee of management, or a person purporting to act in such a capacity, or
ii. an individual who is a controller of the body, or a person purporting to act as a controller.

(b) in relation to an unincorporated association, means any officer of the association or any member of its governing body, or a person purporting to act in such a capacity.
(c) in relation to a partnership, means a partner, and any manager, secretary or similar officer of the partnership, or a person purporting to act in such a capacity.

"Manager" (R3)

in relation to a practice, means a person who has control, authority or responsibility for managing the business of that practice, and includes a nominated officer (MLRO).

4.2.2 Who might be a BOOM?

Without contravening or limiting the definitions in the Regulations, the individuals you should particularly consider seeking approval for as BOOMs include:

- Beneficial Owners: partners who exercise significant control, owners (of a share of 25% or more), those with significant control of the entity (through ownership, voting rights or otherwise).
- Officers: partners who exercise significant control, Executives (e.g., CEO, CFO, CTO), Managing Directors, Board members or equivalent; and,
- Managers: will often include roles sitting below the Officers, including senior leadership team, heads of departments or practice areas.

4.2.3 Approval of BOOMs

The test that must be applied by supervisors is whether an applicant has been convicted of any of the offences in Schedule 3 of the Regulations. If the applicant has no such conviction, the supervisor must approve the application, and can apply their own processes to assess the application.

The updated regulations require applications to include "sufficient" information for the supervisor to determine whether the test is met. You must follow the directions of your supervisor and provide them with the information they require to establish that the applicant

does not have any relevant convictions (this will often take the form of a criminal record check).

Approval must be granted prior to any activity that would bring the practice or the individual into the scope of the Regulations. This is equally relevant to established practices as new ones. Established practices must seek approval for new BOOMs before they take up their role.

Individuals may not be able to port their approval from one practice to another and should clarify the processes and specifics of this with their own supervisor.

If an approved BOOM is convicted of a relevant offence under Schedule 3 their approval will cease to be valid and:

- the individual must cease all activities in scope of the Regulations and notify their supervisor within 30 days starting from the date of the conviction: and,
- the practice must report the conviction within 30 days, starting from the date they became aware of it.

When someone ceases to act as a BOOM, you should notify your supervisor within 14 days.

4.3. Money Laundering Reporting Officer (otherwise known as Nominated Officer)

R21(3) requires all practices to have a nominated officer (MLRO) to receive disclosures for possible submission to the National Crime Agency (NCA) under Part 7 of POCA and TACT.

R21(6) provides that there is no requirement to appoint a MLRO if you are an individual who provides regulated services, but do not employ or act in association with anyone else. In this case the duties of the MLRO will fall with you.

4.3.1 Who should be MLRO?

Your MLRO should be:

- of sufficient seniority to make decisions on reporting which can impact your practice's business relations with your clients and your exposure to criminal, civil, regulatory and disciplinary sanctions.
- in a position of sufficient responsibility to have access to all client files and business information. This will allow them to make decisions on the basis of all information held by the practice; and,
- supported and empowered in the carrying out of their duties by Senior Management.

The MLRO may be a member of the Board of Directors (or equivalent Senior Management body) or able to attend their meetings and should be able to directly report to the board on how the practice is fulfilling its obligations and compliance work in this area.

You should consider whether the person you are appointing has access to sufficient resources in order to be able to effectively fulfil the role, especially if the MLRO is also undertaking other duties.

Practices authorised by the Financial Conduct Authority (FCA) must obtain the FCA's approval for the appointment of the MLRO as this is a controlled function under section 59 of the Financial Services and Markets Act 2000.

4.3.2 Role of the MLRO

Your MLRO is responsible for ensuring that information leading to knowledge or suspicion, or reasonable grounds for knowledge or suspicion of money laundering is properly disclosed to the NCA. The decision to report, or not to report, must not be subject to the consent of anyone else. Your MLRO may liaise with the NCA or law enforcement on whether to proceed with a given transaction or what information may be disclosed to clients or third parties.

The MLRO has a personal responsibility to ensure they fulfil their duties and may be subject to conviction under s.331 of the Proceeds of Crime Act, 2002, for a failure to disclose information to the NCA.

A range of factors, including the type of practice, its size and structure, may lead to the MLRO delegating certain duties regarding the practice's AML/CTF obligations.
All practices must consider arrangements for temporary cover when the MLRO is absent. You may appoint one or more deputy MLROs where appropriate in order to ensure the work is sufficiently resourced and continuously covered. The MLRO and any deputies must have unrestricted and direct access to the NCA SARs online system and the internal records of SARs at the practice.

An MLRO may also be empowered with further duties under delegation from senior management or the Board of the practice, however the delegating party will retain accountability. For example, an MLRO may be appointed responsible by the Board or MLCO for the creation, management and review of the practice's Policies, Controls and Procedures (PCPs) under R19.

An MLRO should consider whether and in what form the content of their disclosures to the NCA should be reported to senior management or their Board.
The identity of the MLRO and deputies should be known to all relevant staff and should be noted in the PCPs.

4.3.3 MLRO Reporting (to the Senior Management Body)

The MLRO should submit an annual report (more frequent reporting may be determined appropriate by the Board or equivalent Senior Management Body) setting out:

- changes to the AML/CTF risks of the practice.
- advised improvements to be made in the coming year.
- progress on any past improvements.
- the results of any internal auditing.
- resourcing concerns/considerations.
- any interactions with their supervisor.
- AML staff training undertaken.
- key information, for example regulatory changes or notable publications/guidance from AML authorities; and,

- other information, for example, trends, deficiencies, lessons relating to SARs made by the practice.

The MLRO may also be the appropriate person to record the AML compliance responsibilities of individuals at the practice.

4.3.4 Responding to enquiries from law enforcement agencies

In accordance with R21(8), a practice must establish and maintain systems which enable it to respond fully and rapidly to enquiries from law enforcement agencies as to:

(a) whether it maintains, or has maintained during the previous five years, a business relationship with any person; and
(b) the nature of that relationship.

In responding to enquiries, practices must consider the privileged nature of any information they hold before sharing it.

Record keeping that meets the requirements of the Regulations will help a practice to comply with these requirements. A practice may appoint the MLRO as the lead person to act as liaison with law enforcement.

4.4 Money Laundering Compliance Officer (MLCO)

R21(1)(a) requires that where appropriate to the size and nature of the business, a practice must appoint a member of the Board (or equivalent management body) or member of the senior management team (the 'Board-Level Person') as being responsible for the practice's compliance with the Regulations. This role is commonly known as the Money Laundering Compliance Officer, or MLCO.

The general focus of this role is being a lead within the senior management of the practice, supporting the work of the MLRO and ensuring that the AML efforts of the practice have appropriate oversight and engagement at the highest level.
The MLCO should have:

- an understanding of the business, its service lines and clients.
- sufficient seniority to direct the activities of all members of staff (including senior individuals) and to influence resourcing levels and AML controls.
- the authority to ensure the business' compliance with the regime; and,
- the time, capacity, and resources to fulfil the role.

4.5 Practices with both a MLRO and a MLCO

You may appoint the same individual to fulfil both the MLRO and MLCO roles.
However, the larger, the more complex and the higher the risk exposure of the practice, the greater the rationale is for appointing separate people to the roles, in order to better resource the compliance efforts. This should be balanced against the possible advantages and synergies of having one person fulfil both.

The MLCO may delegate some of the operational aspects (though never responsibility/accountability) of the day-to-day AML compliance of the practice to the MLRO or other individuals. These delegations must be documented, and roles/responsibilities clearly defined.

When appointing people to the MLRO/MLCO roles, Senior Management should have regard to the risk of any possible conflicts of interest they may face (particularly with any fee-earning duties the MLRO/MLCO may retain) and address this in the policies of the practice. This may be adequately addressed by the general conflicts of interest policy in the practice.

Senior management should also have regard to the amount of resource they have dedicated for the purpose of allowing their MLRO and MLCO to adequately fulfil their duties (e.g., time and access to support staff).

In considering the issue of resource, it is worth highlighting that although it may not be common practice, there is nothing to prevent MLRO/MLCO roles rotating among a group of individuals, as long as they all meet the requirements. This can be particularly advantageous when rotating the lead role (e.g., MLRO) among a group of deputies, as it spreads resource demand while also ensuring deputies are experienced at taking over the lead when required.

4.6 Senior Management Responsibilities

Senior management refers to any officer or employee of the practice with sufficient knowledge of the practice's money laundering and terrorist financing risk exposure, and of sufficient authority, to take decisions affecting its risk exposure.

Senior management should ensure the MLRO/MLCO has:

- active support.
- adequate and competent resources (staff, time, budget, technology, training see Section 8 for further information).
- independence of action.
- access to the relevant information; and
- to be able to fulfil their duties.

Senior Management must mitigate and effectively manage their ML/TF risks via the implementation and approval of PCPs (R19(2)(b)). Reporting by MLROs may assist Senior Management in their efforts to assess and address the practice's efforts to this end.

Any decisions made by Senior Management on issues of AML compliance should be documented and tracked over time. The Practice Wide Risk Assessment should be signed off by Senior Management along with all revisions of this document.

It is important that the Senior Management of a practice is informed and engaged with their responsibilities under the Regulations. They should consider any information their MLRO/MLCO shares with them about ML/TF risk.

Senior Management are also responsible under the Regulations for providing approval for the practice to be able to establish or continue a business relationship with a PEP or a close family member or known associate of a PEP or to enter into business relationships with clients established in high risk third countries.

4.7 Informing your Supervisor of MLRO and MLCO Appointments

You must inform your supervisor of the identity of your MLRO (this must be a specific individual) and where relevant your MLCO within 14 days of appointment (R21(4)(b)).

You must also inform your supervisor of any subsequent appointments to either of those positions within 14 days. If you are operating a rotating model of MLROs among more than one person, the above requirement to inform your supervisor must be met whenever a new person takes over the lead position.

Note that an MLRO will automatically be a manager and must therefore be approved as a BOOM (R26) prior to their appointment. If you are using a rotating model, you should consider all the individuals among whom the role is rotating as BOOMs and get them approved as such.

4.8 Policies, Controls and Procedures (PCPs)

4.8.1 What must be included in PCPs?
R19 requires that practices establish and maintain written policies, controls and procedures (PCPs) for identifying, managing and mitigating the risks identified in the Practice Wide risk assessment (see 5.3 for more information on the Practice Wide Risk Assessment.), The PCPs must be proportionate to the size and nature of the practice unit, documented and must be approved by senior management (this approval should be documented). PCPs should be reviewed and updated regularly. You must record all changes made to these documents over time.

The PCPs must set out your practice's approach to practical AML compliance activities. They must be communicated and made available to all relevant employees, unambiguous and clearly worded. Their content should form one of the core elements of your relevant AML training for all relevant employees, and you must record the steps undertaken to communicate them to relevant employees within your practice.

PCPs must include procedures for the identification of matters that:

- Are unusually complex.
- Are unusually large.
- Have an unusual pattern of transactions.
- Have no apparent economic or legal purpose.
- Are at high risk (i.e., "particularly likely") of being related to money laundering or terrorist financing (see sections 5 and 18);
- Involve products or services that might facilitate anonymity; and
- Trigger a requirement to report a suspicious activity report (see section 11)

- The PCPs must document the practical steps your practice will take when these instances are identified.

They must also set out your procedure for assessing and mitigating the risks of introducing new technology into your practice (see section 7).

PCPs must document the firms approach to compliance across the following areas:

- risk management practices (see sections 5 and 6).
- internal controls (see regulations R21-R24 and section 9).
- customer due diligence (CDD) including the nature and extent of identification of checks to be done under simplified, standard and enhanced due diligence (see R27-R38 and section 6).
- reliance and record keeping (see R39-R40 and sections 6 and 10).
- the monitoring and management of compliance with, and the internal communication of the PCPs (see sections 8 and 9).

4.8.2 Monitoring Compliance with PCPs

Practices must ensure that they regularly review and update their risk assessment and PCPs.

Monitoring compliance will assist you to assess whether the PCPs that you have implemented are effective in identifying and mitigating risks within your practice. Issues which should be addressed include:

- Procedures to be undertaken to monitor compliance, e.g., random file audits or file checklists to be completed before opening or closing a file;
- Reports to be provided to senior management on compliance (see s. 4.3.3)
- How to rectify lack of compliance, when identified; and

How findings or lessons learnt will be communicated to staff and fed back into the risk profile of the practice.

Practices (except sole practitioners) must also have PCPs clearly setting out the process and requirements for making a disclosure to the National Crime Agency under POCA and the Terrorism Act. For further details on Suspicious Activity Reporting see section 11.

4.8.3 Group Level PCPs

Where a practice is a parent undertaking of a group, it must ensure that its PCPs apply to all branches or subsidiary undertakings. This includes those located outside the UK, and all branches established outside the UK, which carry out activities that would fall in the regulated sector in the UK. Steps must be taken to communicate PCPs to all relevant non-UK branches or subsidiary undertakings.

Where the subsidiaries or branches are in an EU state, the PCPs need to reflect the requirement that that these subsidiaries and branches must follow the local law transposing the fifth money laundering directive. The parent undertaking will be held responsible for the conduct of its subsidiaries and branches.

Subsidiary undertakings or branches of a parent in a non-EU country which does not impose equivalent AML requirements must ensure that they impose UK-equivalent requirements where legally allowable.

If local laws prevent application of equivalent requirements the parent undertaking must:

- inform its supervisory authority; accordingly, and

- take additional measures to handle the risk of money laundering and terrorist financing effectively, which must be clearly documented.

5. AML Risk Assessments

Relevant Compliance Principles

Practice-Wide Risk Assessment:

10. Relevant Persons must have a written, up-to-date practice-level risk assessment in place, in line with R18 requirements.
11. Relevant Persons must use this to directly inform their AML PCPs.

Client/Matter Level Risk Assessment:
Practices must have:

12. Client and matter level ML/TF risk assessment procedures that include a requirement to undertake a written risk assessment on each new client and matter/retainer particularly where the matter is non-repetitive.
13. A documented procedure for the application of client/matter level risk assessment outcomes to the due diligence undertaken on any particular client/matter.

5.1 Risk Assessments and the Risk Based Approach

A core principle of AML compliance is taking a risk-based approach (RBA). In short, an RBA refers to adjusting the level and type of compliance work done (frequency, intensity and/or amount), to the risks present. In order to apply an RBA, it is necessary then to have information on the risks inherent to your practice and in any particular client or matter – and the pertinence of these risks which is why these assessments are so important. If you have not fully assessed the risks present across your business or in any particular client or matter, you cannot then apply appropriate controls to mitigate those risks adequately and effectively.

The resulting benefits of this approach include:

- more efficient and effective use of your resources, proportionate to the risks faced;
- minimising compliance costs and administrative burdens on practices and clients; and
- greater flexibility to respond to emerging risks as money laundering and terrorist financing methods change.

Please be aware that the risk-based approach does not apply to reporting suspicious activity, because POCA and the Terrorism Act lay down specific legal requirements not to engage in certain activities (without appropriate consent) and to make reports of suspicious activities once a suspicion is held. Equally it does not apply to the UK and international sanction regime, where requirements are absolute, as opposed to risk-based, in nature.

Being used to facilitate money laundering and terrorist financing poses many risks, including:

- criminal, regulatory and disciplinary sanctions for the practice and individuals in the practice;
- civil action against the practice and individuals in the practice; and
- damage to reputation leading to a loss of business.

These risks must be appropriately identified, assessed and mitigated, like any business risks facing your practice.

Consideration should be given to the resources that can be reasonably allocated to implement and manage an appropriately developed RBA. For example, a sole practitioner or other smaller practice would not be expected to devote an identical level of resources as a large practice. Instead, the sole practitioner would be expected to develop appropriate systems and controls and an RBA proportionate to the scope and nature of the practice and its clients.

Just because a practice is smaller and serves a smaller quantity of clients at any given time, does not necessarily mean that it is lower risk. Smaller practices may be targeted more than large law practices by money launderers, as they may be perceived as lacking resources to effectively guard against them. Equally, smaller practices may practice higher risk types of work, develop a niche in services or have cultural, social or language connections or other features which may be attractive to money launderers.

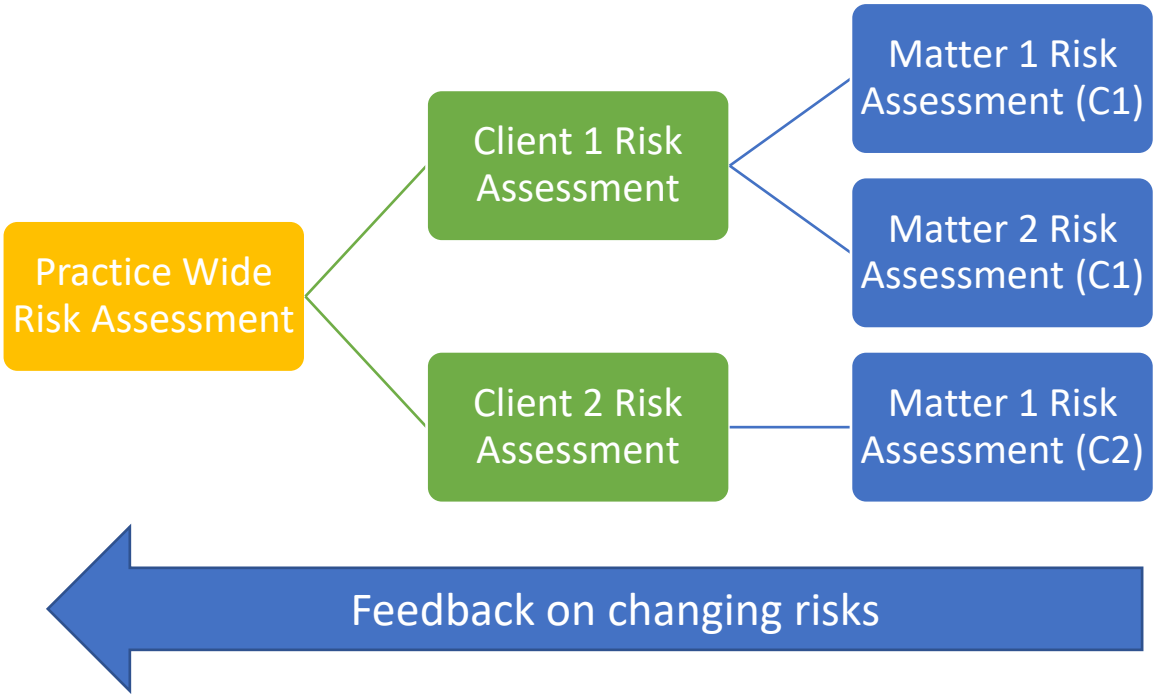
Finally, it is worth keeping in mind that risk is a judgement relying on considering multiple factors holistically. Generally speaking, a single factor may not automatically make a matter or client high risk in and of itself, exceptions include where a client or counterparty is based in a high risk third country or is a Politically Exposed Person (PEP). It should be all the risk factors taken together that informs whether a matter or client is deemed to be high risk.

5.2 Assessing Risk

The assessing of money laundering and terrorist financing risk is an important requirement of the Regulations and a vital step in protecting your practice. There are three important levels of risk assessment:

1. **Practice Wide Risk Assessments** (PWRAs) are required by R18 and should be comprehensive in identifying and assessing all the money laundering and terrorist financing risks your practice faces. The PWRA is central and fundamental to the AML controls implemented across your business and needs to address certain issues, prescribed by the Regulations.
2. **Client risk assessments** should identify and assess the ML/TF risks identified at individual client level.
3. **Matter risk assessments** should be undertaken on each new matter for a client, particularly where risks are novel or non-repetitive.

As new risks are identified at matter/client level, these should inform and allow the updating of higher-level assessments, i.e., the client risk assessment and/or the PWRA.



The relationship between the various levels of risk assessment

5.3 Practice Wide Risk Assessment (PWRA) - Introduction

Under Regulation 18(1) a practice must carry out and maintain a documented (i.e., written) PWRA to identify and assess the risk of money laundering and terrorist financing to which it is subject. This is separate to assessments of risk for individual clients or matters. Your PWRA must be made available to your supervisory authority upon request. Under R18 the PWRA must address risk factors relating to:

- your clients (e.g., demographics, PEPs or close relatives or associates of PEPs);
- the countries or geographic areas in which your business operates (e.g., UK, EU, high risk third countries) or the countries/geographic areas to which your clients are linked or derive their income from;
- your products or services (e.g., conveyancing, tax advice, forming of trusts, client bank accounts);
- your transactions (e.g., size, frequency or complexity); and
- your delivery channels (e.g., online or via apps or portals, in person, remotely).

You must also take into account information made available to you by your supervisory authority's sector risk assessment including information published under R17 and R47, likely including the information from the national risk assessment prepared under R16.

The PWRA is the central reference point for how a practice protects itself from money-laundering and terrorist financing. The better the quality of the PWRA, the easier it will be for

the practice to take a risk-based approach to protecting their business, which allows for greater efficiency and efficacy.

The PWRA must be comprehensive, tailored to the practice, accurate and kept up to date.

For the avoidance of doubt, the PWRA must be a distinct written document. You should retain copes of all previous versions of your PWRA for reference and to evidence your continued compliance.

Your PWRA should be reviewed, discussed and approved by Senior Management. All steps taken to review the risk assessment must be recorded and the date of last review should be recorded.

Templates may be used and can be useful tools to help compliance. You may contact your supervisor to check if they recommend a specific template.

Some supervisors have also observed that some high-quality risk assessments have avoided a template approach helping them to tailor the PWRA directly to the needs of the practice.

It is also worth noting that documents detailing the AML policies, controls and procedures are not in and of themselves a compliant PWRA or a suitable proxy or alternative for one. The PWRA should guide the development of effective, risk-based PCPs under R19.

5.4 Assessing your practice's risk profile

As well as addressing the mandatory risk areas listed in R18, and the other mandatory documents (information published by your supervisor including where relevant content from the national risk assessment) you should consider any general issues raised in SARs made by your MLRO and consult the key people (including partners, fee earners but also compliance staff or others dealing with AML-related risk assessment or administration) in your organisation to understand any risks they may have identified.

It is important to recognise that any amount of exposure to areas of higher risk may impact on the risk profile of the practice.

Your PWRA may also include consideration of:

- the EU's Supra-National Risk Assessment;
- the FATF Risk-based Approach Guidance for Legal Professionals;
- any relevant FATF mutual evaluations of jurisdictions where you provide services or jurisdictions to which your clients are linked;
- non-UK national risk assessments, or publicly available materials in respect of the risks in other jurisdictions in which you offer or provide services;
- relevant material made available by your supervisor or representative or industry body highlighting possible risks, e.g., relevant thematic reviews published by your supervisor, or any other information made available from recognised sources such as the FCA or the Financial Industry's Joint Money Laundering Steering Group (JMSLG) where relevant to your practice; and
- any other material which may be relevant to assess the risk level particular to your practice, for example, recognised press articles from reliable sources highlighting issues that may have arisen in particular jurisdictions.

Practice A	Practice B
A diverse range of clients	Smaller range of clients
Domestic and International Clients	Mostly domestic and local clients
Domestic/International matters	Mostly domestic and local matters
Many different teams/departments	One team in one office
Large number of non-natural clients	Mostly private individual clients
Non-Face to Face relationships	Mostly Face to Face relationships
Higher value matters	Lower value matters
PWRA	
More in-depth PWRA split by department/team and the services each team offers and clients it serves	Single PWRA for whole practice. Likely to be shorter and simpler

Example of how risks and the written assessment of these risks may differ across two different practices

The PWRA should provide a general overview of the practice, addressing its key features, including:

- number of partners/staff and other metrics indicating the scale of the practice;
- (where appropriate) rate of staff turnover and other aspects of staff culture;
- a description of the work areas of the practice and their relative size and significance to the business e.g., in terms of frequency and staff time;
- types of clients served;
- length/depth of client relationships/stability of client base; and,
- location of the practice (including the local catchment area) and where relevant, any international exposure the practice might have.

Does the practice have a high turnover of clients?
Does the practice mostly deal with clients face to face?
Does the practice act for clients across both criminal and civil matters?
Does the practice have clients who may be subject to simplified due diligence, such as public authorities or FCA registered financial institutions?
Does the practice have PEPs on its client list?
Does the practice have clients who run high cash turnover businesses or high value goods businesses, or operate in higher risk sectors?
Does the practice undertake work for corporate clients who have complex or multiple layers of ownership, or have links to international/offshore jurisdictions?

Sample questions to consider in the general overview section of the PWRA

5.5 Reviewing the PWRA

The PWRA is a living document and should be kept under continual review. A practice should undertake periodic reviews (at least every one to two years) to help maintain the accuracy of the PWRA and review emerging risks. It is also important to ensure that the PWRA reflects changes in the practice.

R18(4) requires you to record all steps taken to review the PWRA, which may include consideration of any changes to the level of risk to the practice pertaining to each of the five risk areas listed in the Regulations. These steps may include interviews with appropriate individuals across the practice, and reviews of recent client/matter risk assessments in order to assess whether these have an impact on the overall risks to the practice etc.
You should consider triggers for a review to include:

- providing a new product or service;
- using a new piece of technology in the delivery of your services or in complying with the Regulations;
- a change in the Regulations;
- taking on a new client (particularly a PEP or family member or known close associate of a PEP) or a new type or class of client that presents risks not addressed by the PWRA;
- existing clients that have changed the types of legal services they use, particularly if those activities are moving from lower risk to higher risk;
- merging with or absorbing another practice including their clients;
- operating in a new jurisdiction, or changing the services offered in a given jurisdiction;
- changes in management / control structure to the practice e.g., changing incorporation type or adopting a new system of governance; significant, relevant

updates and/or guidance from regulators, supervisors and/or industry/representative bodies; and
- any significant change in the AML risk exposure of the practice.

For the avoidance of doubt, a review may determine that no changes are needed, but the review, the decision and the reasons for the decision not to change the PWRA should all be appropriately recorded.

5.6 Risk Factors for consideration at all levels of Risk Assessment

The following risk factors should be addressed at any level of your practice's risk assessments but must be considered in the context of your PWRA.

5.6.1 Client Risk Factors

When assessing client risk factors, you should begin by considering your client base. Identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow you to determine proportionate controls to mitigate them. Factors which may affect the level of risk associated with your client base are set out below and should be listed as considerations in your PWRA.

5.6.1.1 Client Turnover

You should take into account the duration and nature of your client relationships, particularly in the context of your business e.g., a practice whose main business is high volume conveyancing would be expected to have a very different client turnover to practices offering boutique or specialist services to a smaller number of clients. This may vary across the different areas of your business, and this variation should be reflected in any risk ratings you make.

If you tend to have shorter relationships and a higher client turnover, you may conclude that your practice does or will not have the opportunity to understand the client's circumstances or background in any detail, therefore the lack of a long and/or strong client relationship meaning your practice may face greater inherent AML risk, and vice versa.

5.6.1.2 Politically Exposed Persons (PEPs)

PEPs, their family members and their known close associates may present a higher risk than non-PEPs as they may be at greater risk of abusing public office for private gain and further, a PEP may use the services of the legal sector to launder the proceeds of this abuse of office.

If you act for a PEP or an entity which may be owned/controlled by PEPs, or commonly provide services which may be attractive to PEPs, you should address this directly in your PWRA and client assessments, as well as any mitigating steps you may take to guard against the risks.

Within the UK, the roles signifying that someone is a PEP are now defined in the FCA guidance (FG 17/6).

Further information regarding PEPs can be found in Section 6 of this guidance.

5.6.1.3 Clients in higher risk sectors

You should take into consideration the elevated risks attached to certain sectors when carrying out your assessments (see below).

Certain sectors have been identified by credible sources as giving rise to an increased risk of corruption and, in some countries, are subject to international or UK, UN or EU sanctions.

A new business in any sector that presents significant financial barriers to entry or may be seen as entering a new or unproven market should be considered as potentially higher risk. Where an entity has access to an illegitimate source of funding, it may find it easier to establish itself in a difficult business environment. For the avoidance of doubt, a sector is not necessarily high risk simply because it has significant financial costs to entry.

Sectors that may indicate higher risk, particularly when coupled with a high-risk jurisdiction include (but are not limited to):

- domestic and international public work contracts and construction, including post-conflict reconstruction;
- businesses utilising new or unproven technology, that might make them vulnerable to being used for money laundering;
- high value goods businesses;
- items of archaeological, historical, cultural and religious significance or of rare scientific value (this may be of particularly high risk in jurisdictions with exposure to terrorism or terrorist financing activities);
- aspects of the nuclear industry with vulnerability to proliferation risk;
- mining (including precious metals, diamonds or other gemstones and trading of these materials);
- arms manufacturing/supply and the defence industry;
- tobacco products;
- gambling;
- crypto-asset wallet providers and exchanges;
- unregulated charities (particularly those operating in higher risk jurisdictions);
- money transfer businesses;
- ivory and other items and materials related to protected species;
- real estate and property development; and
- the oil and gas industry (with the exception of the buying and selling of fuel for domestic consumption or retail).

Clearly not all work in these sectors will be higher risk in all instances, but it is essential to be aware of the higher risks inherent in these industries so that practices can implement appropriate and proportionate CDD and ongoing monitoring procedures.

Practices should consider and document whether any of these sectors are involved as part of the client or matter risk assessment and adjust risk ratings accordingly.

Where an entity is supervised for AML itself (high value goods businesses, crypto-asset wallet providers etc.) to a comparable standard, this may be seen as presenting reduced risk.

5.6.1.4 Clients with cash intensive businesses

You should consider whether your practice frequently acts for clients who operate or benefit from high cash turnover operations as these may be appealing to criminals seeking to launder money. Non-business entities may fall into this group also, including charities, where funds are coming from multiple sources and are difficult to verify, though this may be of greater risk in a terrorist financing context.

Equally you should consider the potential risks where a client has low cash turnover, but an unexplained large cash balance.

5.6.2 Geographic Risk

Geographic risk refers to the countries or geographic areas in which your business operates, receives funds from or where clients reside. It may also extend to considering any social, cultural or language ties which might increase a link to a known high risk jurisdiction country or geographic area.

In assessing this risk at PWRA level, you may want to consider the following questions:

- Does the practice operate outside of the UK/EU or equivalent jurisdictions (i.e., those where AML regulation may not be comparable) and/or in areas with potentially higher levels of corruption?
- Does the practice receive funds from jurisdictions outside the UK/EU or equivalent jurisdictions (i.e., those where AML regulation may not be comparable?
- Does the practice have a specific client-base, niche or undertake work for clients from outside of the UK/EU or equivalent jurisdictions (i.e., those where AML regulation may not be comparable)?

5.6.2.1 Higher Risk Jurisdictions

The European Commission publishes a list of 'high risk third countries', contained in Commission Delegated Regulation (EU) 2016/1675 which changes from time to time. Go to their website for the up-to-date list.

The Regulations mandate prescriptive steps where your client is established in a high risk third country, please see Section 6 for more on this.

You should note that there may be other jurisdictions that present a high risk of money laundering that are not on this list.

Resources to help you consider whether a country is high risk include:

- FATF and HM Treasury statements on unsatisfactory money laundering controls in overseas jurisdictions;
- Transparency International's corruption perception index;
- The Basel AML Index;
- CIA World Factbook;
- U.S. International Narcotics Control Strategy Reports (INSCR);
- FATF Jurisdictional Information; and

- The Know Your Country rating table.

FATF in particular provides a source of valuable information on the relative risks associated with particular jurisdictions in its system of mutual evaluations, which provide an in-depth description and analysis of each country's system for preventing criminal abuse of the financial system. It also produces a list of jurisdictions with 'strategic deficiencies' in their money laundering initiatives and a list of jurisdictions with 'low capacity', the latter being countries which have economic or sociological constraints preventing them from implementing AML/CTF measures effectively.

In addition, information is publicly available regarding countries that present bribery and corruption risks and those regarded as secrecy jurisdictions or jurisdictions that permit the use of nominee shareholders.

The consolidated sanctions list, also details the countries in which sanctioned individuals and organisations are based, which may also provide an indication of the relative risk of each jurisdiction.

You should list all of the countries to which your practice is exposed in your PWRA and give a risk rating to each one. Being exposed to a country includes offering services, facilitating a matter involving or having clients established in that country.

For the avoidance of doubt, prohibiting clients from outside of the UK or that are not UK-nationals, is not a requirement of the Regulations. Geographic risk is primarily associated with jurisdiction, which may or may not extend to a client that has exposure to that jurisdiction, depending on the circumstances.

It is important to consider the levels of exposure your practice and any clients may have to higher risk jurisdictions. For example, a practice that has a significant proportion of its business connected to or in association with a country of higher risk, may have a greater risk exposure than a practice that only has one client, who uses only some ancillary services from that same jurisdiction. Practices should consider this along with the relative risks posed by the legal services offered to clients from such jurisdictions. On the other hand, experience of working in a high-risk jurisdiction can help practices to identify risks, while those with only a minor exposure may lack such experience and may struggle to correctly identify risks.

Increasing globalisation means the likelihood that the work you do will involve other jurisdictions and the international dimension may not always be obvious. You should bear this in mind when assessing geographic risks and whether a client or matter may involve a higher risk jurisdiction.

Country risk factors should feature prominently in a practice-wide risk assessment. Key issues to consider are whether the jurisdictions in which your clients, or the beneficial owners of your clients, are based or operate their businesses:

5.6.2.2 Indicators of lower risk:

- has stable, strong and independent political and legal systems, with legally protected commitments to transparency, accountability and integrity across the key institutions of government;

- has compulsory suspicious activity reporting requirements in the regulated sector;
- money laundering is criminalised, on a wide basis (e.g., all-crimes approach or a specific list), and an effective sanctions regime is in place; or
- the country has transparency of beneficial ownership disclosure requirements and an established financial intelligence unit.

5.6.2.3 Indicators of higher risk:

- has deficient anti-money laundering legislation, systems and practices and/or inadequate AML supervision;
- has high levels of acquisitive crime or higher levels of corruption;
- are a jurisdiction where the production of drugs, drug trafficking/trade, terrorism or corruption is prevalent;
- are considered to be 'offshore financial centres' or tax havens;
- permit nominee shareholders to appear on the share certificate or register of owners; or
- local requirements around company structure or equivalent governance are unclear or otherwise make it challenging to understand the control structure of an entity.

Where your clients or the beneficial owners of your clients are based or operate their business in low-risk jurisdictions this should also be reflected in the Practice-wide risk assessment.

It is also important to consider whether your practice is involved in multi-jurisdictional matters. Money launderers are commonly attracted to matters which move money or value across borders, in order to obscure ownership and frustrate investigations.
If you do not have the ability or expertise to effectively assess the risk posed by a particular jurisdiction, you should consider whether it is appropriate to continue to act in relation to clients or matters associated to those jurisdictions. Please note that jurisdictional risk is not an assessment of a client's nationality. Not accepting business solely due to a client's nationality is unacceptable and may lead to charges of discrimination and/or create access to justice issues for your practice.

It may also be necessary to consider risks posed by non-nations that for whatever reason may pose a different risk to the nation within which they sit, e.g., regional jurisdictions such as Darfur in Sudan.

5.6.3 Product or Service Risks

You should consider the following questions:

- Does the practice offer any services which may attract a higher level of risk such as large volume/high value conveyancing, corporate acquisitions, tax mitigation strategies, work involving high-risk jurisdictions or the creation and/or management of specialist entities?
- Does the practice have the necessary expertise and experience to undertake the work requested?

- Does the practice undertake work which may be of lower AML risk (e.g., executorship, wills, litigation)?

The National Risk Assessment highlights that independent legal professionals face the greatest potential risks in the following areas:

- misuse of client accounts;
- sale/purchase of real property;
- creation of trusts, companies and charities;
- management of trusts and companies; and
- sham litigation.

Consideration should be given to whether the practice undertakes work with exposure to these risks and this should be documented in your PWRA accordingly.

Other factors to consider are the value, complexity and nature of work in these areas in the context of the client and/or the nature of the work that your practice normally undertakes.

5.6.3.1 Sale/purchase of real property

According to law enforcement authorities and the national risk assessment, the sale and purchase of real estate is a common method for disposing of or converting criminal proceeds.

Real estate is generally an appreciating asset and the subsequent sale of the asset can provide an apparently legitimate reason for the existence of the funds. Property matters are an attractive method of laundering criminal proceeds because:

- Property is often a high value asset – it offers the opportunity to legitimatise large amounts of money in one go;
- The value of property generally appreciates – this is unusual for criminals who usually lose money when laundering;
- The nature of conveyancing means that matters/transactions often happen extremely quickly – and therefore it is easier to hide behind a complicated money trail which can be constructed very quickly, and the onward sale of a property can give the appearance of a legitimate income stream;
- Property can be used to generate additional quasi-legitimate income streams e.g., rental; and
- Property can be used by the money launderer or an associate as a residence.

Transfers of real estate from one owner to another without the exchange of funds, may present an equal risk to the purchase of property.

5.6.3.2 Client accounts and payments

You should consider the risk that criminals may attempt to misuse your client account. Putting the proceeds of crime through your client account can give funds the appearance of legitimacy, as the subsequent transfer will show as having originated from a regulated legal practice. It will also help obscure the audit trail of funds whether the money is sent back to the client, on to a third party, or invested in some way.

Introducing cash into the banking system can be part of the placement stage of money laundering. The risk of this occurring, along with the controls in place at the practice to prevent this happening, should form part of your PWRA.

Generally speaking, you should avoid accepting cash payments to your client account in relation to transactions. If you do choose to accept these as a policy of your practice, it should be considered high risk within the PWRA particularly where large in size (e.g., above £1,000). At a client or matter level, you should establish Source of funds for any cash payments and treat the funds on a risk sensitive basis. There may be valid reasons for accepting cash into the client account (e.g., access to justice or in cases of domestic disputes) – reasons for accepting any cash payment should be clearly documented.

5.6.3.3 Formation and management of trusts and companies

Company and trust structures may be exploited by criminals who wish to retain control over criminally derived assets while creating impediments to law enforcement agencies in tracing the origin and ownership of assets. Criminals may ask legal professionals to create companies and trusts and/or to manage companies and trusts, to provide greater respectability and legitimacy to the entities and their activities.

Your PWRA should consider the practice's exposure to this type of work, and the risks involved– especially where the practice undertakes complex company or trust work for clients involving higher risk jurisdictions. This is particularly important where beneficial ownership or nature of business can be obscured or anonymised, or the use of nominees or bearer shares is permitted.

Shell companies are corporate entities that do not have any business activities or assets. They may be used for legitimate purposes such as serving as a temporary transaction vehicle. However, they can also be an easy and inexpensive way to disguise beneficial ownership and the flow of illegitimate funds and so are attractive to criminals engaged in money laundering. You should consider it as high risk if a client engages your services only in connection with the routine aspects of forming an entity, without seeking further legal advice on the appropriateness of the corporate structure and related matters. In jurisdictions where members of the public may register companies themselves with the company registry, the engagement of a legal professional to register the company (or to use the practice's address) may indicate that the client is seeking to add the appearance of legitimacy to a company.

5.6.3.4 Other Services

Other services to consider in risk assessments are:

- Services where legal professionals may represent or assure the client's standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs;
- Acquisitions of businesses in liquidation; and
- Services offered to clients in the context of trade based or trade-finance arrangements.

5.6.3.5 Risk of offering both in-scope and out-of-scope services

Many practices have both an AML-compliant client onboarding (take-on) process and a separate process for those areas of activity outside the scope of the Regulations. This is permissible, but it does create a risk.

The risk is that if a client is onboarded via an AML non-compliant process for out-of-scope work, and then transferred over to AML in-scope services, there is likely to be a need to apply further due diligence, in order to bring the original due diligence up to the required standard.

To mitigate this risk practices may either have clear and robust PCPs in place to manage the transition or conduct full AML-compliant CDD regardless of the nature of the matter. This would enable a client to be transferred more easily between a practice's out-of-scope and in-scope services.

5.6.3.6 Dealing with payments credited to your client account without permission

Legal professionals may receive funds that are either overpayments, or completely unasked for deposits. You should give consideration to the possibility that any unsolicited payment or unexpected overpayment may have been engineered for the purposes of money laundering and treat these instances appropriately (including consideration of the submission of a SAR as appropriate). A repayment of funds from a legal professional's account may help to legitimise the proceeds of crime.

Such instances should be recorded in an appropriate place, for example in a client or matter risk assessment, or in the records of the MLRO.

One way to deal with such matters is to set an internal value threshold, beyond which, greater consideration must be given to whether the circumstances prompt suspicion and a subsequent disclosure to the NCA. Except in exceptional circumstances funds received in such a manner should only be returned to the source from which they were received.

R31(2) confirms that you are not prevented from repaying money deposited in your client account, provided that, if you have suspicion of money laundering, you obtain consent/DAML from NCA for the transaction.

If you display your client account details freely, for example, on your letterhead or a website, the risk of them being abused by criminals is greatly increased. This is something you should avoid.

5.6.4 Delivery Channel Risk

Questions to ask when assessing inherent delivery channel risk for your PWRA.
What % of its business is conducted on a non-face to face basis?
Does the practice undertake work which is conducted through intermediaries or other 3rd parties?

How you deliver your services must be considered in your PWRA. You should consider this along the following lines:

- The proportion and characteristics of clients you do not meet face to face or do not verify with robust electronic identification and verification; (EID&V)
- How many of your matters rely on indirect contact with your client (e.g., via a representative or agent) rather than holding a direct relationship with the client;
- How much of your activity is delivered online or via any other channel that may facilitate anonymity; and
- The methods used to undertake identification and verification and general due diligence requirements.

5.6.4.1 Acting for individual clients without meeting them

You should consider this as a risk factor when you carry out your PWRA. You should also consider how you mitigate the risk, for example by using an EID&V platform. It may also extend to the remote methods (e.g., telephone, email, live video) you use to contact your client, as not all methods provide the same level of anonymity. Contact that is limited to text-only should be considered as higher risk.

When you act for clients without meeting them you must be satisfied that it makes sense in all the circumstances that you have not met the client and you should be comfortable that you can mitigate the risks of identity fraud. You should consider whether any form of Enhanced Due Diligence may be appropriate.

Use of an appropriate EID&V platform to mitigate the risks of not being able to meet a client can be helpful but is not in itself a guaranteed or automatic solution to these challenges. A clear understanding of the limitations of such tools is needed if they are to be used correctly. See Section 7 for more information on this.

5.6.5 Transaction risk

You should consider the types of transactions you facilitate, particularly with regards the complexity and the risk that there may be parties to the transaction that you are not able to identify.

This is a potentially complicated area of risk and you should seek to set out what are the most common types of transaction for your practice, and how you rate the risk of transactions that fall outside of these scenarios.

For example, you may want to set out the common range of values for the transaction you are normally involved with, and other characteristics e.g., residential conveyancing transactions in a certain area. You would want to set out the risks involved with this activity and any other common areas of practice and consider what the risk levels may be for activities that fall outside of these clearly assessed areas.

5.7 Conclusions of a risk assessment

Practice-wide risk assessments may be based on inherent risks or can be taken further in order to identify the residual risk facing your practice, after taking into account the inherent risks and the controls and other mitigatory factors in place. Stating the inherent risks, mitigating measures, and residual risk can make it easier to review and adapt the risk assessment in future.

You may find it helpful to rate a particular risk on a three-tier basis of low, medium or high or on a more granular scale in order to better differentiate between factors and their relevance to the practice. Whichever rating system you choose to use, it is important to keep the approach consistent throughout the document to allow comparability across risk types.

Alternatively, you may wish to record the risk narratively, however this may make a consistent approach to risk management more challenging.

5.8 Application of Risk Assessments

While risk assessments can be useful tools, they are only as effective as their application.

Ultimately the aim of risk assessments is to help you meet the requirements that you must:

- take appropriate steps to identify, assess and understand the money laundering and terrorist financing risks your business faces;
- ensure mitigation reflects your assessment of risk arising in any particular matter (as per R28(12)(ii));
- apply a risk-based approach to compliance with CDD obligations (subject to any specific provisions in the Regulations); and
- have documented policies, controls and procedures that enable your business to manage, monitor and effectively mitigate the different risks that have been identified.

If the risk assessments are not properly used when assessing client or matter risks, or do not inform the PCPs you have in place, your practice will be exposed to the risk of abuse by criminals. PWRAs should be the basis and cornerstone for the development of effective, risk-based PCPs under R19.

Furthermore, it should be made widely available and understood by all fee earners undertaking activities under the Regulations as well as all other relevant employees.

It is not expected that a practice seeks to eradicate all financial crime risk. However, it must ensure that the PCPs adopted as a result of the assessments are appropriate in light of the risks faced. Comprehensive and documented PWRA and client/matter assessments combined with written records of decisions made on individual clients and matters will enable you to justify your decisions and actions to law enforcement and your supervisor.

5.9 Client and Matter Risk Assessments

For each client and matter you should (as per the FATF Guidance for a Risk Based Approach for Legal Professionals):

- Identify the client and the beneficiaries of the matter and obtain an understanding of the source of funds and wealth of the client/owners and the purpose of the matter;
- Understand the service you are going to provide and whether you have the expertise to deliver it, and whether/how the service could lead to the laundering of money;
- Understand why your services are needed, whether a personal or commercial rationale and whether it appears reasonable or genuine;
- Be vigilant to red flags;
- Make a determination as to what action you need to take, including what evidence you need to collect and ongoing monitoring requirements; and
- Document and record all steps taken.

5.10 Client Risk Assessments

Regulation 28(12) states that: The ways in which a relevant person complies with the requirement to take customer due diligence measures, and the extent of the measures taken must reflect the PWRA.

As such, you must record a risk assessment for every client you act for as a part of CDD. In doing so, you should consider which of the risk factors (detailed in Section 6) are relevant in the case of a specific client, paying particular notice to where your PWRA suggests they may be high risk, or if the PWRA does not address certain risks at all. In the case of the latter, you should consider reviewing and updating your PWRA to reflect the new risks.

5.10.1 Timing of a Client Risk Assessment

Your initial risk assessment should always be performed at the beginning of a client relationship in conjunction with performing CDD. However, for some clients, additional information to inform the risk profile may only emerge once further information becomes available or the relationship/matter progresses. Practices should be aware of this and incorporate this into their risk assessment procedures. Information learned while acting for the client should also inform your client and matter risk assessment. The better you know your client and understand your instructions, the better placed you will be to assess risks, spot suspicious activities and protect your practice.

R28(13) requires that in assessing the level of risk arising in a particular case you must take into account:

- the purpose of the matter or business relationship,
- the size of the matters undertaken by the customer; and

- the duration of the business relationship including accounting for any significant gaps.

Fundamental to any assessment of client risk is an assessment of whether the client's financial circumstances, main business activities, and source of wealth and source of funds align with the background and wider profile of the client. You should detail these considerations in your client/matter risk assessments.

Other considerations and factors relevant to client risk assessments are whether:

- the structure, complexity or nature of the client entity or relationship makes it difficult to identify the true beneficial owner or any controlling interests;
- the client appears to be attempting to obscure understanding of their business, ownership or the nature of their matters;
- the client is a PEP, or is closely related to or associated with a PEP;
- the instruction from the client is channelled through a 3rd party and there is a lack of direct interaction with the client;
- there are any geographic risks associated with the client;
- the client wishes to conduct the business relationship or request services in unusual circumstances;
- the practice is aware that clients hold residence rights or citizenship in a jurisdiction in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities in that jurisdiction; and
- the client is seeking advice or implementation of an arrangement that has indicators of a tax evasive purpose, whether identified as the client's express purpose, in connection with a known tax evasion scheme or based on other indicators from the nature of the matter.

The above list is not exhaustive, and where such businesses are regulated for AML purposes, or traded on a publicly traded exchange, this may provide some mitigation of risk and comfort to the practice.

You should also assess and have regard to whether negative/adverse media or press coverage is apparent regarding the client. This can be readily checked by conducting research on the client (e.g., via straightforward web searches) the nature and intensity of which should be done to a degree appropriate to the risks identified. Consideration should be given to the source (including the profile of the particular media or press outlet) of allegations and its reliability/veracity, along with the relevance, timings and seriousness of any allegations.

In order to have confidence in the results of any media check, you should be satisfied that the overall CDD material for your client is reliable and allows you to identify the client and verify their identity.

Other areas of client risk tie in with matter types or types of service, including unusually complicated matters, matters that lack an obvious economic purpose or are in some other way unusual. You should consider how you might ensure that your staff can identify any warning signs alongside other relevant training as a mitigation to be recorded in your PWRA.

5.11 Matter-Level Risk Assessments

Are there any features in the matter which may represent higher risk?
Is the matter generally complex in nature?
Is the matter undertaken at short notice, within a short timescale or involving high volumes?
Does the matter involve new sources of finance – anything unregulated e.g., involving crowd funding platforms or some aspects of bitcoin/cryptocurrencies?
Does the matter involve trust or other legal entity company formation, management or service provision?
Is the matter routine for the practice, and if not, does lack of experience or expertise add to the risk?
Do the source of funds or the parties to the matter frequently change?
Is the matter longer term in nature, or does it involve funds being locked in for substantial periods of time?
Is the matter publicly funded by the UK or similarly reputable government?
Is the matter publicly funded from jurisdictions where corruption is prevalent?

Matter Risk Sample Questions

Matter risk assessments should focus on the specific risk factors that a matter presents, beyond the client risks already identified.

It may not be necessary to undertake a written risk assessment for every matter. A matter risk assessment is less likely to be needed where:

- matters undertaken for a given client are highly repetitive in nature, with risk remaining consistent between one matter and another and the risk is addressed comprehensively by the client risk assessment; and
- the practice is providing an ongoing Registered Office facility for the client, though ongoing monitoring of this relationship should still be required.

Matter risk assessments will help you to consider whether you are comfortable acting and, if so, to adjust your internal controls to the appropriate level according to the risk presented. For example, different aspects of your CDD controls may be adjusted to meet the different risks identified.

If, having conducted the necessary due diligence you assess the matter as being high risk, you may require fee earners to monitor the matter more closely.

Both client level and matter level risk factors should be considered when composing a matter-level risk assessment tied to a specific piece of work.

These factors include when:

- The size, nature, purpose, commercial rationale, context or complexity of the matter are unusual or unclear;
- The source of wealth or funds involved in the matter is unclear or obscured;
- There is involvement of or payment to or from 3rd parties, especially where the relationship between the parties does not be appear clear or the payments do not make sense in the overall transaction;
- There is difficulty in identifying structures/beneficiaries/interests involved in a matter;
- The matter involves structuring of a transaction which obscures understanding of the nature of the transaction or ownership of the entities involved; and
- the level and type of matter does not fit the client's profile or involves a sector in which the client would not ordinarily operate.

5.12 Undertaking Client/Matter Risk Assessments

Risk assessments should document the circumstances and the identified risks with reference to the PWRA, rate the risks, and justify these ratings with a supporting rationale. They should not be a tick box exercise.

A category-based approach can be taken with high/medium/low ratings applicable to given categories (e.g., conveyancing matters of value £1,000,000 or more are high risk). A practice may develop a client/matter risk assessment template in order to help those legal professionals making risk assessment decisions. Where this approach is adopted, internal guidance and training on the use of the template should be provided including how to assess the background and circumstances of the client and matter, and all key risk factors. Make sure that the use of a template does not lead to a tick-box approach to risk assessments.

Where legal professionals are involved in longer term matters, risk assessments should be undertaken at suitable intervals across the life of the matter on a risk sensitive basis, to ensure no significant risk factors have changed in the intervening period (e.g., new parties to the matter, changes in ownership and control, new sources of funds etc.).

5.13 Risk Weightings

When weighting risk factors, practices should take a holistic approach and make an informed judgement about the relevance of different risk factors in the context of a particular customer relationship or occasional matter.

This often results in practices allocating different ‘scores’ to different factors.

For example, a practice may decide that a client’s personal links to a jurisdiction associated with higher ML/TF risk adds 7 points, but the high-risk nature of the service sought only adds 5. In this way, the final score takes account of both factors in proportion.

Ultimately, the weight given to each factor is likely to vary across practices, clients and matters.

Care should be taken if using a “matrix style” or scoring approach where there is cumulative addition of risk ratings, to produce an overall risk score. This may lead to inappropriate minimisation of serious risks in the context of lower ones.

In any scoring system you should consider whether it may be appropriate to have automatic high-risk triggers, that make a client or matter high risk, regardless of whether they meet a score threshold or not.

Inappropriate use of scoring

In this example, there is a cumulative scoring system, with each risk area assessed out of 20. Two factors score a maximum score but because all the others are zero, it will not meet the threshold and be rated lower risk.

The fact that the first two categories get a maximum risk score, mean that assigning an overall risk rating of low (because it does not meet the threshold) may, depending on the nature of the risks, be inappropriate.

High risk threshold =	50
Geographic risk	20/20
Client risk	20/20
Delivery channel risk	0/20
Transaction risk	0/20
Products services risk	0/20
Total score =	40/100

40<50 therefore low risk.

Where either, or both, the customer and the service are considered to carry a higher risk of money laundering or terrorist financing, it may be appropriate to consider the overall risk of the matter as high risk.

You should clearly document the reasons for any deviation from this approach. Dependent on the nature of the deviation you will want to consider if this is documented on a matter-by-matter basis or as part of your PWRA.

When weighting factors, practices should ensure that:

- Weighting is not unduly influenced by one factor;
- Economic or profit considerations along with desire to preserve relationships with clients do not influence the risk rating;
- Weighting does not lead to a situation where it is impossible for any business to be classified as high risk;
- The system adopted does not have any unintended consequences e.g., certain risks might be outweighed by others leading to an inappropriate overall rating;
- The practice's weightings have regard to situations specifically identified by national legislation or risk assessments as presenting a high money laundering risk (these may be documented in the overarching PWRA); and
- Practices should be able to override any automatically generated risk scores where necessary with the rationale for the decision to override such scores being documented appropriately. Short complementary notes explaining the rationale for each weighting may be a useful addition to the risk assessment.

Where a practice assesses the risk of a particular factor differently from the National Risk Assessment or any piece of supervisory guidance, for example due to the nature of the

Practices' mitigating activities and/or PCPs, this should be clearly documented in their PWRA.

An overall conclusion of the risk of the client/matter should always be reached after all relevant risk factors have been considered, before determining what is the overall risk category and the appropriate level of mitigation controls to be applied.

5.14 Recording and Documenting Risk Assessments

There is no prescribed approach to the recording of risk assessments, however they must be written down so that you can evidence them to your supervisor.

What is important is that risk assessments are adequately documented, all relevant factors are considered, and decision-making/rationale is recorded. An overall risk level of the particular client/matter must be recorded, and the assessment should be signed (manually or digitally) and dated by the individual who has conducted it.

Risk assessment documentation should be kept up to date, be clear in providing an audit trail of the decision-making process, methodology and rationale – in order to demonstrate adequate consideration of risks to the practice's its supervisor, law enforcement or the courts.

Risk assessments should be:

- Available to those professionals working on relevant matters; and
- Reviewed at appropriate intervals to ensure they are up to date and reflect changing risks.

5.15 Application of Risk Assessments

As per the requirements of R28(12) the result of the client and matter risk assessments will dictate the level and extent of due diligence undertaken on a client or matter.

As per R33(1) where the client/matter is assessed as being of higher risk, enhanced due diligence must be applied.

In all other cases due diligence as per the requirements of R28 and R29 must be applied.

In certain lower risk situations, simplified due diligence may be applied, in line with requirements under R37.

Further information on what this means in practice can be found in Section 6.

5.16 Risk Mitigation

Having assessed the money laundering and terrorist financing risks your practice faces, you should then consider any risk mitigating controls that you can implement to manage these risks.

You can find some common risk mitigation controls below.

5.16.1 Appropriate CDD

Introduce a means of identifying potentially higher risk factors and do detailed internet-based research on higher risk clients and beneficial owners. Probe, evidence and document source of funds and wealth in higher risk cases, including where shareholders have no apparent online presence, but the matter value is substantial.

Please see Section 6 for further information

5.16.2 Client accounts and payments

Always ensure that you comply with the client account rules of your regulator.

Prohibit the use of your client account without delivery of accompanying legal services and include a process to ensure that information about all payments is cross-checked where possible.

Ensure completion of CDD before taking money on account, including adequately understanding the matter.

Avoid disclosing your client account details until you are ready to accept a payment/transfer and discourage clients from passing the details on to third parties. Ask them to use the account details only for previously agreed purposes.

Prohibit or restrict cash payments. Large payments or a series of smaller payments made in actual cash may be a sign of money laundering. You should consider establishing a policy of never accepting cash payments. If this is unavoidable, you should set a limit above which you will not accept cash payments. Clients may attempt to circumvent such a policy by depositing cash directly into your client account at a bank. You may consider advising clients in such circumstances that they might encounter a delay in completion of the final matter or in the return of their funds. If a cash deposit is received without solicitation, you should consider making a disclosure to the NCA.

Where money is accepted into the client account in respect of a matter or from a client on account and the matter is aborted, carefully consider the level of risk analysis and CDD conducted at the outset, the legitimacy of the matter and the parties to it, and the circumstances of the aborted matter. You should not return funds without considering the need to make a SAR. You should only return funds to the original sender of those funds and not to any other designated person except in exceptional circumstances e.g., the death of the individual.

Ensure appropriate checks are made and the rationale for and size of a matter and any payments into your accounts by third parties is clearly understood before any third-party payments are accepted into the client account. You should make enquiries into sources of funding from other parties and always be alerted to warning signs.

5.16.3 Sale/purchase of real property

Seek to understand all aspects of the matter, including undertaking appropriate due diligence on the parties involved in line with regulatory requirements, and understanding the source of funds/source of wealth used.

Keep up to date with emerging issues. It may be useful to review resources from relevant regulators in other countries to supplement knowledge in this area.

Provide information and/or training, where appropriate, to staff on these updates so that they are better equipped to spot issues.

5.16.4 Creation of trusts, companies and charities

Be aware of higher risk jurisdictions where ownership may be concealed.

If a prospective client simply requests you to undertake the mechanical aspects of setting up a trust, company or charity, without seeking legal advice on the appropriateness of the company structure and related matters, you should conduct further investigation.

5.16.5 Management of trusts and companies

Ensure you understand the entities concerned, including, where relevant, source of funds and wealth of the trust or company to minimise the money laundering risk.

Provide information and/or training, where appropriate, to staff on possible red flags and their duties as a company/trust manager.

Seek to understand the commercial rationale/reason for the matter structure.

If you have been asked to sit on the board of an entity in another country, you should consider asking a trusted and knowledgeable source with local knowledge whether it is consistent with local/cultural norms or if there is a legal reason. If you do need to rely on another source to advise you in this way, you should consider whether you have appropriate expertise to be working in this area.

6. Client Due Diligence

Relevant Compliance Principles

The practice must have clearly documented PCPs based on their practice-wide risk assessment which include:

15. Client Due Diligence procedures (including procedures to identify the ownership and control structures of non-natural persons)
16. Identification and verification (ID&V) procedures relating to natural persons (this includes ID&V procedures in relation to the ultimate beneficial owners of non-natural clients, and those purporting to act on behalf of a client)
17. Procedures to facilitate a clear understanding of the client's source of wealth and funds in relation to a transaction, and the level of evidence required, in line with the risk profile of the client/matter.
18. Procedures to facilitate reporting of discrepancies between Beneficial Ownership information obtained through due diligence checks and what is held on the Companies House register
19. Enhanced Due Diligence procedures – including the provision of adequate controls to manage higher risk clients/transactions, and measures to establish Source of Funds/Source of Wealth where appropriate
20. The practice's position on the use and application of Simplified Due Diligence.
21. The timing of any due diligence procedures
22. The practice's position on the use of R39 Reliance and any related procedures
23. The ongoing monitoring of clients and their matters
24. The identification of instances where it is required or appropriate to re-apply or renew CDD or EDD on a client
25. Dealing with the return of un-solicited or apparently accidentally deposited funds
26. Identification and scrutiny of any complex or unusually large transactions, or an unusual pattern of transactions, or those which serve no apparent economic or legal purpose
27. Any additional measures to prevent products/transactions that support anonymity being used for ML/TF
28. Identification of Politically Exposed Persons (PEPs), their relatives or close associates and the control of any associated risks

6.1 General Comments

Undertaking appropriate Client Due Diligence (CDD) is required under R27, and is one of the key controls you have, to protect your practice from Money Laundering and Terrorism Financing (ML/TF) risks.

CDD is the collective term for the checks you must do on your clients, which may differ depending on the circumstances. **It is holistic in nature and is wider than simply undertaking identification and verification of clients.**

Aside from any specific CDD requirements you must take under the Regulations, the amount, type and level of CDD undertaken should reflect and mitigate the nature of particular risks inherent in each client, transaction or matter.

Practices must be able to demonstrate to their supervisory authority that these CDD measures are appropriate in mitigation of these risks, by recording their reasoning and actions in this regard.

Useful information in regard to understanding the nature and purpose of a relationship may include:

- The nature and details of the business/occupation/employment;
- Source of funds and source of wealth information; or
- Anticipated levels and nature of activity to be conducted.

Beyond adherence to the Regulations, there is a natural incentive for practices to establish with confidence who their client is and the details of any transaction they are involved in or facilitating. It will protect them from unintentionally facilitating a range of financial crimes or being defrauded themselves.

Identifying and verifying clients, is also essential for a practice to be able to accurately report suspicious activity to the National Crime Agency (NCA), identify Politically Exposed Persons (PEPs) or other high-risk individuals, and ensure the practice is not undertaking business in breach of applicable sanctions regimes.

In relation to CDD, the Policies, Controls and Procedures (PCPs) of your firm should be set out clearly, in writing in a way that is accessible to all relevant staff in your practice.

6.2 Long-standing/Personal Relationships

There is no provision in the Regulations for waiving CDD requirements on the basis of long-standing or personal relationships. Taking this approach will not satisfy the requirement to undertake independent verification, though these factors may inform your risk-based approach.

6.3 Application of CDD

You are required to apply CDD for services in scope of the Regulations when:

- establishing a business relationship;
- carrying out an occasional transaction that amounts to a transfer of funds within the meaning of Article 3.9 of the Funds Transfer Regulation (Regulation (EU) 2015/847)[1] exceeding 1,000 Euros;

[1](9) 'transfer of funds' means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including:
(a) a credit transfer as defined in point (1) of Article 2 of Regulation (EU) No 260/2012;
(b) a direct debit as defined in point (2) of Article 2 of Regulation (EU) No 260/2012;
(c) a money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC, whether national or cross border;
(d) a transfer carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or post-paid device with similar characteristics;

- carrying out an occasional transaction that amounts to 15,000 Euros or more, whether it is executed in a single operation or in several operations which appear to be linked;
- you suspect money laundering or terrorist financing; or
- you doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.

The Regulations as amended prescribe further situations where you must re-apply CDD for existing clients. These arise when you have any legal duty in the course of the calendar year to contact a client to review information:

- relevant to your client risk assessment (or practice-wide/matter risk assessment as appropriate); or
- concerning beneficial ownership information of the customer, including information which helps you understand the ownership or control structure of any entity that is the beneficial owner of the client.

The duty also arises where a practice has a duty to contact the client under the International Tax Compliance Regulations 2015.

6.4 Definition of Business Relationship

There may be several indicators that a client is establishing a business relationship, as opposed to the matter being an “occasional transaction” including but not limited to:

- an explicit expectation from the client or practice that a business relationship is being established;
- the nature of the client or the transaction suggests they may wish to undertake more than one transaction e.g., it is in the nature of their business;
- or the transaction itself will inherently take time to complete e.g., the buying/selling of real property.

The definition of business relationship under the Regulations requires the legal practitioner to have an expectation at the time the contact is established, that the relationship will have “an element of duration” (R4). This should be interpreted in the broadest sense, as it is reasonable to assume that any legal professional will have an expectation of possible further business from any initial contact made with a client. When dealing with a client for the first time, you should assume that a business relationship is being formed unless you have explicit reasons to know that this is not the case i.e., that there will not be an “element of duration.”

The nature of the relationship should be recorded in the client risk assessment. Any reasons for not applying CDD must be clearly recorded and this will in practice be in the rarest of exceptions.

For the avoidance of doubt, any company formation on behalf of a client immediately implies the establishment of a business relationship as per R4(2).

6.5 Definition of an occasional transaction

A transaction that falls outside of a “business relationship,” is known as an occasional transaction.

By definition it can only apply where a practice-client relationship lacks an expectation of an “element of duration.” For this definition to apply, the relationship must be limited to a single service provided at a certain point in time.

It will still be necessary to undertake CDD for an occasional transaction where it has a value of 15,000 Euros or more. Any transaction worth 15,000 Euros or more. is by definition not an occasional transaction. 15,000 Euros relates only to the sums involved in the transaction(s) and does not include legal fees or distributions.

Due to the ongoing duties a practice would have in most foreseeable circumstances, this definition is not likely to apply to the relationship between a legal practice and a client for any transaction.

It may apply in the case of a limited ancillary service, provided as a one-off or in some examples of notarial work in particular. Please see Part 2 for more information on notarial work.

6.6 Intermediaries, agents or representatives

If your client is represented by an intermediary, agent or representative (i.e., someone purporting to represent them), you must comply with R28(10) and identify and verify the intermediary's identity and their authority to act on behalf of your underlying client.

Examples of someone purporting to represent might include:

- a parent on behalf of an adult child;
- an individual not employed by your client; or
- a situation where the instructing persons authority to instruct is not clear or does not make sense.

In the absence of factors that give rise to a concern, an employee of a company would not be considered to be ‘purporting to instruct’. A risk-based approach should be taken to the level of identification verification applied. Authority to instruct can be addressed by an engagement letter or equivalent but it should come directly from the underlying client (including where instructed by an employee of the company).

Even where someone does not purport to act on someone else’s behalf, you should consider if it is possible there may be an underlying client that is the recipient (potentially by proxy via another professional service provider) of your services on more than a single isolated basis. If you think this is possible, you should satisfy yourself that you have identified and verified who the underlying client is or establish a suitable reliance arrangement with the professional you are dealing with.

You should ensure you understand who your client relationship is with. There may be times when an intermediary is your client (in that your contract is with them) but the intermediary’s client is the ultimate beneficiary of your work and advice. The regulations make clear that a “beneficial owner” is the individual on whose behalf a transaction is being conducted and you should treat such a client as a beneficial owner, including undertaking reasonable measures to identify and verify their identity. This is different to a situation where an entity refers a client to you (see below.)

Where the intermediary is an entity, you may consider whether you need to undertake Ultimate Beneficial Ownership checks on a risk-based approach.

See 6.14.9 for how to identify and verify individuals in these situations.

6.7 Referrals to another legal practice (or referrals between other entities in scope of the regulations)

The difference between the circumstances described in 6.6 and making referrals to another practice is described in the below table.

This table relates to solicitors only - for arrangements relating to Barristers and Advocates, please consult the relevant section in Part 2.

Intermediaries, Agents or Representatives	**Referrals**
If you are instructed by a law firm, or other professional intermediary the law firm/professional intermediary are your client, and you will need to undertake CDD on them. If the effective beneficial owner of the advice is that law firm's/professional intermediary's client, you should consider the risks and identify/verify their client as you would any other ultimate beneficial owner. This could include understanding the checks the intermediary has carried out.	Where a legal practice or other intermediary refers a client to you and you have the direct relationship with the client, you should treat the referred entity as the client and carry out CDD on them as the client in the usual way. You may wish to consider, having regard to the risks (and regulated status of the referring entity), whether a reliance agreement with the referring entity is appropriate in the circumstances.

6.8 Timing of CDD

CDD must be completed before you:

- deliver substantive work or benefit;
- permit funds to be deposited in your practice's client account unless they are for fees and disbursements;
- allow property to be transferred; or
- allow final agreements to be signed and completed.

A legal practice should ensure that CDD has been completed as early as possible, before any money has been taken from the client, though money on account of costs/fees may be accepted on a risk sensitive basis.

Conducting CDD as early as possible also helps you to avoid any delays further along in the matter and will help you in your duty to report suspicious activity, at an early stage. This can help protect you from needing to submit a suspicious activity report (SAR) seeking a defence against money laundering (DAML) to return funds that have been paid into your client account, where you have a suspicion the funds may be the proceeds of crime.

R30 requires you to verify your client's identity, the identity of any person purporting to act on their behalf and that of any beneficial owner before you establish a business relationship or carry out a transaction which amounts to 15,000 Euros or more (subject to R30(3)(a)).

6.9 What happens when you cannot complete CDD?

R31 provides that if you are unable to complete CDD in time, including identification & verification, you must:

- not carry out a transaction with or for the client through a bank account;
- not carry out a transaction otherwise than through a bank account; or,
- terminate the business relationship.

For the avoidance of doubt, you should consider a failure to apply CDD under R28(10) (persons acting as agents) as also triggering the above requirements in R31.

If you are unable to complete CDD, you must in addition to terminating any existing business relationship consider making a disclosure to the NCA.

You cannot seek consent from the NCA to proceed with a transaction solely because you have been unable to complete CDD measures as required by R28 and reporting a matter to the NCA is not a substitute for your responsibility to complete CDD. Although you should consider making a disclosure to the NCA where you have been unable to complete CDD, this does not mean you are automatically required to submit a SAR. For further information refer to Section 11.

6.10 Exceptions to the timing requirement

There are exceptions to the timing requirement and the prohibition on acting for the client until CDD has been completed.

Where there is a delay in completing CDD you should consider why, and whether this gives rise to a suspicion which should be disclosed to the NCA.

A practice should document any occasion where CDD was delayed in the matter risk assessment and take appropriate mitigatory steps in order to manage any risks this may create.

In the event that you think either of the below exceptions apply, you should consider and record your reasoning as to why.

However, when acting for a:

- UK company (registered or unregistered as defined in the Unregistered Companies Regulations 2009(1));
- UK Limited Liability Partnership; or
- Scottish Partnership

- you must collect proof of registration (e.g., via the client) or an excerpt from the relevant register before commencing a business relationship even when relying on an exception to the timing requirement.

6.10.1 Exception 1 - Normal conduct of business

R30(3) provides that verification of the client and the beneficial owner may be completed as soon as practicable after contact is first established, during the establishment of the business relationship if:

- it is necessary not to interrupt the normal conduct of business; and
- there is little risk of money laundering or terrorist financing.

This should be considered in the context of the points in 6.8 of this guidance.

If there is little risk of money laundering (due to the nature of the client or transaction) thus allowing a delay in CDD completion, the reasons for this view must be included in the client and/or matter risk assessment, along with any mitigations you have put in place for this.

Consider your Practice Wide Risk Assessment (PWRA) when assessing which work, if any, can be undertaken prior to verification being completed. This exception does not apply if your matter is an occasional transaction.

6.10.2 Exception 2 - Ascertaining legal position

R31(3) provides that the prohibitions in 31(1) do not apply where:
'An independent legal professional or other professional adviser is in the course of ascertaining the legal position for their client or performing the task of defending or representing that client in, or concerning, legal proceedings, including giving advice on the institution or avoidance of proceedings.'

We interpret this to mean that this exception does not generally apply to transactional work but may be relevant when considering work undertaken as a tax adviser or when ascertaining the legal position an anticipation or preparation of early stages of transactional work or early stages of representation or provision of legal advice on other topics.

6.11 Undertaking CDD on Clients

R28 requires that you must:

- Identify the client and verify their identity on the basis of documents (e.g., passport or driver's license) or information obtained from a reliable source which is independent of the client (which may include a digital verification system, subject to meeting certain criteria – further details provided under Section 7), unless the identity of the client is already known to you and has been verified by you;
- Identify where there is a beneficial owner who is not the client and take reasonable measures to verify the identity so that you are satisfied that you know who the beneficial owner is;
- Take reasonable measures to understand the ownership and control structure of the legal person, trust, company, foundation or other similar legal arrangement;
- Assess, and where appropriate obtain information on the purpose and intended nature of the business relationship or occasional transaction; and
- Conduct ongoing monitoring, scrutinise transactions and make sure CDD documents are up to date.

6.12 Identification and verification

Identification of a client or a beneficial owner is simply being told or otherwise coming to know a client's identifying details, such as their name and address.

Verification is obtaining evidence which supports this claim of identity.

6.13 A risk-based approach

R28(12) provides that to comply with the requirement to take CDD measures, you must reflect:

- the PWRA (R18); and
- your assessment of the level of risk arising in any particular case i.e., the client/matter risk assessment.

6.14 Methods of verification

Verification should be completed on the basis of documents or information which come from a reliable source, independent of the client. There are a number of ways in which you may verify a client's identity including:

- obtaining or viewing original documents from a trusted and independent source (public or private);
- on a risk sensitive basis viewing copies of documents (certification of a copy may give you a higher level of confidence than an uncertified copy, but you should consider and document the risks of relying on certified copies for this);
- conducting electronic verification, through a platform that is a reliable source (i.e., secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity, to a degree that is necessary for effectively managing and mitigating any risks of money laundering and terrorist financing); or
- obtaining information from other regulated persons.

6.14.1 Independent sources

You need a reliable source(s) to verify your client's identity, which is independent of the client e.g. a passport or driver's license, or, in the case of a corporate entity, evidence of registration from the relevant registry or reputable company services provider.

You are permitted to use a wider range of sources when verifying the identity of the beneficial owner and understanding the ownership and control structure of the client.

Sometimes only the client or their representatives will be able to provide you with this information. You may consider whether the documents or information should be certified as accurate by a professional regulated for AML to an equivalent standard.

R28(9) confirms that the register of people with significant control, or the confirmation statement, which is published on the Companies House website, cannot be solely relied upon for the purpose of identifying or verifying the identity of the beneficial owner of a company or LLP client. Remember, if you are not satisfied with the information you have on the identity of your client/beneficial owner, you should not undertake business with that client, (or cease business if an existing client) as per the requirements of R31.

Documents should be in date if an expiry date is given, and recently dated (taking a risk-based approach) if no expiry date is given. Expired documents should not be relied upon in the absence of any others but may be useful in support.

6.14.2 Forged Documents

You must not ignore obvious forgeries, but you are not required to be an expert in forged documents. You may however consider providing relevant employees with appropriate training and equipment to help identify forged documents where relevant to the processes of your practice where proportionate to the risk.

You may make use of guidance on how to identify a forged document from the issuing body, or a similarly reputable source. For example, the Passport office issues such information, and current bill formats are available on utility provider websites.

6.14.3 Electronic verification

As technology has developed, use of electronic identification and verification (EID&V) tools have become more common. While you can never outsource your ultimate responsibility, EID&V tools can be useful in protecting your practice.

R28 sets out minimum requirements for EID&V processes to be regarded as reliable sources in applying CDD.

Test for whether you are able to use an EID&V tool

Meeting the definitions in the (*R2014/910/EU of the European Parliament and of the Council of 23rd July 2014*) as below

Electronic identification - means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person

Trust service - means an electronic service normally provided for remuneration which consists of:
(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services;
(b) the creation, verification and validation of certificates for website authentication; or
(c) the preservation of electronic signatures, seals or certificates related to those services

-and being secure from fraud, misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity, to a degree that is necessary for effectively managing and mitigating any risks of money laundering and terrorist financing.

There is further information available on this in Section 7.

6.14.4 Natural persons

The **name, date of birth and current address** of a natural person should be verified, using independent sources.

Practices may use government photo-card identification (including passports or driving licenses) to accomplish this.

To do this you should obtain either:

- one government document which verifies either name and address or name and date of birth; or
- a government document which verifies the client's full name and another supporting document which verifies their name and either their address or date of birth.

The requirement to obtain suitable verification should not preclude access to legal services, especially to vulnerable, elderly or disadvantaged clients. In these situations, where it is not possible to obtain such documents, consider the reliability of other sources and the risks associated with the client and the matter. See the “Clients unable to produce standard documentation” section below.

Where you are reasonably satisfied that an individual is nationally or internationally known, for example, because they are a public figure or a well-known celebrity (i.e., that you can confidently recognise them as the person they are purporting to be), a record of identification may include a file note of your satisfaction about identity, including an address. You should consider whether the individual may be a PEP, or family member or known close associate of a PEP.

6.14.5 Meeting clients face to face

The following sources may be useful for verification of UK-based clients:

- current, signed passport, driving license or birth certificate;
- marriage certificate (e.g., particularly useful for evidencing name changes);
- current government-issued identity card/certificate with photograph (e.g., gun license);
- residence permit issued by the Home Office;
- photographic registration cards for self-employed individuals and partnerships in the construction industry;
- benefit book or original notification letter confirming the right to benefits;
- a tax or utility bill or statement, or a certificate from a utility supplier confirming an arrangement to pre-pay for services;
- a recent bank or mortgage statement/passbook from an FCA-regulated lender;
- confirmation from an electoral register that a person of that name lives at that address;
- land registry confirmation of address;
- local council or housing association rent card or tenancy agreement; or
- house or motor insurance certificate.

Where you are provided with an electronic copy of a document (such as a downloaded bank statement) you should continue to take a risk-based approach while being conscious that its value as proof of address may be less than a standard hard copy.

Part of the reason to accept documents such as a hard copy posted bank statement and letters from government agencies is to demonstrate that the individual has access to the property to which they were delivered. Part of that comfort is removed when print outs of electronic statements/bills are used. This does not mean that such print- outs cannot be accepted but this loss of comfort should be considered on a risk sensitive basis.

If documents are in a foreign language you should take appropriate steps to be satisfied that the documents in fact provide evidence of the client's identity and

more generally that you understand what they say. Unless you have a sufficient level of understanding of the language, you should consider engaging the services of a translator.

You should be mindful that some aspects of an individual's identity (particularly name and/or sex) may change over time for entirely legitimate reasons, for example due to a change in sex or gender, or due to other life events such as a marriage or discretionary change of name. Such changes should not be used as a reason to withhold legal services in isolation, or necessarily interpreted as an indicator of higher AML risk

6.14.6 Natural Persons not able to meet face to face

In the case of persons you cannot meet face to face, consideration should be given to any geographic/jurisdictional (which could be at a regional or national level) risks this may present (see risk assessment section of this guidance for further information).

The client's address may be identified or verified via:

- an official overseas source;
- a reputable directory; or
- a person regulated to an equivalent standard for money laundering purposes in the country where the person is resident who confirms that the client is known to them and lives or works at the address given.

When you do not meet the client, you should consider the reason for this and whether this represents an additional risk which should be taken into account in your risk assessment of the client and the extent of the due diligence measures you apply. EID&V may be a particularly useful tool in these circumstances.

6.14.7 Clients unable to produce standard documentation

Sometimes clients are unable to provide standard verification documents. The purpose of the Regulations is not to deny people access to legal services for legitimate transactions, but to mitigate the risk of legal services being used for the purposes of money laundering. You should consider whether the inability to provide you with standard verification is consistent with the client's profile and circumstances or whether it might make you suspicious that money laundering or terrorist financing is occurring.

If you decide that a client has a good reason for not meeting the standard verification requirements, you may accept a letter from an appropriate person who knows the individual and can verify the client's identity.

For example:

- Clients in care homes might be able to provide a letter from the manager;
- For elderly clients, you may be able to accept a letter from a General Medical Practitioner;
- Clients without a permanent residence might be able to provide a letter from a householder named on a current council tax bill or a hostel manager, confirming temporary residence;

- A refugee might be able to provide a letter from the Home Office confirming refugee status and granting permission to work, or a Home Office travel document for refugees;
- An asylum seeker might be able to provide their registration card and any other identity documentation they hold, or a letter of assurance as to identity from a community member such as a religious official, GP, or local councillor who has knowledge of the client;
- A student or minor might be able to provide a birth certificate and confirmation of their parent's address or confirmation of address from the register of the school or higher education institution; or
- A person with mental health problems or mental incapacity might know medical workers, hostel staff, social workers, deputies or guardians appointed by the court who can locate identification documents or confirm the client's identity.

6.14.8 Professionals

Where other professionals use your services, in their capacity as a professional (e.g., when representing a client or on behalf of their practice) you may consider using Simplified Due Diligence as per R37.

Where other professionals use your services in their capacity as a private individual, you will still need to complete full due diligence on them as you would with any other private individual. In order to verify their identity and business address you may consult their professional directory or register along with other sources. Being a regulated professional should not lead to automatic treatment as being low risk in all cases.

You may consider the section on SDD in this context.

6.14.9 Persons acting on behalf of the client

In accordance with R28(10) where a person (the intermediary, agent or representative) purports to act on behalf of your client, you must:

- verify that the intermediary, agent or representative is authorised to act on your client’s behalf (i.e., obtain written confirmation from your client);
- identify the intermediary, agent or representative; and
- verify the identity of the intermediary, agent or representative on the basis of documents and information from a reliable source which is independent of both the representative and the client e.g., via a copy of their passport or driving license.

Someone employed by your client (depending on their position or seniority) or a director of your client may be considered as having apparent or ostensible authority to provide instructions on behalf of the client, though you may seek comfort of this on a risk sensitive basis. They should not be considered to be intermediaries, agents or representatives. Where it is not clear or apparent what their authority to instruct on behalf of the client is, CDD should not be considered to be complete.

For further information please also refer to 6.6 and 6.7.

6.14.10 Non-natural persons

R28(3A) states that where the customer is a legal person, trust, company, foundation or similar legal arrangement the relevant person must identify the customer and take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or similar legal arrangement.

This requires tracing ownership back to any ultimate beneficial ownership of the entity by a natural person(s). You must then take reasonable measures to verify the identity of the beneficial owner so that you are satisfied you know who the beneficial owner is.

This may be more challenging in cases where there are complex ownership and control structures.

When considering this test of reasonableness, you should consider whether you are comfortable that you would be able to demonstrate and evidence the extent to which you have sought such information and verification, to your supervisor upon request. It should not be misinterpreted as an allowance to not fulfil your duty to understand the full ownership and control structure of the client.

Where you have been unable to verify the identity of the beneficial owners of a non-natural person, you should consider the reasons for this and whether this should lead to a disclosure to the NCA. Further consideration should be given to whether to act or continue to act for the client, particularly where the complexity of the structures is out of your normal scope of business or make completing CDD difficult.

You should record all of your considerations as a part of the client or matter risk assessment, for more information see Section 5.

6.14.11 Companies – General Requirements

You must identify and verify

- the name of the company;
- its company number or other registration number; and
- the address of its registered office, and if different, its principal place of business.

Furthermore, the practice must take reasonable measures to determine and verify the law to which the company is subject, and its constitution (whether set out in its articles of association or other governing documents) and the full names of the board of directors (or if there is no board, the members of the equivalent management body) and the senior persons responsible for the operations of the body corporate.

A practice must collect proof of registration (e.g., via the client) or an excerpt from the relevant register before establishing a business relationship with a:

- UK company (registered or unregistered as defined in the Unregistered Companies Regulations 2009(1));
- UK Limited Liability Partnership; or
- Scottish Partnership.

You must collect proof of registration (e.g., via the client) or an excerpt from the relevant register.

Discrepancies in this information must be reported to the registrar, see Section 12 for more details.

Where the client is beneficially owned by another person, the practice must also:

- identify the beneficial owner; and
- take reasonable measures to verify the identity of the beneficial owner, along with the ownership and control structure of the non-natural person R28(4)(c).

These reasonable measures for verifying the identity of a non-natural person, may be easier to undertake for smaller entities where the beneficial owners may be more accessible. For larger entities where the beneficial owners may be more difficult to contact directly, EID&V may be of significant help when verifying their identities.

Where a company is well-known or regulated for AML to a standard equivalent to which you are subject to in the UK you may consider that the level of money laundering and terrorist financing risks are low and apply CDD on a risk-based approach. For listed companies see below.

Where you commence acting for a wholly owned subsidiary of an existing client, you may refer to the CDD file for your existing client for verification of details of the subsidiary, provided that the existing client has been identified to the standards of the Regulations or to a similar standard in another jurisdiction.

6.14.11.1 Public companies listed on Regulated Markets

You must obtain and verify the:

- company name;
- company number or other registration number; and
- address of the registered office and, if different, principal place of business.

In accordance with R28(5), if the company is listed on a regulated market it is not necessary to:

- obtain information about the beneficial owners of the company; or
- take reasonable measures to determine and verify the law to which it is subject or the names of its directors and senior persons.

This may also be applied to a majority-owned subsidiary of such a company where you have established the nature of ownership via an independent and reliable source.

For a wholly owned subsidiary of a listed company, you will also require evidence of the parent/subsidiary relationship. Such evidence may be:

- the subsidiary's last filed annual return/confirmation;
- a note in the parent's or subsidiary's last audited accounts or annual report;
- information from a reputable electronic verification service provider or online registry; or

- information from the parent company's published reports, for example, from their website.

"Regulated market" is defined as follows:

- Within the EEA, the meaning given by Article 4.1 (14) of the Markets in Financial Instruments Directive; and
- Outside the EEA, a regulated financial market which subjects' companies whose securities are admitted to trading to disclosure obligations which are equivalent to the specified disclosure obligations.

"specified disclosure obligations" means—

(a)disclosure obligations set out in Articles 17 and 19 of Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16th April 2014 on market abuse (22);
(b)disclosure obligations consistent with Articles 3, 5, 7, 8, 10, 14 and 16 of Directive 2003/71/EC of the European Parliament and of the Council of 4th November 2003 on the prospectuses to be published when securities are offered to the public or admitted to trading(23);
(c)disclosure obligations consistent with Articles 4 to 6, 14, 16 to 19 and 30 of Directive 2004/109/EC of the European Parliament and of the Council of 15th December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market(24); and
(d)disclosure requirements consistent with EU legislation made under the provisions mentioned in sub-paragraphs (a) to (c);

If a regulated market is located within the EEA there is no requirement to undertake checks on the market itself. Under a risk-based approach you may wish to simply record the steps taken to ascertain the status of the market.

Consider a similar approach for non-EEA markets that subject companies to disclosure obligations which are contained in international standards equivalent to specified disclosure obligations in the EU. Jurisdictional AML risks should also be considered – see the risk assessment section of this guidance for further information.

Consult the register on the European Securities and Markets Authority website.
Following an assessment that the client is low risk it will be sufficient, for a listed company, to obtain confirmation of the company's listing on the regulated market.

Such evidence may be:

- a copy of the dated page of the website of the relevant stock exchange showing the listing;
- a photocopy of the listing in a reputable newspaper; or
- information from a reputable electronic verification service provider or online registry.

Where a listed company is owned by multiple parties that are themselves held on a regulated market(s), this does not need to be treated differently to a listed company that is a wholly owned subsidiary of one, except that you need to collect the details of all owners as above.

When assessing a listed company's relationship with a market, you should have regard to whether a company's ownership is only partially available on a market i.e., only a percentage is publicly held. In this context, you should consider seeking further information about any owners whose relationship is not through a regulated market on a risk sensitive basis. In other words, a company having any proportion of a listing on a regulated market however small, does not mean you do not need to check other owners.

The regulated market in the UK is the London Stock Exchange. You may consider whether it is appropriate to treat companies listed on other markets in the same way as those meeting the definition of "regulated markets" on a risk sensitive basis. For example, AIM is not a 'regulated market', but you may consider, on a risk-based approach, treating it as such.

Where further CDD is required for a listed company (i.e., when it is not on a regulated market or where you otherwise deem it necessary) consider the nature of the risks presented and obtain additional information/comforts to address those risks. This may include obtaining relevant information or particulars of the company's identity or business practices.

Verification sources may include:

- a search of the relevant company registry (such as Companies House);
- a copy of the company's certificate of incorporation;
- a copy of their audited accounts; or
- information from a reputable electronic verification service provider.

You are still required to conduct ongoing monitoring of the business relationship with a publicly listed company to enable you to spot suspicious activity.

Companies whose listing does not fall within the above requirements should be identified in accordance with the provisions for private companies.

6.14.11.2 Private and unlisted companies in the UK

Private companies are generally subject to a lower level of public disclosure than public companies. In general, however, the structure, ownership, purposes and activities of many private companies will be clear and understandable.

Sources for verifying corporate identification may include:

- certificate of incorporation;
- articles of association (or equivalent formation documents);
- details from the relevant company registry, confirming details of the company and of the director/s and their addresses;
- filed audited accounts; or
- information from a reputable electronic verification service provider.

R43 requires UK companies not listed on a regulated market to provide information about their identity on request, including their articles of association or other governing documents and information about beneficial owners.

6.14.11.3 Private and unlisted overseas companies

Obtaining CDD material for these companies may be more difficult, particularly regarding beneficial ownership where ownership is held in jurisdictions where no publicly available corporate registers are available, or ownership can be otherwise concealed through the use of nominees. If this is the case, it should be taken as an increased risk factor and may warrant the application of enhanced due diligence measures.

The company's identity should be established in the same way as for UK private and unlisted companies.

Where you are not obtaining original documentation, you should consider the need for further comfort on authenticity on a risk-based approach. Certification of documents does not automatically guarantee documentation is genuine.

6.14.12 Trusts

These obligations set out below, apply to all trusts including will trusts and personal injury trusts.

6.14.12.1 Who is the client?

In the UK, trusts do not have legal personality. As such, a trust cannot be your client. When advising in relation to a trust, your client may be:

- the settlor;
- the trustee(s);
- the protector(s); or
- one or more of the beneficiaries.

Your client(s) will be the person to whom you owe your duty of care and who will receive the benefit of your advice.

Where an express trust has yet to be established and you are providing tax or transactional advice to a prospective settlor in anticipation of creating a trust, your client will usually be the settlor. Your responsibilities to verify the identity of the client and their source of funds, is then no different to any other client, except that you will also need to understand the nature and extent of the assets that will be settled on the trust.

6.14.12.2 Specific CDD requirements when instructed in relation to an existing trust

Where you are instructed in relation to an existing trust, when applying CDD: you must obtain and verify the identity of your client including beneficial owners where applicable:

- where you act for several beneficiaries (subject to conflicts issues), you must obtain and verify the identity of each of them, unless you are acting for them as a class (in which case you should identify the class by its name);
- you must, where your client has had a trust funding role, understand your client's source of wealth and the source of funds which were contributed (or which were used to acquire assets which were contributed) to the trust;
- you must understand the nature and extent of the assets settled on the trust; and
- you must understand and record the identity of the (non-client) settlor, trustee(s), protector(s), and/or beneficiary(ies) and any person who otherwise has control of the trust, as trust beneficial owners.

If the trust is a relevant trust for registration, you must also identify potential beneficiaries.

If, when you carried out CDD in relation to a trust (or legal entity/arrangement other than a body corporate) the beneficiaries were designated as a class you must establish and verify the identity of any beneficiary before you are involved in the payment to, or exercising of rights of, a specified beneficiary.

When applying CDD to a trust, or any other legal arrangement/entity which is not a company, involving a class of beneficiaries, you must always verify the identity of the beneficiary or beneficiaries before any payment is made to them or they exercise their vested rights in the trust or legal entity/arrangement (R 30 (7)).

6.14.12.3 CDD where the identified client (i.e., the trustee or the settlor) of a trust is an entity

If the identified beneficial owner is an entity, you may need to understand who its ultimate beneficial owners are, depending on the entity's status (e.g., whether it is a company or some other type of entity).

The extent of the measures you take to identify the ultimate beneficial owner of one of the trust's defined 'beneficial owners' will depend on its role in relation to the trust. The ultimate beneficial owner of a settlor, protector or sole beneficiary entity should be fully identified.

6.14.12.4 Who is a 'beneficiary' for the purposes of CDD where you act in relation to trusts?

R6(1) implies that individual beneficiaries need not be identified in CDD unless it has been determined that they will benefit from the trust. That is, unless and until they have a vested interest in the capital of the trust.

If you do not note all individual beneficiaries named in the trust deed or any associated document on the basis that their benefit from the trust has not yet been determined, you must identify any named class of beneficiaries, by its description. For example:

- grandchildren of [X]; or
- charity [Y].

As CDD can only take account of circumstances at a point in time, you should note the names of all discretionary beneficiaries (including those who have yet to acquire determined interests) named in the trust deed and any document from the settlor relating to the trust,

such as a letter of wishes. Their interests may vest (or otherwise be determined) while you are acting in relation to the trust, thus bringing them within the group of individuals who need to be noted in CDD as beneficiaries, as defined in R6(1)(c).

When considering the identity of those in whose main interest a trust is set up or operates and there are several classes of beneficiary, consider which class is most likely to receive most of the trust property. For example:

- where a trust is for the issue of [X], then the class is the issue of [X] as there is only one class;
- where a trust is for the children of [X], if they all die, for the grandchildren of [X] and if they all die for charity [Y], then the class is likely to be the children of [X] as it is unlikely that they will all die before the funds are disbursed; or
- where a discretionary trust allows for payments to the widow, the children, their spouses and civil partners, the grandchildren and their spouses and civil partners then all interests are equal, and all classes will need to be identified.

When in doubt about which class has the main interest, you should identity all classes.

However, where you act in relation to a discretionary trust, if you decide against noting in your CDD the names of individual beneficiaries who are named in the trust deed or any associated document on the basis that their benefitting from the trust has not yet been determined, you will need to seek regular updates from your client, as part of your on-going monitoring measures on a risk-based approach. This may include when and whether beneficiaries' interests in the trust will be or have been determined.

The wider approach, involving noting all beneficiaries and potential beneficiaries named in the trust deed and any associated document at CDD outset, may therefore be preferable from the outset.

6.14.12.5 What does 'an individual who has control over the trust' mean?

R6(1)(e) brings any individual who has control over the trust within the definition of the beneficial owners of a trust and they will therefore need to be identified when you act in relation to a trust.

R6(2) defines control as a power, whether exercisable alone, jointly or with the consent of another, under the trust instrument or by law to:

- dispose of, advance, lend, invest, pay or apply trust property;
- vary or terminate the trust;
- add or remove a person as a beneficiary or to or from a class of beneficiaries;
- appoint or remove trustees or give another individual control over the trust; or
- direct, withhold consent to or veto the exercise of one of the above powers.

R6(4)(b) specifically excludes from the definition of an individual who has control over a trust an individual ('P') who has control solely as a result of:

- P's consent being required in accordance with section 32(1)(c) (power of advancement) of the Trustee Act 1925;

- any discretion delegated to P under section 34 (power of investment and delegation) of the Pensions Act 1995;
- the power to give a direction conferred on P by section 19(2) (appointment and retirement of trustee at instance of beneficiaries) of the Trusts of Land and Appointment of Trustees Act 1996; or
- the power exercisable collectively at common law to vary or extinguish a trust where the beneficiaries under the trust are of full age and capacity and (taken together) absolutely entitled to the property subject to the trust (or, in Scotland, have a full and unqualified right to the fee).

6.14.12.6 CDD implications arising from the register of beneficial owners of taxable relevant trusts

If you or your practice on occasions acts as (as opposed to for) a trustee of a taxable relevant trust, pursuant to R44 of the Regulations you will need to maintain accurate and up to date records of all beneficial owners and potential beneficiaries of the trust.

Even if your practice is also acting for the trustee(s) and has applied CDD, this may involve you in more extensive investigations.

A taxable relevant trust is:

- a UK express trust, meaning that either all the trustees are resident in the UK or at least one trustee is UK resident and the settlor was UK resident and domiciled when the trust was set up or when the settlor added funds to it; or
- any other (non-UK) express trust which, in any tax year, becomes liable to pay one or more of UK income tax, capital gains tax, inheritance tax, stamp duty land tax, land and buildings transaction tax or stamp duty reserve tax in relation to UK income or assets.

If you form a business relationship in your role as trustee with a relevant person, which could be an advisory relationship with your practice (if it is subject to the Regulations), you will need to inform the relevant person that you are acting as a trustee and, on request, provide the relevant person with information identifying the trust’s beneficial owners and potential beneficiaries.

That obligation lies on (external) trustees of relevant trusts who enter into transactions in relation to which you or your practice are required to apply CDD or who form a business relationship with you or your practice (if you are subject to the Regulations). This should assist you in your compliance with your CDD obligations and is another reason why it makes sense to extend your CDD in relation to a relevant trust's beneficial owners also to cover potential beneficiaries.

Otherwise, from a reputational risk and advisory perspective, as law enforcement authorities may gain access to information not only about the trust’s beneficial owners as defined in R6(1) but also the names of those individuals who are referred to in any document from the settlor, such as a letter of wishes, relating to the trust, it is prudent to note such wider information in your CDD records where you act for any client in relation to a relevant trust, and where you act in relation to any trust.

6.14.12.7 Practical considerations of CDD for trusts

Applying CDD where you act in relation to an existing trust should generally involve your having sight of the trust deed or documents which relates to it and obtaining an appropriate understanding of their content. In some circumstances, this understanding of the content may come from an explanatory note provided by another professional regulated for AML to a similar standard. The rationale for obtaining such evidence in this manner should be documented.

In low-risk situations (as determined by appropriate and thorough documented risk assessment) you may be able to record an account of the terms of the trust given by the client or another regulated person who has had an involvement with setting up or managing the trust. However, before doing so, you should be assured that the reason for your not being provided with the trust deed and any document which relates to it makes sense in all circumstances, is recorded by you and is not indicative of a higher risk of money laundering.

You will also need to assure yourself that in identifying the trust's beneficial owners, the client or other regulated person, as appropriate, had proper regard to whether they included any individual (other than the settlor, the trustees and the beneficiaries) who has control over the trust, and potential beneficiaries.

6.14.13 Partnerships, limited partnerships, Scottish limited partnerships and UK LLPs

A partnership, other than in Scotland, is not a separate legal entity, so you must obtain information on the constituent individuals.

Where partnerships or unincorporated businesses are well-known, reputable organisations, with long histories in their industries and with substantial public information about them, their principals, and controllers the following information may be sufficient:

- name;
- registered address, if any;
- trading address; and
- nature of business.

You must still verify the identity of the partnership's beneficial owners.

R5(3) provides that in the case of a partnership (but not a limited liability partnership) the following individuals are beneficial owners:

- any individual ultimately entitled to or who controls, (whether directly or indirectly), more than 25 per cent of the capital or profits of the partnership or more than 25 per cent of the voting rights in the partnership; or
- any individual who otherwise exercises control over the management of the partnership.

Relevant points to consider when applying R5(3) are:

- the property of the entity includes its capital and its profits; and

- control involves the ability to manage the use of funds or transactions outside of the normal management structure and control mechanisms

You should also consider whether there are any other registries on which you may be able to verify the details of the partnership.

Other partnerships and unincorporated businesses which are small and have few partners should be treated for identification and verification purposes in the same way as private individuals (i.e., identifying and verifying each partner). Where the numbers are larger, they should be treated for identification and verification purposes in the same way as private companies.

Where a partnership is made up of regulated professionals, it may be sufficient to confirm the practice's existence and the trading address from a reputable professional directory or search facility with the relevant professional body. Otherwise, you should obtain evidence on the identity of at least two partners and evidence of the practice's trading address. You must still verify the identity of the partnership's beneficial owners.

For a UK LLP or SLP, you should obtain information in accordance with the requirements for companies as outlined above as these are treated as corporate entities.

Careful consideration should be made regarding clients where partners themselves are overseas entities, particularly where these overseas entities are located in jurisdictions where no publicly available corporate registers are available, or ownership can be otherwise concealed through the use of nominees or similar structures. This is particularly relevant where the vehicle is used to hold assets or is involved in transactional or other potentially high-risk activities, or conversely, where no discernible business activity can be determined, from internet searches or other sources. Such factors may be indicative of shell companies and are likely to be indicative of higher ML risk. You should give consideration to why the use of such structures may not be legitimate and the nature and purpose of the business. Your client may be able to help you understand this. Information obtained should be considered in light of other CDD information available.

Where you have assessed the client risk to be higher risk because of its structure or factors as above, then you must put in place enhanced due diligence and ongoing monitoring.

6.14.14 Foundations

Foundations may or may not have legal personality. You should investigate whether this is the case and whether it is appropriate to take on the foundation as your client or whether your client should be the board of trustees or another party involved with the foundation.

If the foundation lacks legal personality, you should approach CDD, as you would where you act for a client in relation to a trust. R6(5) provides that 'beneficial owner' in relation to a foundation or other legal arrangement similar to a trust, means those individuals who hold equivalent or similar positions to the (defined) beneficial owners of trusts.

6.14.15 Charities

Charities may take a number of forms. In the UK, you may come across five types of charities:

- small;
- registered;
- unregistered;
- excepted, such as churches; or
- exempt, such as museums and universities.

For registered charities, you should take a record of their full name, registration number and place of business. Details of registered charities in the UK can be obtained from:

- the Charity Commission of England and Wales;
- the Office of the Scottish Charity Regulator; or
- the Charity Commission for Northern Ireland.

Other countries may also have charity regulators which maintain a list of registered charities. You may consider it appropriate to refer to these when verifying the identity of an overseas charity.

For all other types of charities, you should consider the business structure of the charity and apply CDD appropriately. You may also get confirmation of UK charitable status from HMRC. Further, in applying the risk-based approach to charities it is worth considering whether it is a well-known entity or not. The more obscure the charity, the more likely you are to want to view the constitutional documents of the charity, along with any other documents that may clarify the individuals in control and its status.

Due to the numerous examples of charities and not-for-profit organisations as fund raising vehicles for terrorist organisations you may want to also consult HM Treasury's consolidated list of persons designated as being subject to financial restrictions to ensure the charity is not a designated person.

Another point to consider is Source of Funds, in that charities may fund transactions effectively through crowdfunding, which can make a Source of Funds check difficult to complete. Taking a risk-based approach you should consider whether you need to seek information as to who those individuals or entities are that are funding the charity, particularly those contributing larger percentages or amounts.

6.14.16 Deceased persons' estates

When acting for the executor(s) or administrators of an estate, you should establish their identity using the procedures for natural persons or companies set out above. When acting for more than one executor or administrator, you should verify the identity of at least two of them. You should also get copies of the death certificate, grant of probate and any letters of administration.

If a will trust is created, and the trustees are different from the executors, the procedures in relation to trusts will need to be followed when the will trust comes into operation.

6.14.17 Churches and places of worship

Places of worship may either register as a charity or can apply for registration as a certified building of worship from the General Register Office (GRO) which will issue a certificate. Further, their charitable tax status will be registered with HMRC. As such, identification details with respect to the church or place of worship may be verified:

- as for a charity;
- through the headquarters or regional organisation of the denomination or religion;
- with reference to the GRO certificate; or
- through an enquiry to HMRC.

6.14.18 Schools and colleges

Schools and colleges may be a registered charity, a private company, an unincorporated association or a government entity and should be verified in accordance with the relevant category. The Department of Education maintains lists of approved educational establishments which may assist in verifying the existence of the school or college.

6.14.19 Clubs and associations

Many of these bear a low money laundering risk, but this depends on the scope of their purposes, ownership structure, activities and geographic spread.

The following information may be relevant to the identity of the club or association:

- full name;
- legal status;
- purpose;
- any registered address; or
- names of all office holders.

Documents which may verify the existence of the club or association include:

- any articles of association or constitution;
- statement from a bank, building society or credit union;
- recent audited accounts; or
- financial statements presented to the annual general meeting.

6.14.20 Government agencies and councils

The money laundering and terrorist financing risks associated with public authorities vary significantly depending on the nature of the retainer and the home jurisdiction of the public authority. It may be simple to establish that the entity exists, but where there is a heightened risk of corruption or misappropriation of government monies, greater monitoring of retainers should be applied.

The following information may be relevant when establishing a public sector entity's identity:

- full name of the entity;
- nature and status of the entity;
- address of the entity;
- name of the home state authority;
- name of the directors or equivalent;
- name of the individual instructing you and confirmation of their authority to do so; or
- extract from official government website.

Under R37(3) the fact that the client is a public administration or publicly owned enterprise is one of the factors to consider when deciding whether it is low risk and whether to apply simplified due diligence. It will usually be appropriate to apply simplified due diligence to UK public authorities and to some non-UK public authorities, particularly those in the EEA.

6.14.21 Further Information

You may wish to consider the UK Financial Services Joint Money Laundering Steering Group (JMLSG) guidance Part 1 – (available here) as a useful source of information on possible ways to apply CDD on the above entities, and across a broader range of other entity structures. You should note though that in the context of legal services, the LSAG guidance takes precedent.

6.15 Beneficial ownership requirements

6.15.1 Definition of a beneficial owner

A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted. In respect of private individuals (i.e., a natural person), the client themselves may be treated as the beneficial owner, unless there are features of the transaction, or surrounding circumstances, that indicate otherwise.

Therefore, if your client is an individual, you may want to consider whether they are acting on their own behalf. A question to ask yourself in this context and more generally is: “do the services I am being asked to provide make sense given what I know about the client?”

R5(1) defines the beneficial owner of a body corporate, other than a listed company, as meaning:

any individual who:

- exercises ultimate control over the management of the body corporate;
- ultimately owns or controls, directly or indirectly, including through bearer share holdings or other means, more than 25% of the shares or voting rights in the body corporate;
- otherwise controls the body:
    - by satisfying one or more of the conditions set out in Part 1 of Schedule 1A to the Companies Act 2006 (persons with significant control); or
    - if the individual were an undertaking, the body corporate would be a subsidiary undertaking of the individual under section1162 of the Companies Act 2006 read with Part 7 of that Act.

This does not apply to a company listed on a regulated market. It does apply to UK limited liability partnerships.

Regulation 6(1) In relation to a trust, the Regulations define the beneficial owner as each of:

- the settlor;
- the trustees;
- the beneficiaries, or where the individuals benefiting from the trust have not been determined, the class of persons in whose main interest the trust is set up, or operates; and
- any individual who has control over the trust.

In relation to a foundation or other legal arrangement similar to a trust, the beneficial owners are those who hold equivalent or similar positions to those set out above in the case of trusts.

In relation to a legal entity or legal arrangement which does not fall into the above, the beneficial owners are:

- any individual who benefits from the property of the entity or arrangement;
- where the individuals who benefit from the entity or arrangement have yet to be identified, the class of persons in whose main interest the entity or arrangement is set up or operates; and
- any individual who exercises control over the property of the entity or arrangement.

Unincorporated associations and foundations are examples of entities and arrangements likely to fall within these requirements.

When applying this, relevant points to consider are:

- the property of the entity includes its capital and its profits;
- determined benefits are those to which an individual is currently entitled;
- contingent benefits or situations where no determination has been made should be dealt with as a class to which (and because) benefit has yet to be determined;
- a class of persons need only be identified by description;
- an entity or arrangement is set up for, or operates in, the main interest of the persons who are likely to get most of the property;
- control includes the ability to manage the use of funds or transactions outside the normal management structure and control mechanisms; and

- where you find a body corporate with the requisite interest outlined above, you will need to make further proportionate enquiries as to the beneficial owner of the body corporate.

6.15.2 Other forms of control

You should be alert to the risk that a corporate entity can also be subject to control by persons other than shareholders. Such control may rest with those who have power to manage funds or transactions without requiring specific authority to do so, and who would be in a position to authorise changes to internal procedures and control mechanisms. Depending on the control structures in an entity, this could be a senior role operating without actual or effective supervision or another entity.

You should remain alert to any person or entity with such powers while you are obtaining an understanding of the ownership and control structure of the corporate entity and make such further enquiries you need in order to understand the control structure. Monitor situations within the retainer where control structures appear to be bypassed or unduly complex on a risk sensitive basis.

6.16 CDD on a beneficial owner

6.16.1 General Comments

Beneficial Owners must be identified, and reasonable measures must be taken to verify their identities so that you are satisfied you know who the beneficial owner is and that they are in fact the beneficial owner in question.

In complex structures, practices may have to look through layers of ownership (and consider any associated dilution of that ownership) to arrive at any natural persons owning or controlling the client entity.

It is important to review both shareholdings **and** voting rights in respect of beneficial ownership, along with understanding the class and value of shares any individual holds.

Where the shareholding of an entity indicates that no one owns or controls over 25% of a client you may wish to consider whether it is appropriate that the senior manager (e.g., CEO, board, controlling mind of the company) be considered as the beneficial owners under R5(1))(a) and (c). This is subtly different to the requirements of R28(8) and would not necessarily raise a concern of extra risks as the circumstances of R28(7) might.

When conducting CDD on a client, you will need to identify any beneficial owners as defined above. This may be undertaken by obtaining:

- shareholder details from a reputable online registry or commercial provider;
- a copy of a detailed structure chart; and
- a copy of the trust deed, partnership agreement or other such document.

It is not enough to solely rely on the information contained in a company's register of persons with significant control. You should consider what is the appropriate level of verification required on an RBA.

These reasonable measures to verify a beneficial owner, may differ to those you may use to verify the identity of a client that is a natural person. For example, you may not require passports or driving licenses in these circumstances, but EID&V may present an effective way to verify the identities of beneficial owners.

It is for your practice to determine a tailored and risk sensitive approach that is appropriate to ensure you are satisfied you know who a beneficial owner is and that you fully understand their relationship with the non-natural person.

6.16.2 Requirements introduced in 2020

If you cannot identify the beneficial owner (where they have 25% or more holding of the company), you should consider whether this makes the client or matter higher risk and treat it accordingly and consider whether you should continue to act for the client.

If you cannot identify a beneficial owner pursuant to the above despite having exhausted all possible means of doing so or if you are not satisfied that the person is the beneficial owner, you must then take reasonable measures to verify the identity of the senior responsible manager of the body corporate. Depending on the circumstances, it may be that you have already concluded this is the case on the basis that the individual "exercises ultimate control over the management of the body corporate" under Regulation 5(1)(a), although you should note that the scope of Regulation 5(1)(a) is not limited to this scenario.

In practice, this may be the Chief Executive Officer or President of the group, or someone else in the executive team with high level responsibility for the running of the relevant aspect of the body corporate.

You must also record:

- All the actions you have undertaken to this end; and
- Any difficulties encountered.

6.16.3 Agency

R6(9) says a beneficial owner generally means any individual who ultimately owns or controls the client or on whose behalf a transaction is being conducted.

In most cases, it is presumed that the client is acting on their own behalf, unless the features of the transaction indicate that they are acting on someone else's behalf. As highlighted above you should make enquiries when it appears the client may be acting on behalf of someone else.

Situations where a natural person may be acting on behalf of someone else include:

- exercising a power of attorney - the document granting power of attorney may be sufficient to verify the beneficial owner's identity;

- acting as the deputy, administrator or insolvency practitioner - appointment documents may be sufficient to verify the beneficial owner's identity; or
- acting as an appointed broker or other agent to conduct a transaction - signed letter of appointment may be sufficient to verify the beneficial owner's identity.

You should be alert to the possibility that purported agency relationships are actually being utilised to facilitate a fraud, leading to possible encounters with the proceeds of crime. Understanding the reason for the agency, rather than simply accepting documentary evidence of such at face value, will assist to mitigate this risk. Where a client or retainer is higher risk, you should obtain further verification of the beneficial owner's identity in line with the suggested CDD methods to be applied to natural persons.

This may also include where a legal practice commissions your services on behalf of someone else.

6.16.4 Companies

6.16.4.1 A proportionate approach

Where you have adequately assessed ML risk to be lower, it would not be generally proportionate to conduct independent searches across multiple entities at multiple layers of a corporate chain to see whether, by accumulating very small interests in different entities, a person finally achieves more than a 25 per cent interest in the client corporate entity. Nevertheless, you must be satisfied that you have an overall understanding of the ownership and control structure of the client company. This provision does not apply in any situations of higher risk, where EDD should be applied.

6.16.4.2 Companies with capital in the form of bearer shares

A bearer share is a form of equity (i.e., a stock or share in a company or equivalent) wholly owned by whoever holds the physical stock certificate. Given this, there is no way to register the owner of the stock confidently or consistently nor track transfers of ownership

These pose a much higher risk of money laundering as it is often difficult to identify beneficial owners and such companies are often incorporated in jurisdictions with lower AML/CTF regulations. You should consider whether the risk posed is acceptable for your practice before proceeding.

If you do proceed, you must adopt procedures to establish the identities of the holders and material beneficial owners of such shares and ensure you are notified whenever there is a change of holder and/or beneficial owner (i.e., who they are held on behalf of).

This might be achieved by:

- requiring that the shares be deposited with you or a regulated person with whom you have a binding covenant; or
- getting appropriate assurance that either such a regulated person or the holder of the shares will notify you of any change of records/holder/ownership relating to the shares.

Ultimately it is for your practice to determine the confidence you can place in any assurances that the bearer shares will not be used to hide money laundering or terrorist financing, however extreme caution must be exercised. Bear in mind that the issuance of bearer shares has been banned in the UK since May 2015, primarily due to money laundering and transparency concerns. Enhanced due diligence and ongoing monitoring should be performed and practices must be able to demonstrate the effectiveness of controls in place to their supervisor.

Where a practice does undertake work for clients where beneficial ownership is held in the form of bearer shares, this should be articulated in the Practice-Wide Risk Assessment.

6.16.5 Trusts

Whenever you are instructed by someone involved with an existing trust to advise in relation to it, you must extend your CDD to the trust's beneficial owners.

You should take a risk-based approach to verifying the identity of the ultimate beneficial owner/s of a professional trustee entity (as they should have no interest in the assets placed in trust). Higher-risk indicators may be where the professional trustee entity is unregulated or where the professional trustee is not independent of the settlor (e.g., family offices). Where such factors are present, reasonable measures should be taken to verify the identity of the beneficial owner/s of the trustee. Lower risk factors may be where the professional trustee is itself a regulated entity (or owned by one) or is large, well-known and/or listed on a regulated market. In such low-risk instances, you should not need to identify and verify beneficial ownership of the professional trustee, although you should document the rationale for your actions.

R28(4)(a) requires a relevant person to identify the beneficial owner 'of a client' which is beneficially owned by another person. R6(1) defines 'the beneficial owners in relation to a trust' as the settlor, the trustees, the beneficiaries (or class of beneficiaries) and any individual who has control over the trust. Although your client will not actually be the trust (because a trust does not have legal personality), if you advise any client in relation to a trust, the Regulations require you to understand who the trust's other beneficial owners are, as defined in R6(1).

6.17 Source of Funds and Source of Wealth

6.17.1 Overview

A fundamental element of client due diligence is understanding the nature, background and circumstances of the client, including their financial position – and making an assessment as to whether the legal services provided to the client are in keeping with your understanding of that background and circumstances.

The extent to which you must obtain, review and evidence your client's financial position is dependent upon the risk profile of the client or matter. In enhanced due diligence situations this requirement is more stringent.

The financial circumstances of a client can broadly be categorised into Source of Funds (SoF), and Source of Wealth (SoW).

A practice must scrutinise transactions on a matter-by-matter basis, with the objective of understanding what the source of funds are for transactions you undertake on behalf of a client. This is a fundamental aspect of holistic CDD. It is important to remember that understanding the SoF and SoW is a key protection for your practice, and it should be approached as an opportunity to protect your practice from being used for money laundering.

The type of documentation accepted to verify SoW or SoF should depend on the level of ML/TF risk presented by the customer. The higher the risk, the more comprehensive and reliable documents you obtain should be.

Taking a risk-based approach, you may consider funds remitted from a legal practice regulated for AML to equivalent standards as the Regulations as being of lower risk.

You must take adequate measures to check SoF and SoW as a part of EDD when applied to PEPs. You should also consider doing so as a part of ongoing monitoring of any business relationship (whether high risk or otherwise). You should also apply a source of wealth check in other applications of EDD on a risk-based approach.

It is good practice to check the SoF even if a business relationship as defined in the Regulations has not been formed, and the matter is an occasional transaction. It should be considered that checking source of funds is a useful practical tool for protecting your practice generally.

It is important to document the source of funds checks conducted on each client or matter – this may be by way of the collation of information/evidence obtained, and/or the inclusion of a file note outlining what checks were undertaken, what evidence obtained, and the conclusions derived from these checks.

SoF and SoW do not mean the same thing, although there can be significant overlap between the two and they do not exist in isolation to each other.

6.17.2 Source of Funds

Source of Funds

Source of Funds refers to the funds that are being used to fund the specific transaction in hand – i.e., the origin of the funds used for the transactions or activities that occur within the business relationship or occasional transaction. The question you are seeking to answer should not simply be, “where did the money for the transaction come from,” but also “how and from where did the client get the money for this transaction or business relationship.” It is not enough to know the money came from a UK bank account.

For further reference see point 87 in the following FATF guidance here.

6.17.2.1 Establishing Source of Funds:

The types of data and documents that you use for verification of Source of Funds will vary depending on the circumstances and the information that the customer provides to you.

The SoF pertains directly to the funds that are being used to fund the specific transaction in hand i.e., the origin of the funds used for the transactions or activities that occur within the client's business relationship with you. Checking this means ascertaining where those funds came from, how they were accumulated by the client and ensuring on a risk-based approach that they are not the proceeds of crime.

SoF is not simply be limited to knowing from which financial institution the funds in question may have been transferred, except where the financial institution is providing financing for the transaction e.g., via mortgage. It should also not be limited to checking that the client's name matches the name on the account.

In addition to documenting the

- Amount;
- Currency, and
- The remitting account details (bank, account number, sort code, name on account)-

-the information obtained should be substantive and establish a provenance or reason for having been acquired e.g., salary, gift etc.

Acquiring bank statements, Wills, full payslips, audited financial accounts showing funds disbursed to the client, sales/purchase agreements, receipts of other transactions or similar documentation may all be useful in establishing source of funds. Establishing income from share capital, business activities, a bequest of gift etc. can also help you.

In circumstances where a client declares that they have been given funds for a transaction from a third party you may wish to record information relating to that original transaction too. You may verify this by requesting bank statements and other relevant documentation relating to this transfer.

SoF can often be difficult to determine without some understanding of the source of wealth of the individual. This can particularly be the case where the funds for a transaction have become mixed with other funds in an account. Here, to understand the SoF, you may need to have an awareness of the SoW of the individual, although your level of confidence in the source of wealth in such a case, should be considered on a risk-based approach.

6.17.3 Source of Wealth

Source of Wealth

The source of wealth refers to the origin of a client's entire body of wealth (i.e., total assets).

SoW describes the economic, business and/or commercial activities that generated, or significantly contributed to, the client's overall net worth/entire body of wealth. This should recognise that the composition of wealth generating activities may change over time, as new activities are identified, and additional wealth is accumulated.

You should seek to answer the question: "why and how does the individual have the amount of overall assets they do – and how did they accumulate/generate these?"

For further reference see point 88 in the following FATF guidance here.

SoW is a holistic appraisal as to where an individual or an entity has derived their overall wealth (i.e., the origin of their entire body of assets), rather than any specific portion of it.

To check SoW in a low/medium risk transaction, you may be comfortable identifying the SoW by asking and recording how the client has accrued their wealth or by verifying the client's business interests through public searches. For low/medium risk transactions in relation to companies and other body corporate clients you could be comfortable that the intended transaction is consistent with what you know about the company. For guidance in establishing SoW in higher risk situations see 6.18.3.

For further information on source of wealth requirements please see the Enhanced Due Diligence section below.

In-depth guidance on Source of Wealth and Source of Funds requirements has been issued by the Wolfsberg Group and can be found here.

6.18 Enhanced Due Diligence

R33 provides that you must apply enhanced due diligence (EDD) and enhanced ongoing monitoring in addition to the CDD measures required in R28, where:

- the case has been identified as one where there is a high risk of money laundering or terrorist financing in your risk assessment or in the information made available to you by your supervisor under R17(9) and R47;
- you carry out an occasional transaction and either party to the transaction is established in a high-risk third country;
- the client is a politically exposed person (PEP), or a family member or known close associate of a PEP;
- the client is established in a high-risk third country;
- the client has provided false or stolen identification documentation or information on establishing the relationship and you have decided to continue dealing with the client;
- there is any other situation which you have assessed as presenting a higher risk of money laundering or terrorist financing; or
- wherever the transaction:
    - is complex

- unusually large
- there is an unusual pattern of transactions, or
- the transaction or transactions have no apparent economic or legal purpose.

6.18.1 Enhanced Due Diligence and the Beneficial Ownership Threshold

In high-risk situations warranting the application of enhanced due diligence, it may be appropriate to examine beneficial owners with less than 25% ownership if you have concerns regarding the ownership structure or feel that the ownership structure is a pertinent risk factor, to fully understand control and ownership interests in the client.

6.18.2 What is EDD?

The Regulations specify that you must take measures to examine the background and purpose of the transaction and to increase the monitoring of the business relationship where enhanced due diligence is required. The Regulations are not prescriptive about exactly what must be included in EDD, with the exception of clients that are PEPs.

As per R33(5), EDD may include (while not being restricted to):

- seeking additional independent, reliable sources to verify information provided or made available to you;
- taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction;
- taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship; or
- increasing the monitoring of the business relationship, including greater scrutiny of transactions.

In the case of a High Risk Third Country (HRTC), EDD is more restrictive.

If you are establishing a business relationship with a client in a HRTC, you will need to apply the EDD including the steps below. You will also need to apply the steps below when either your client or the counterparty is established in a HRTC where you are undertaking an occasional transaction (within the meanings of R27(1)(b) and (2)).

In these circumstances, EDD must include:

- obtaining additional information on the client and on the client's beneficial owner;
- obtaining additional information on the intended nature of the business relationship;
- obtaining information on the source of funds and the source of wealth of the client and the client's beneficial owner;
- obtaining information on the reasons for the transactions;
- obtaining the approval of senior management for establishing or continuing the business relationship; and
- conducting enhanced monitoring of the business relationship including increasing the frequency and number of checks or other controls applied; and selecting patterns of transactions that trigger a requirement of further explanation to your practice.

If a client with whom you have a business relationship (not in a HRTC) is engaging in a transaction where the counterparty is based in a HRTC, you should consider the risks this presents and whether it is appropriate to apply EDD to the transaction.

You should also consider whether it is appropriate to go beyond the above minimum requirements, particularly in circumstances of higher risk or where you have identified red flags. This may include for example seeking greater verification of the client's identity, background and circumstances from independent and reliable information sources. It may also mean lowering beneficial ownership thresholds below 25% or conducting further screening or adverse media searches on directors or beneficial owners of the client.**=**

6.18.3 Establishing source of wealth

(Please also see 16.7.3)

An important additional EDD measure should include understanding the financial situation of the client – in practice this means taking additional measures to understand the SoW as well as the SoF of the client.

You should consider the level and nature of verification required in light of the risks posed by the client, transaction and/or business relationship.

As part of your EDD process you should verify the SoW with evidence obtained from the client and/or independent sources until you are comfortable that you understand where the client's overall wealth has been derived from and (to the best of your knowledge) that it is legitimate. You should document your rationale in a file note.

When addressing SoW, you should consider whether the SoW is commensurate to your client in general i.e., does it make sense that the client in front of you obtained their wealth in the way that they have advised you?

The SoW refers to the origin of a client's entire body of wealth (i.e., total assets). This information will usually give an indication as to the volume of wealth the client would be expected to have, and a picture of how the person acquired such wealth.

It does not however require you to account for all of a client's assets, but to build a rationale and reasoning as to why they have such wealth and to provide assurance that it was obtained through legal means. This will help you to establish whether the transaction makes sense.

In many complex scenarios it may be difficult to determine original sources of wealth, possibly accrued many years ago. In such scenarios, reasonable efforts must be undertaken to obtain relevant information from the client, and this must be reviewed in light of other risk factors, such as jurisdictional/geographic risk, adverse media, PEP status and transaction type (especially transactions which may help obscure the ownership or transfer of assets).

Although a practice may not have specific information about assets not deposited or processed by them, it may be possible to gather general information from commercial databases or other open sources.

Where the client's SoW is not readily apparent, the first step in establishing either SoF or SoW is asking questions of your client and where appropriate seeking independent verification and corroboration of information across a variety of sources, to build a picture of the client's background and circumstance which may require asking questions of the client.

Actions taken, documentation and materials reviewed, and decisions taken (including rationale) must be clearly recorded. These may be reviewed at a later date by your supervisor or other relevant authorities.

Where you cannot successfully establish the SoW in higher risk situations, you should consider ceasing to act for the client and whether you need to submit a report to the NCA.

6.18.4 Enhanced monitoring

Enhanced ongoing monitoring is automatically required whenever EDD is applied.

One aspect of keeping transactions under review is to ensure they are still in line with the CDD information held on the client, and information contained in the client and matter risk assessments. Whatever controls you have in place to monitor other business relationships, may be intensified in order to apply enhanced monitoring.

This may include:

- requiring a greater level of information and explanation from the client when activity diverts from that addressed in their client risk assessment;
- greater frequency of checks on transactions, particularly SoF; or
- undertaking more frequent due diligence checks on your client.

You should ensure that funds paid into your client account come from an expected source and are for an amount commensurate with the client's known wealth and with what is expected to be deposited in relation to the matters on which you act for them.

6.19 When to apply EDD

6.19.1 High-risk third countries

You must apply EDD measures in any business relationship with a person established in a high risk third country or in any transaction where either party is established in a high-risk third country. The list of countries is available here.

Being “established in” a country means:

- in the case of a legal person, being incorporated in or having a principal place of business (head office) in that country, or for a financial institution having its main regulator in that country; or
- in the case of a natural person, being resident in that country but not necessarily simply having been born in that country.

However, this requirement does not apply if:

- the client is a branch or majority owned subsidiary of an entity which is established in an EEA state and subject to the 5th Money Laundering Directive;
- it complies with the group wide policies established by the entity under Article 45 of the Directive, and

- you do not consider EDD measures to be necessary taking a risk-based approach.

Under the Regulations, a high-risk third country is defined as a country which has been identified by the European Commission under Article 9.2 of the 5th Directive. The current list of high-risk third countries can be found here.

Note that not all countries where there may be a higher risk of money laundering are 'high-risk third countries' for these purposes. Other jurisdictions may equally pose higher ML risks – these should be assessed as part of client and matter risk assessments, and additional, enhanced due diligence measures should be applied accordingly.

6.19.2 Other situations of higher risk of money laundering or terrorist financing

Enhanced due diligence is also required where there is a higher risk of money laundering or terrorist financing. In determining whether there is a higher risk of money laundering or terrorist financing in a given case, you must consider the risk factors set out in R33(6), along with the outcomes of your practice-wide, client and matter risk assessments.

Instances of high risk as detailed in your supervisor's risk assessment and in the National Risk Assessment also require EDD to be applied.

Please see the features outlined in Section 5 and 18 of this guidance for further information. You should consider the situation in context of the CDD information held on your client, including their background and financial circumstances.

Regulation 33(6) – Risk Factors you must consider when determining whether to apply EDD

When assessing whether there is a high risk of money laundering or terrorist financing in a particular situation, and the extent of the measures which should be taken to manage and mitigate that risk, relevant persons must take account of risk factors including, among other things—

(a)**customer risk factors**, including whether—
(i) the business relationship is conducted in unusual circumstances;
(ii) the customer is resident in a geographic area of high risk (see sub-paragraph (c));
(iii) the customer is a legal person or legal arrangement that is a vehicle for holding personal assets;
(iv) the customer is a company that has nominee shareholders or shares in bearer form;
(v) the customer is a business that is cash intensive;
(vi) the corporate structure of the customer is unusual or excessively complex given the nature of the company's business;
(vii) the customer is the beneficiary of a life insurance policy; o
(viii) the customer is a third country national who is applying for residence rights in or citizenship of an EEA state in exchange for transfers of capital, purchase of a property, government bonds or investment in corporate entities in that EEA state;

(b)**product, service, transaction or delivery channel risk factors**, including whether—
(i) the product involves private banking;
(ii) the product or transaction is one which might favour anonymity;

(iii) the situation involves non-face-to-face business relationships or transactions, without certain safeguards, such as an electronic identification process which meets the conditions set out in regulation 28(19);
(iv) payments will be received from unknown or un-associated third parties;
(v) new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products;
(vi) the service involves the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in a third country;
(vii) there is a transaction related to oil, arms, precious metals, tobacco products, cultural artefacts, ivory or other items related to protected species, or other items of archaeological, historical, cultural or religious significance or of rare scientific value

(c) **geographic risk factors**, including—
(i) countries identified by credible sources, such as FATF mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing;
(ii) countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism (within the meaning of section 1 of the Terrorism Act 2000(86)), money laundering, and the production and supply of illicit drugs;
(iii) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
(iv) countries providing funding or support for terrorism;
(v) countries that have organisations operating within their territory which have been designated—
(aa) by the government of the United Kingdom as proscribed organisations under Schedule 2 to the Terrorism Act 2000(87), or
(bb) by other countries, international organisations or the European Union as terrorist organisations; and
(vi) countries identified by credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or non-governmental organisations as not implementing requirements to counter money laundering and terrorist financing that are consistent with the recommendations published by the Financial Action Task Force in February 2012 and updated in June 2019.

As well as considering the risks identified above, you should have regard to any of the risk factors discussed in Section 5 that may be present in a given client or matter.

6.19.3 Screening, Due Diligence & Other Control Measures - Politically-Exposed Persons

Politically Exposed Persons (PEPs) present risks as they have the opportunity to use their political position to enrich themselves through corrupt activities. In order to treat PEPs in a risk-based way, it is a precondition that you can correctly identify them.

6.19.3.1 Who is a PEP?

A PEP is a person who has been entrusted within the last year (or for a longer period if you consider it appropriate to address the risks in relation to that person) with one of the

following prominent public functions by a public institution, an international body, or a state**, including the UK**.

Listing of PEP roles R35(14)

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliament or similar legislative bodies;
- members of governing bodies of political parties;
- members of supreme courts, of constitutional courts, or any judicial body whose decisions are not subject to further appeal, except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, charges d'affaires and high-ranking officers in the armed forces;
- members of the administrative, management or supervisory bodies of state-owned enterprises; or
- directors, deputy directors and members of the board of equivalent function of an international organisation.

In addition to the primary PEPs listed above, a PEP also includes (R35(12)):

- family members of a PEP – spouse, civil partner, children, their spouses or partners, and parents; and
- known close associates of a PEP – persons with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relationships, or who is a sole beneficial owner of a legal entity or arrangement set up by the primary PEP.

Middle ranking and junior officials are not PEPs. In the UK, only those who hold truly prominent positions should be treated as PEPs and the definition should not be applied to local government, more junior members of the civil service or military officials other than those holding the most senior ranks. This should be borne in mind as many commercially available PEP checking tools may have a much lower threshold for considering an individual a PEP.

In the Government consultation on 5MLD, it was strongly suggested that the FCA's guidance on PEPs should be the standard across the board.

Section 2.16 of this FCA guidance sets out the FCA's view of what categories of person should be treated as PEPs in the UK (building on the above).

6.19.3.2 Identifying a PEP

R35(1) requires you to have appropriate risk management systems and procedures to determine whether a client or beneficial owner is a PEP.

Practices must take a risk-based approach to identifying PEPs.

To assess your risk of encountering a PEP, you must consider your PWRA, the level of risk of money laundering or terrorist financing inherent in your business and the extent to which that risk would be increased by a business relationship with a PEP.

In larger or more specialist practices where it may be reasonably expected to undertake work on behalf of PEPs in the normal or regular course of business, frequency and intensity of PEP screening should be increased (potentially using an established commercial provider), both at the outset of the matter and an ongoing basis. Many practices use services that can run checks against PEP databases which they maintain.

Where you have a higher risk of having PEPs as clients or you have reason to suspect that a person may actually be a PEP contrary to earlier information, you should consider conducting some form of electronic verification.

The range of PEPs is wide and constantly changing, so any EID&V will not give you total certainty. You should have reference to Section 7 when considering the possible confidence you may place in the abilities of any EID&V tool.

Regardless of the result of any single check you should consider the wider possibility that your client is a PEP.

Questions you should ask with regard to PEP Status

- What role(s) does the individual hold?
- What is the nature and context of business relationship?
- What services or products does the PEP wish to use?
- What is the potential for the product to be misused for the purposes of corruption?
- Do you know if they have close family members or known associates and if so, what roles do they hold?
- What level of public scrutiny, exposure, governance, disclosures or accountability in their role is the PEP subject to?
- Are their accompanying geographic risks associated with the PEP relationship?
- If you have identified a PEP, were they helpful in providing this information and if not, should and how would this impact my assessment of the risk present?
- Does the nature of their PEP status impact in the level of EDD that needs to be applied, and if so, how?

In practices where undertaking work on behalf of PEPs is unlikely or a very rare occurrence, it may be acceptable to use publicly available or open sources. Checking for PEP status should be undertaken on a risk-based approach, in light of other CDD information held (such as employment) which may lead to the practice suspecting PEP status.

Simple measures may include:

- asking the client or their representative (as appropriate) whether the person is a PEP, as a part of client onboarding;
- performing an internet search in order to check whether the individual may hold any position that qualifies them as a PEP; or
- reviewing the information, they submit to you carefully to determine whether any information you have access to, suggests they may be a PEP.

Other indicators that may indicate your client is a PEP include:

- receiving funds from a government account;
- correspondence on official letterhead from the client or a related person;
- information from the client or person related to the matter linking the client to a PEP; and
- any information which comes to your attention suggesting your client is actually a PEP or linked to one.

Where you suspect a client is a PEP but cannot establish that for certain, you should consider what steps you could take in order to resolve this uncertainty. If you are not able to resolve the issue to your satisfaction, you may consider (on a risk-based approach) applying aspects of enhanced due diligence procedures (as a lack of clarity as to whether a person is a PEP could, in and of itself, be indicative of a heightened risk of money laundering).

It is worth reiterating from the outset that family members of PEPs, and known close associates of PEPs, must be treated as PEPs in terms of the due diligence you apply. You should apply the same standard of investigation when identifying whether someone is a family member of a PEP, as you do for a PEP.

R35(15) sets out a different process for “known close associates.”

“For the purpose of deciding whether a person is a known close associate of a politically exposed person, a relevant person need only have regard to information which is in its possession, or to credible information which is publicly available.” This means that you are only expected to be able to identify a known close associate where the information you already hold tells you that this is what they are, or if it is publicly available.

6.19.3.3 Mitigation of PEP Risk

In deciding what risk mitigation to apply you must (R35(2)) take account of—

- your PWRA;
- the client or matter risk assessment; and
- any information published by your supervisor.

PEPs may pose a higher risk, by virtue of having a greater potential opportunity to be involved in corruption, due to the positions or access to public funds they hold. Being a PEP should not, preclude access to legal services, provided the practice undertakes the necessary enhanced due diligence measures.

When there is a PEP relationship (including where a PEP is a beneficial owner of a client and where a client or its beneficial owner is a family member or known close associate of a PEP), the Regulations specify that you must take the following steps to deal with the heightened risk:

- have senior management approval for establishing a business relationship with a PEP or an entity beneficially owned by a PEP;
- take adequate measures to establish the SoF **and** SoW which are involved in the business relationship or occasional transaction;
- conduct closer ongoing monitoring of the business relationship; and

- consider which aspects of your EDD protocol are appropriate for the PEP in question.

Where you have a beneficial owner who you know to be a PEP, you should consider on a risk-based approach what extra EDD measures, you need to take when dealing with that client.

Where the client is a state-owned entity and the PEP in question is only a PEP due to their position in the State-Owned Entity, you may consider whether this mitigates the risks present.

A useful source of further information is the FCA's guidance on the treatment of politically exposed persons for anti-money laundering purposes. The guidance is aimed at practices supervised by the FCA, but you should take it into account in accordance with R35(4)(b)(i).

6.19.3.4 Senior management approval for onboarding a PEP

R3(1) defines 'senior management' as:

An officer or employee of the relevant person with sufficient knowledge of the relevant person's money laundering and terrorist financing risk exposure, and of sufficient authority to take decisions affecting its risk exposure.

The FCA guidance referred to above sets out their view as to who, for the purposes of the Regulations, should be treated as coming within the definition of senior management.

For legal practices, senior management may be:

- a member of the board of directors or equivalent senior management team;
- the head of a practice group or department or function;
- a senior or managing partner; or
- the MLRO or, if different, the MLCO.

Other individuals may fall into this category depending on the nature and structure of your practice.

Senior Management may delegate the application of their roles to other suitably senior and competent individuals however they remain ultimately responsible and accountable. You should advise those responsible for monitoring risk assessments that a business relationship with a PEP has begun, to help their overall monitoring of the practice's risk profile and compliance.

For sole practitioners, you should appropriately record your decision e.g., as a conclusion to the client or matter risk assessment.

6.20 Simplified Due Diligence

Under R37, you may be allowed to relax the type, timing and extent of measures undertaken under CDD where a matter is eligible for Simplified Due Diligence (SDD). You

must continue to monitor the relationship and transactions to ensure that SDD continues to be appropriate.

You must carry out sufficient monitoring of the relationship or transaction to enable you to detect any unusual or suspicious transactions.

Earlier iterations of the Regulations listed circumstances where one **could** apply SDD. While the factors below no longer signify that you can *automatically* apply SDD they may still indicate entities which may qualify.

It may also be useful to consider these in the context of determining that SDD would **not** be appropriate, regardless of other circumstances that may be present.

6.20.1 When is it appropriate to use simplified due diligence?

SDD is the lowest permissible form of due diligence and must only be used where you have determined that the client presents a low risk of money laundering or terrorist financing.

You must record your reasoning for why you have determined that it is appropriate to use SDD via your client or matter risk assessment. It may be that due to factors recognised in your PWRA, it may not be appropriate for your practice to use SDD at all.

When assessing whether there is a low risk of money laundering or terrorist financing such that SDD can be applied, you must consider:

- your PWRA and any sectoral risk assessment information supplied by your supervisor or HMT under R17 or R47 and;
- whether the client is:
    - a public administrator or a publicly owned enterprise;
    - an individual resident in a geographic area of lower risk;
    - a credit or financial institution which is subject to requirements in national legislation;
    - implementing the 5th Directive and supervised for compliance with those requirements in accordance with the 5th Directive;
    - a company listed on a regulated market (including majority owned subsidiaries) and the location of the regulated market;
- product, service, transaction or delivery channel risk factors, including whether the product or service is one of the insurance policies, pensions or electronic money products specified in R37(3)(b); and
- geographic risk factors based on where the client is established and where it does business, for example, an EEA state or third country with effective systems to counter money laundering or terrorist financing or with documented low levels of corruption or other criminal activity.

For further details on the factors to consider when assessing whether to apply simplified due diligence, see R37.

Conversely, you should not apply SDD where the client is not:

- supervised for AML or subject to equivalent requirements outside of the UK
- listed on a regulated market;

- an independent legal professional; or
- a Public Authority, or majority owned entity of a public authority in the EEA or jurisdiction with similar levels of AML controls.

You must cease SDD and apply a higher standard of due diligence if:

- you doubt the truth of any documents submitted for identification or verification;
- any risk assessment you do identifies that it is not an instance of low risk;
- you suspect money laundering or terrorism financing; or
- there is an obligation to apply EDD under R33(1).

6.21 Ongoing Monitoring

R28(11) requires that you conduct ongoing monitoring of business relationships. Ongoing monitoring is defined as:

- scrutiny of transactions undertaken throughout the course of the relationship, (including where necessary, the source of funds), to ensure that the transactions are consistent with your knowledge of the client, their business and their risk profile; and
- undertaking reviews of existing records and keeping the documents, or information obtained for the purpose of applying CDD, up to date.

You must also be aware of obligations to keep clients' personal data updated under the Data Protection Act 1998 and the GDPR or their equivalent.

In order to comply, you may:

- renew and re-evaluate CDD at appropriate intervals (including during the course of a given transaction), noting that as outlined in R27(8), this is mandatory in certain circumstances ;
- suspend or terminate a business relationship until you have updated information or documents, though this may be excessive if you are satisfied you know who your client is, and keep under review any request you have made for information or documents; or
- use technology to aid your ongoing monitoring.

You should operate a system of regular review and renewal of CDD and take a risk-based approach to such activity. You should consider reviewing (although not necessarily redoing) the CDD upon each new matter. Where there has been a significant gap between instructions (anything above a year may be considered a significant gap in relation to those clients or transactions assessed as higher-risk), you should consider refreshing the CDD.

You must update the CDD when you become aware of any changes to the client’s identification information. This would include change of name, address, beneficial owner or business.

In accordance with R27(9) you must apply (or reapply) CDD to existing clients on a risk-based approach and when you become aware that the circumstances of the existing client have changed.

In determining this, you must consider:

- any indication that the identity of the client, or beneficial owner has changed;
- any transactions which are not reasonably consistent with your knowledge of the client;
- any change in the purpose or nature of the relationship; and
- any other matter which may affect your assessment of the money laundering or terrorist financing risk in relation to the client.

It may also be necessary to undertake ongoing monitoring through the course of a single matter – particularly where there is an element of duration to the matter, and parties to the matter, or the SoW/SoF involved may have changed.

Each time a practice engages in ongoing monitoring (which may or may not include full reverification) it should record:

- what aspects of the issue they considered;
- action taken (if any);
- the reasons for that decision; and
- who undertook the monitoring and the date on which it was undertaken?

Bear in mind also that the Regulations as amended prescribe further situations where you must re-apply CDD for existing clients – these being when a practice has any legal duty in the course of the calendar year to contact a client under the International Tax Compliance Regulations 2015 or to review information:

- relevant to their client risk assessment (or where appropriate practice-wide/matter risk assessment as appropriate); and
- concerning beneficial ownership information of the customer, including information which helps them understand the ownership or control structure of any entity that is the beneficial owner of the client.

6.22 Records

R40 requires you to keep records of your CDD, EDD and SDD documents. You must also keep information and sufficient supporting records in respect of any transaction which is the subject of any ongoing monitoring.

Please see Section 10 for information relating to record keeping and retention requirements.

6.23 Reliance and outsourcing

Reliance has a specific meaning within the Regulations and relates to the process under R39 where, in certain circumstances, you may rely on another person to conduct CDD for you, subject to their agreement.

Reliance does not necessarily mean obtaining certified copies of documentation from other regulated professionals for due diligence purposes.

You should note that you remain liable for any non-compliance with CDD requirements when you rely on another person. For this reason, you should view reliance as a risk as, if

things go wrong, it is you that will be held responsible. It may not always be appropriate to rely on another person, especially where there is a higher risk of money laundering, requiring enhanced due diligence measures.

The benefit of reliance is that in certain circumstances it may allow practices to avoid duplication in complying with their CDD obligations and facilitate a client's swift and convenient access to legal services.

You cannot rely on due diligence carried out by another party without fulfilling the qualifying conditions below.

For the avoidance of doubt, any assumption that funds are not the proceeds of crime because they have come from a UK-based bank which would have applied its own CDD, is incorrect and may be viewed as a breach of requirements by your AML supervisor.

6.23.1 Relying on a third party

In order to rely on another regulated person to apply CDD measures you must as a precondition, obtain from them all the information (though it should be noted not the underlying documentation) needed to satisfy the requirement to apply CDD measures in accordance with R28(2) to (6) and (10).

Subsequently you must:

- enter into arrangements with the other person, which
    - enable you to obtain from the other person immediately on request copies of any identification and verification data and any other relevant documentation on the identity of the client and/or its beneficial owner; and
    - require the other person to retain copies of the data and documents in accordance with R40; and
- Obtain evidence to establish that the person relied upon, falls into the category of persons who may be relied upon as per R39(3).

If you choose to rely on another professional, you should ask for written confirmation of the CDD measures and enquiries the other person has undertaken to ensure that they actually comply with the Regulations. You should also consider whether they have applied a consideration of risk and approach to mitigation similar to your own.

In practice, if you are relying on the confirmation of a third party you must obtain
- the identity of the customer or beneficial owner whose identity is being verified;
- the level of CDD that has been carried out; and
- confirmation of the third party's understanding of their obligation to make available, on request, copies of the verification data, documents or other information.

If you routinely rely on CDD checks done by a particular third party, it is good practice to request sample documents to test their reliability.

This is particularly important when relying on a person outside the UK. Before relying on a person outside the UK you should satisfy yourself that the CDD has been conducted to a

standard compatible with the 5th Directive, taking into account the ability to use sources of verification and jurisdictional specific factors.

You should be aware that the risk assessment of the person you are relying on may not match your own, and therefore commensurate due diligence/enhanced due diligence may not have been applied.

6.23.2 Granting reliance

Another relevant person may seek to rely on the CDD checks you have completed, and this will more likely be the case where you instruct such a person on behalf of your client. In such a situation you should consider whether you wish to enter into an arrangement to allow the relevant person to rely on your CDD checks, noting that it may be beneficial for your client.

Before agreeing to enter into such an arrangement, you should ensure that:

- You can make the required CDD information available immediately on request; and
- You have appropriate consent from your client to disclose the CDD information to the other party.

You may wish to consider adopting an exclusion of liability clause as part of the arrangement allowing reliance between you and the other party.

Before granting reliance, you should also consider whether, by doing so, you would be breaching a contract with another party, such as an electronic verification service provider.

6.23.3 Reliance in the UK

You can only rely on relevant persons as defined under the Regulations.

6.23.4 Reliance in an EEA state

You can only rely on a person in an EEA state if they are:

- subject to requirements in national legislation implementing the 5th money laundering directive; and
- supervised for compliance with the requirements laid down in the 5th Directive in accordance with section 2 of Chapter VI.

6.23.5 Reliance in other countries

You can rely on a person who carries on business in a third country, other than a HRTC, only if they are:

- subject to requirements in relation to CDD and record keeping equivalent to those laid down in the 5th Directive; and
- supervised for compliance with those requirements in a manner equivalent to section 2 of Chapter VI of the 5th Directive.

6.23.6 Reliance in High-risk Third Countries

You cannot rely on a third person established in a country that has been designated by the European Commission as a HRTC, unless:

- the third person is a branch or majority owned subsidiary of a person established in an EEA state who is subject to the fifth money laundering directive; and
- the branch or subsidiary complies fully with the procedures and policies established for the group under Article 45 of the 5th Directive.

Even then, you should consider whether the location of the branch or subsidiary, impacts on the risk of relying on that third person and whether it is still appropriate to rely on them. This should also be reflected in your matter risk assessment.

The list of countries designated as high risk third countries by the European Commission is here.

6.24 Transferring clients between jurisdictions ("passporting")

Many practices have branches or affiliated offices ("international offices") in other jurisdictions and will have clients who utilise the services of a number of international offices. It may not be proportionate for a client to have to provide original identification material to each international office.

Some practices may have a central international database of CDD material on clients to which they can refer. Where this is the case you should review the CDD material to be satisfied that CDD has been completed in accordance with legislation in that jurisdiction. Relevant members of the practice must have access to this information, particularly the MLRO/MLCO. If further information is required to be in full compliance, you should ensure that it is obtained and added to the central database. You should also ensure that the CDD approval controls for the database are sufficient to ensure that all CDD is compliant.

A central database of CDD may also aid international practices in compliance with all relevant, global sanctions requirements, including screening of client information.

Other practices may wish to ask their international office simply to provide a letter of confirmation that CDD requirements have been undertaken with respect to the client. This may be acceptable provided that:

- the international office is a member of the same group;
- that group applies CDD measures, rules on record keeping and programmes against money laundering and terrorist financing in accordance with the Regulations, the 5th Directive, or rules of equivalent effect;
- the effective implementation of those requirements is supervised at group level by an authority of an EEA state with responsibility for the implementation of the 4th Directive or by an equivalent authority of a third country; and
- the individual legal practitioners working on the file have access to the underlying CDD documentation and are satisfied with the documentation.

Finally, practices without a central database may wish to undertake their own CDD measures with respect to the client but ask their international office to supply copies of the

verification material, rather than the client themselves. This may not be considered reliance but may be considered outsourcing. Outsourcing is permitted under R39(7), on the condition that the arrangements with the outsourcing provider provide that you remain liable for any failure to apply CDD measures.

It is important to note that you will need to have in place a process for checking whether a person passported into your office is a PEP (or family member or known close associate) and, if so, to undertake appropriate EDD measures and enhanced ongoing monitoring.

UK-based practices will have to undertake their own ongoing monitoring of the matters they act on, even if an international office is also required to do so.

6.25 Using CDD Information in relation to sanctions measures

The UK has many different international trade sanctions against individuals and groups. These sanctions are written into law, and compliance with them is mandatory, albeit outside of the Regulations.

When CDD information held is accurate, up-to-date and reliable it will facilitate accurate screening against sanctions lists, where appropriate.

The Office of Financial Sanctions Implementation (OFSI) maintains a consolidated list of asset-freeze financial restrictions in force in the UK. Practices can access this list, register for updates and obtain further information on financial restrictions.

Please note that the US Office of Foreign Assets Control sanctions lists, and regimes are not included in this list, but may apply to your practice.

See this page for further information on obtaining a licence from HM Treasury to undertake transactions with or on behalf of persons or entities subject to financial restrictions.

6.26 Communicating with your clients about CDD

While not specifically required by the Regulations, we consider it useful for you to tell your client about your AML/CTF obligations. Clients are generally more willing to provide information when they are made aware of requirements upfront and see it as a standard requirement as part of the normal course of business.

You may wish to advise your client of:

- the legal requirement to conduct CDD.
- whether any electronic verification is to be undertaken during the CDD process.
- the legal requirement to report suspicious transactions; and
- the use and retention of their CDD information held.

Consider the manner and timing of your communications, for example whether the information will be provided in the standard client care letter.

It can be difficult to explain to clients why your practice needs the information it does in order to fulfil your responsibilities. It may be of use to point clients (particularly natural persons who may not be familiar with the requirements legal professionals are subject to) towards the

below wording in order to help explain why you need this information from them. Further information may be available on your supervisor's website.

"Legal professionals in the UK must verify who their client is when providing certain services. If they are suspicious of the underlying transaction, they have a duty to report this to the National Crime Agency.

A legal professional may also need to establish the source of funds and source of wealth of a client.

Prior knowledge that a legal professional may have of their client may not always be relied upon for these purposes and verification of these details must be established.

Failing to comply with these requirements may have serious consequences, such as a fine or imprisonment, for the legal professional."

6.27 Acquisition/Merger of Practice Units

When a practice acquires the business and customers of another practice, either as a whole, or as a portfolio, the acquiring practice should be aware of the AML risks inherent in the acquired portfolio and the strength of controls which were in place to mitigate these risks.

The acquiring practice's due diligence enquiries should include some sample testing in order to confirm that the customer identification procedures previously followed by the acquired practice have been carried out correctly, however is not necessary for the identity of all existing customers to be re-verified, provided that:

- all underlying customer records relevant for due diligence are acquired with the business; or
- a warranty is given by the acquired practice, or by the vendor where a portfolio of customers or business has been acquired, that the identities of its customers have been verified.

In the event that:

- the sample testing of the customer identification procedures previously undertaken shows that these have not been carried out to an appropriate standard;
- the procedures cannot be checked; or
- the customer records are not accessible by the acquiring practice

- verification of identity will need to be undertaken as soon as reasonably possible for all transferred customers, in line with the acquiring practice's risk-based approach.

You may wish to consider how much you can rely on any of the CDD done by the practice being acquired.

7. Technology

The practice must have clearly documented PCPs based on their practice-wide risk assessment which include:

30. Measures taken when new technology is adopted to protect against ML or TF risks
31. Where practices use electronic identification and verification (EID&V) tools they should document the role of the tool, the data sources it uses, and in what circumstances (clients/matters) it is appropriate to use the solution

7.1 Overview

There is a large range of regulatory and compliance-related technology (commonly referred to as “RegTech”) available to legal practices, to help them comply with their Anti- Money Laundering (AML) and Terrorist Financing (TF) duties.

These tools can be loosely split into three categories:

- Electronic means to help legal practices verify an individual’s identity
- Corporate Registry and Beneficial Ownership checkers
- Electronic tools to screen clients against sanctions, PEP and Adverse Media watchlists

Some of these are free to use, however many of these are services made commercially available by third parties - the market for these is both diverse and growing.

Please note that the Legal Sector Affinity Group does not endorse any one service provider, and these services may not be subject to statutory regulation.

While these tools can be helpful, they are not a guaranteed solution to AML/TF issues or risks nor a guarantee that by using them you are in compliance with the Regulations. Responsibility will always ultimately sit with the legal practice and practitioner.

7.2 Choice of Solution

The relative merits of free/open source, commercial, in-house or external systems should be understood, along with the capabilities and limits of any system ultimately chosen. The decision should be based on the complexity and risk profile of the practice and consideration should be made to tailoring the system functionality according to the risk profile of the firm. When choosing a solution, ongoing control and support should be considered along with system capability to integrate with existing systems and its ability to undertake different types of manual and automated screening.

7.3 Electronic Verification

Legal practices may wish to make use of technology, particularly electronic identification and verification (EID&V) tools in order to help fulfil their obligations under the Regulations.

Use of EID&V tools may be helpful in that they:

- can improve efficiency in customer identification and verification at on-boarding;
- allow the undertaking of checks that may be resource intensive to be done more efficiently;
- can be applied on a consistent basis from client to client; and
- can support ongoing due diligence and scrutiny of transactions throughout the course of the business relationship via automated monitoring of client/transaction features as set against red flags or risk factors.

In an increasingly digital age, it is clear that non face-to-face customer onboarding can no longer be viewed as always high risk (although it remains a key risk factor to be assessed in the context of the wider relationship) – a more nuanced approach should therefore be adopted to these types of relationships.

The use of EID&V is increasingly viewed as being as robust as traditional verification methods (physical documentary evidence such as passports, driving licenses etc.) Electronic verification methods are becoming increasingly more secure and sophisticated and may in fact be lower risk than traditional means in some circumstances. They can be used both at client on-boarding stage and as a tool for ongoing monitoring and the reapplication of CDD.

The use of EID&V is not without risk – for example with respect to cyber and data security, fraud or privacy. Benefits and risks should be understood by anyone using EID&V.

EID&V is also sensitive to human error, and mistakes of data input can lead to the incorrect individual being checked. Practices should consider the risks of this and how they mitigate, e.g., dip sampling past files to check accuracy, ideally by another individual at the practice. Practices should also be alert to any surprising results that may indicate human error at the data input stage.

It is not acceptable to simply run a search on a prospective or current client and file it as having completed the identification and verification process, without consideration of the wider risks (see Section 5). Practice units must bear in mind that identification and verification is one element of overall customer due diligence requirements necessary under the Regulations.

To comply with R28, the Regulations state that due diligence information may be regarded as obtained from an independent, reliable source when 'it is obtained by using electronic identification means' via a process that 'is secure from fraud and misuse.' The source must also be able to provide assurance that the person claiming a particular identity is in fact the person with that identity, to a degree that is necessary for effectively managing and mitigating any risks of money laundering and terrorist financing.

It should be noted that other systems, which do not fully comply with the requirements above, may be used as part of a suite of systems and controls, which in combination satisfies the requirements of R28.

A practice should be able to adequately demonstrate to its supervisor that any electronic verification system or process used, properly establishes your customer's identity, rather than just establishing that the identity exists.

This may be viewed in terms of three separate stages:

1. Identity & verification of that identity.
2. Private information or credentials that tie the person in control of those credentials to the verified identity.
3. Establishing that the verified individual has possession/control of those credentials.

A practice may mitigate inherent risk by corroborating electronic verification with some other CDD material, including private information known only to the client. Increasingly, the use of other strong evidence, such as biometric identification may be an effective way of reducing these risks.

Some electronic verification providers can offer a higher degree of comfort than others – particularly where multiple sources of data are used, and sources use robust underlying data sources, where individuals are forced to prove identity in some way. Data from one source alone is unlikely to be a strong verification method.

Firms must remain alert to (and account for) the fact that some electronic verification sources rely solely on publicly recorded and unchecked information, submitted directly by the individual or sources controlled by the individual. Where there is other information or evidence to suggest that the information obtained is inaccurate or incorrect, this must be taken into consideration in deciding whether it meets the test in the Regulations.

“Negative” information sources used by EID&V providers (such as deceased persons lists or information originating from established fraud databases) may also help a firm gain comfort in the verification of a client’s or beneficial owners’ identity by EID&V.

Firms should also ensure they are aware of, and comfortable with how often the information provided is refreshed.

Ultimately, the firm must decide whether the level of comfort derived from a particular system is adequate to mitigate the risks of ML/TF or fraud to which the business is exposed – as documented by the Practice Wide Risk Assessment.

7.4 Understanding the system used

Any practice must develop an in-depth understanding of any tools they choose to incorporate into their ML/TF risk mitigation processes. They should consider their advantages and limitations and factor these into the practice’s risk-based approach to client due diligence.

The firm should be able to demonstrate an adequate understanding of:

- Inputs to the system;
- The data sources used by the system to verify identity;
- The outputs from the system and what they mean; and
- How the system complies with relevant sections of the Regulations.

When considering whether to use a provider, a practice should:

- Understand the level of assurance of the EID&V system’s technology, architecture and governance to determine its reliability/independence;
- Make a risk-based determination of whether the particular EID&V system, given its level of assurance, provides an appropriate level of reliability and independence in light of the potential risks; and

- Consider the level of assurance you require, and whether it is appropriate to use a process for some levels of due diligence and not others.

7.5 Tiered Services

Many digital ID providers will provide a tiered service, allowing practices to subscribe to varying levels of verification which should be utilised in proportion to the level of risk presented by any given client/matter. Greater technical reliability should be employed for higher risk ML/TF situations, and conversely, lower risk ML/TF situations may permit use of systems with lower levels of assurance for the purposes of simplified due diligence.

When making this determination, you may also consider whether the provider:

- can link an applicant to both current and previous circumstances using a range of positive information sources;
- accesses negative information sources, such as databases on identity fraud and deceased persons;
- accesses live databases of politically exposed persons and individuals/entities subject to sanctions (see Section 6);
- accesses more than one relevant data source;
- has transparent processes enabling you to know what checks are carried out, the results of the checks, and how much certainty they give on the identity of the subject; and
- allows you to capture and store the information used to verify an identity.

7.6 Digital ID Certifications

FATF Guidance recommends providers of EID&V seek assurance testing and certification by the government, an approved expert body, or another internationally reputable expert body. You should ask whether the digital provider has certification or assurances like this - and the reasons why if they do not - before subscribing to their services.

In this context, an ‘assurance level’ measures the level of confidence in the reliability of an EID&V system and its components.

Examples include –

- eIDAS framework (European Union) – where compliant service providers qualify against EU-wide regulations meeting low, substantial or high ratings of assurance depending on the degree of confidence in the claimed or asserted identity of a person; and
- GOV.UK Verify – an identity assurance system has been developed by the UK government that works with different organisations to facilitate verification of an individual’s identity to a standard level of assurance. Though the UK Government does not maintain a list of approved providers, you may wish to consider if the providers are part of this scheme.

Depending on the nature of the checks undertaken, when using EID&V, you may not be required to obtain consent from your client, but they should be informed that this check will take place.

7.7 Training Considerations

Robust, ongoing training of staff is important, commensurate to their roles and responsibilities within the organisation

Staff who are responsible for conducting searches using an electronic verification system must be adequately trained to ensure the validity and accuracy of client data input, and that all necessary data is submitted in the right fields.

Staff responsible for evaluating and making decisions on sanctions, PEPs or adverse media screening outputs must be adequately trained with regards to what those outputs mean, and what further actions may be required to ensure required verifications are obtained.

Specific training should be given to employees undertaking an active role in due diligence procedures or discounting/escalating potential screening matches.

7.8 Record Keeping and Data Protection considerations

Practices should ensure that they have access to or have a process for enabling relevant authorities such as law enforcement or supervisors to obtain, the underlying identity information and evidence or digital information needed for identification and verification of individuals.

Practices should ensure the system and use of personal data by the system is compliant with all relevant regulations – including payment of the data protection fee to the UK Information Commissioners Office (ICO) in compliance with the UK data protection legislation.

The firm should ensure the system and use of personal data by the system is compliant with all relevant regulations – including registration with the ICO in compliance with the UK data protection legislation.

Other positive certifications which may give comfort include registration with an independent, international standards organisation such as the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Faster Identity Online (FIDO) Alliance, or the OpenID Foundation (OIDF) or with industry-specific organisations such as the International Telecommunications Union (ITU) or the Global System for Mobile Communications.

Access rights to the system must be rigorously controlled- and may use standards such as two-factor authentication (2FA) as a means of ensuring security.

7.9 Use of Technology to Conduct Employee Screening and Verification

EID&V tools can be used to screen employees. They can verify their claim of identity, and also check their names against PEP, sanctions and adverse media lists held by the provider. Screening of relevant employees is a requirement in R21 (depending on the size and nature of the firm) of the Regulations where practices are required to assess the ‘conduct and integrity’ of an individual both before and during their employment. See Section 9 for further information.

7.10 Company Registry Checkers & Verification of Beneficial Ownership of non-natural persons

Open-source (free) and commercially available databases can also be useful for conducting due diligence on non-natural persons or legal entities. These can be helpful particularly when establishing background, business type, structure, and control and ownership of legal entities both domestically and overseas.

Issues to consider when using Company Registry Checkers:

- Reports from such services are generally compiled using data submitted by the company itself to national corporate registries. They should therefore be used in conjunction with other sources of evidence in order to build a picture of ownership and control. Due diligence should include checking information that is independent from the entity itself – for example independently audited or certified documents such as passports, financial statements or corporate annual reports. Practices must therefore make a risk-based determination of the reliability and independence of the system/tool – in light of the ML/TF risks inherent in the client/transaction;
- The depth and structure of information available is often limited by the nature and public availability of the underlying corporate registries. Thus, it may not provide a complete picture of control, ownership or other features of the legal entity in question – particularly where company structure or ownership lies in or passes through jurisdictions where data is not held or made publicly available; and
- Practices should also ensure they are aware and comfortable with the timing of data refreshes in such systems (how often and when the data is renewed or refreshed) along with whether the data has been obtained direct from source or through an intermediary/3rd party. Practices should always check the date stamp of due diligence assembled and consult providers for relevant assurances.

7.11 Initial and Ongoing Sanctions/PEP/Adverse Media Screening

7.11.1 Senior Management Responsibility

Responsibility and accountability for any screening measures deployed should be established at senior management level. These responsibilities should be documented.

7.11.2 Risk Assessment

Practices should take a risk-based approach to sanctions, PEPs and adverse media screening.

Decisions made in respect of the nature, depth and level of screening tools and systems deployed should include consideration of the size and nature of the practice unit.

Small firms, with limited exposure and lower risk profiles may deploy open source, free or off the shelf sanctions, PEP and adverse media screening tools and solutions. Those practices with higher exposure or risk profiles should consider more complex, comprehensive or bespoke solutions.

Furthermore, screening may not be necessarily appropriate for all client types, products and services offered. Screening should therefore be considered in areas where it will be most useful and effective. As the sanctions regime is absolute, practices should ensure there are

other appropriate measures in place to ensure they do not undertake unauthorised business with sanctions targets in areas of less risk. This may include open-sourced searches.

Risk factors in determining what type of screening should be conducted may include:

- Jurisdictional risk – e.g., the geographic location of the practice's operations or where employees/customers are located or operate;
- Client, Product and Activity Profile – i.e., the risks the practice is exposed to given the products & services it offers, or the clients or sectors it transacts with. This could extend to risks associated with its supply chain, its employees, associated parties or intermediaries; and
- Factors relating to distribution channels, operating environment, complexity and volume of business should also be considered along with business strategy - for example, any risk the firm becomes exposed to after merger and acquisition activity.

7.11.3 Screening Policy & Procedures

Sanctions, PEP and adverse media screening cannot stand in isolation and governance frameworks should be applied in conjunction with other financial crime control processes. Screening effectiveness is conditional on the reliability and accuracy of the data input. The reliability and accuracy of the data input is in turn conditional on the quality of due diligence undertaken. Therefore, screening systems and controls should fit into a wider, holistic approach to financial crime risk mitigation, where interfaces and interdependencies between policies, procedures and controls are considered. One key example of this is how the accurate collection and verification of CDD is critical in effective screening.

These should be established and informed by the firm's legal requirements and risk exposure and made readily accessible to all relevant staff.

Where a firm is multi-jurisdictional, consideration should be made to the application of a business-wide policy, therefore assisting the application of minimum group standards at a local country level.

Practices should further document what datasets must be screened (e.g., clients, counter parties to a matter, beneficial owners, directors of corporate clients) and the frequency and timing of screening (at onboarding and as part of ongoing monitoring) - along with roles, responsibilities, escalation routes and sign-offs.

Where appropriate, procedures should cover operational data, technology & screening considerations such as the maintenance, age and management of data and lists used, the functionality and administration of systems, and management of alerts generated.

Policy/procedures should be reviewed periodically in order to ensure any changes across the business are reflected (e.g., new CDD/EID&V collection processes) new legislation is considered, and developing risks are mitigated.

7.12 Specific Screening System Considerations

7.12.1 Considerations at Pre-screening Stage

The accuracy and completeness of data input into screening tools is crucial. Consideration should therefore be given to ensuring data is sent/received accurately from other systems and mechanisms for cleansing data where necessary before input, are robust. Any data used must also be sorted correctly to ensure that relevant attributes are used in the process.

Pre-screening procedures should include measures to prevent the intentional tampering of data or manual circumvention entered into the screening tool.

7.12.2 Considerations during Screening

When using a commercial screening provider, a practice must be aware of how the screening is being conducted, against which lists and what filters/rules are being used to generate or limit the number of alerts.

Any system or screening tool implemented should also have the capability to “fuzzy match” – i.e., the ability to screen and identify names and other datasets with minor alterations such as reverse order, partial text and abbreviations. It should also be able to recognise non-Latin scripts, such as Chinese characters or commercial code data. Matching should be customizable to ensure minimisation of false positives.

Importantly, systems must produce relevant management information (MI) and performance reporting metrics along with all necessary information to allow decision-making and investigation at post screening stage.

7.12.3 Considerations Post-screening

Considerations must include the efficient prioritisation and management of potential matches and false positives, and the escalation and investigation of potential matches by suitably trained and skilled staff.

Procedures and controls for blocking client business or transactions must be developed should confirmed sanctions matches be found, along with procedures to escalate and report to relevant authorities.

Procedures for escalation of PEP matches for senior management approval should also be introduced.

Management Information regarding investigation outcomes must be available to enable senior management decision-making, determine screening effectiveness and to satisfy regulatory requirements.

7.12.4 Review of screening processes

Regular review of screening processes should be undertaken where appropriate. Screening frameworks such as policies, risk assessment, training and investigation/escalation processes should be tested, along with data integrity and the screening functionality itself.

7.13 New Technologies relevant to AML Control in Legal Practices

For larger, more complex practice units, new technologies such as biometrics, machine learning or the use of artificial intelligence may be considered as part of an overall AML control environment. In addition to overarching considerations described in the preceding guidance, consideration should be given to the below factors.

The use of biometric indicators such as facial recognition software as part of an overall identity verification process is now widely used across various industries, and may be considered proven technology, helpful in meeting a practice's AML obligations, especially in non-face to face situations, remote client take-on situations. Where used, consideration must always be given to the use and storage of such data, where collected, stored and retained

The use of machine learning and artificial intelligence may be helpful in some high-volume businesses, particularly in regard to reducing numbers of false positive screening PEP/sanctions/AM matches or discounting potential matches which have arisen. Where a practice considers the use of technology as useful and viable in the context of their business, careful consideration must be given to the timeliness, quality and accuracy of data used within the system, in order to ensure the validity of output – along with the filters/settings used by the system deployed to identify potential matches. Machine learning by its very nature learns from historic data and outcomes, and therefore may have limited use in predicting future outcomes. This is particularly important to consider where the outputs of automated systems may create a risk of discrimination against prospective clients based on protected characteristics or any other access to justice issues. You may consider it appropriate to undertake an equality impact assessment in order to examine any such issues in depth.

8. Training

Compliance Principles:

The practice must have clearly documented PCPs based on their practice-wide risk assessment which include:

32. Measures deployed to ensure AML relevant training of partners, staff and agents, including the maintenance of records relating to such training. This training must include awareness of MLR, POCA Part 7 and Terrorism Act Part 3 reporting requirements, legal professional privilege and data protection requirements. Training should also cover recognition of red flags/risk indicators as relevant to their duties and responsibilities, along with other relevant laws.
33. Procedures for the communication of PCPs to partners and staff

8.1 General Introduction

Your staff members and others that provide services to your customers are your most effective defence against your firm becoming inadvertently involved in money laundering or terrorist financing. Providing them with adequate training, in order to equip them with appropriate AML awareness, skills and knowledge is a key part of your AML controls, and an important way to mitigate the risks your practice faces.

R24(1)(a) requires that you take appropriate measures to ensure partners, relevant employees and any agents you use for the purposes of your regulated business:

- Are made aware of the law relating to money laundering, terrorist financing and the requirements of data protection which are relevant to the implementation of the Regulations
- Are regularly provided with training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing, and
- Can identify and report suspicions of money laundering or terrorist financing (see Section 11).

In deciding what measures are appropriate you should consider the size and nature of the business and the areas of risk identified in, and outcomes of your Practice-Wide Risk Assessment (PWRA).

You should also consider questions relevant to any other form of training including:

- How to assess the success of training, both in terms of information retention and whether training is reflected in the practices of individuals.
- How and when to review and update training.
- What the triggers for an individual redoing training are; and
- What content should there be widespread training on and where are there specialised needs.

A practice should set the answers to these questions out in a written training policy, which should be reviewed and updated as needed.

Sole Practitioners must ensure that they are trained in appropriate areas in order to adequately protect their practice from money laundering risks and should record all relevant training undertaken.

8.2 Who should be trained?

The Regulations require that all relevant employees and agents you use are trained. A relevant employee or agent for the purpose of training is someone whose work is:

- relevant to the business' compliance with the Regulations; or
- capable of contributing to the identification or mitigation of the risks faced by the business, or the prevention or detection of money laundering and terrorist financing.

You may decide to treat all employees as relevant employees which will bring the added benefit of allowing more fluid internal transfers of staff across roles and work area. Support staff (such as those who deal with clients, handle client money or otherwise assist with compliance) have an important role in identifying AML red flags. Again, training should be appropriate for each post holder and business area, and relevant to the risks they are likely to come across.

You may decide that, for example, those members of staff who undertake cleaning, maintenance of offices or catering do not require training.

Staff or agents who undertake work relating to documents and electronic information, such as Information Technology and records staff, should be made aware of the law relating to data protection, as it relates to money laundering, as required under R24(1)(a).

8.2.1 Training for MLROs and MLCOs

While there is no explicit requirement in the Regulations for MLROs or MLCOs to receive training beyond that which should be widespread in a practice (as per R24), a practice should consider whether it is appropriate for MLROs/MLCOs to complete extra training or relevant professional AML-related qualifications in order to competently carry out their duties.

Particularly with regards MLROs, particular attention should be paid to the technical requirements of making disclosures to the NCA including any and all guidance they issue on submissions.

The MLCO and MLRO should both monitor publicly available information on best practice such as thematic reviews by their supervisors and reports relating to enforcement actions.

8.2.2 Agents

The Regulations include agents as being subject to the requirements on training, but the term agent is undefined.

Our interpretation is that the intent of this is to ensure that a lack of a straightforward or traditional employer-employee relationship does not automatically mean the individual is exempt from the training requirements. If an individual works in the manner of an employee,

albeit under a different relationship (e.g., independent contractor) then you should treat them as an employee for training purposes.

In law, an agent is a person who is authorised to act for you as principal through employment, by contract or apparent authority. The agent can bind the principal by contract or create liability if he/she causes loss or injury while acting within the scope of the agency.

Therefore, your agents may include consultants, other law firms you instruct and temporary contract lawyers working in your firm. However, if the agent is also a relevant person within the meaning of the Regulations then, taking a proportionate and risk-based approach, it may be sufficient to check with them that they have undertaken the relevant training themselves and retain a record of this check. You should also include a term to this effect in your agreement with the agent.

There is a distinction between an agent and someone with whom you merely have a contract for services, such as a stationery supplier or external caterer. The level of control you exercise over the person is important, if they have less discretion in how to undertake their role, they are more likely to be an agent. If an individual works in the manner of an employee in your firm, albeit under a different relationship (e.g., under temporary contract) then you should treat them as an employee for training purposes. See further guidance below:

An Agent

- acts under your supervision and control;
- is bound by your instructions; and
- can bind you by his/her act.

A Service Provider

- uses their own equipment and materials;
- is bound by the terms of the contract with you; and
- cannot bind you.

Ultimately it is for a practice to ensure that anyone that may fall into the bracket of employee or agent, has the required training.

8.3 What should be included in training?

Your AML/CTF training programme should enable employees and agents to identify and detect when risk indicators are present and relevant changes in client activity by reference to risk-based criteria. The training should include:

- an explanation of the relevant law within the context of the services and products your practice supplies.
- AML/CTF ‘red flags’, risk assessment and an explanation of the risks identified in your PWRA.
- AML/CTF policies, controls, and procedures, including CDD and EDD as applied in your practice.
- Identifying suspicious activity and the processes for internal reporting, and where necessary for making a SAR; and
- Record Keeping and Data protection requirements.

It is important to tailor training to the specific roles and responsibilities of relevant staff and the AML risks of your practice – as identified in your PWRA. It is best practice for all relevant employees to receive some level of AML training.

Training should be targeted so that relevant employees and agents understand the risks posed by the services they provide and the types of clients they deal with. This is particularly important for those dealing with higher risk clients or undertaking higher risk work.

In addition, you may consider providing relevant employees and agents involved in the client identification and verification process with training and equipment to help identify forged documents or refer them to the guidance provided by the UK Home Office. Other examples may include training in red flags and risk indicators for those involved in the risk assessment process.

8.4 What might be considered as training?

Training may include:

- in-house or external training seminars or real-time webinars by persons suitably qualified and experienced in AML matters. Pre-recorded webinars may also be useful in certain circumstances or across certain topics.
- completion of AML-specific online training sessions.
- attendance at AML/CTF conferences, peer learning and similar events (e.g., roundtables) While these can be extremely useful, mere attendance at AML/CTF conferences is not likely, in itself, to satisfy training requirements under R24;
- review of publications on current/relevant AML/CTF issues.
- review of training materials prepared by the firm.
- review of relevant website materials and documents published by AML Supervisory authorities, FATF, law enforcement, government.
- completion of recognised industry AML training qualifications; or
- review of internal communications to relevant employees explaining internal processes and controls (e.g., the PCPs and/or the PWRA) and/or changes to the regulatory environment.

The MLRO/MLCO of your practice is responsible for the content, roll-out and completion of AML training across the practice and ensuring that relevant employees and agents complete it.

You should consider how to assess training outcomes, so that the MLRO/MLCO/Senior Management can be reasonably confident of the adequacy of that training, and that key messages in relation to regulatory requirements and the policies, controls and procedures of the practice have been delivered effectively.

8.5 Timing of Training

New relevant employees and agents should be trained as soon as possible after they join, ideally as part of their induction process and before undertaking any regulated work.

All employees and agents should receive training at regular and appropriate internals both to update on new developments and to refresh existing knowledge.

You should take a risk-based approach to determining how often specific, role-based AML training should take place, although some form of high-level basic AML awareness/refresher training should be taken annually across all relevant employees. The form this takes will vary, including such examples as listed under 8.4.

The frequency and depth of AML training over and above this should be based on:

- any changes in legislation, regulation or professional guidance.
- changes in your practice's policies, controls and procedures; and
- changes in your practice's risk profile or potential red flags.

Frequency and depth of specific AML training should be guided by the level and types of risks as documented in the PWRA.

In addition, practices should be aware of internal staff transfers. Where staff roles or responsibilities change, their training needs may change. This should be considered and addressed by the practice as soon as possible after a member of staff has moved internally.

8.6 Training Records

You must keep a comprehensive written record of all training undertaken at the practice including:

- Training documentation (presentations, notes, hand-outs, copies of online content etc.).
- Attendance records.
- Dates of training; and
- The results of any assessments carried out.

This information must be made available to your supervisor, upon request.

9. Internal Controls

Compliance Principles

Where appropriate to the size and nature of the practice:

3. a member of the board (or equivalent) or of senior management must be appointed to be responsible for compliance of the practice with the Regulations. This position is referred to as the Money Laundering Compliance Officer (MLCO). The practice must notify its supervisory authority of this appointment within 14 days of the date of the appointment

34. The practice must conduct an independent audit of the adequacy and effectiveness of its AML policies, controls and procedures
35. The practice must undertake screening of relevant employees – both at pre-employment stage and on an ongoing basis

9.1 General Overview

Regulation 21(1) sets out three internal controls which practices are required to adopt where it is appropriate "with regard to the size and nature of its business". These controls are designed to help businesses that may be larger or more complex than others, by ensuring that there are ways to ensure risks introduced by a practice's size and/or complexity can be recognised and mitigated. It also will apply to practices engaged in higher risk services as assessed in their PWRA.

Not all practices are expected to adopt these measures, though if you consider that you do not need to adopt these, you should record your reasoning as to why. You may have to justify to your supervisor how and why you do not meet this requirement, considering how your firm will not benefit from the extra protections that these measures might provide.

You do not need to implement these internal controls if you do not employ or act in association with any other person (R21(6)) e.g., if you are a sole practitioner who does not employ any staff nor use any agents.

Factors you may consider when determining whether it is appropriate to apply the controls include:

- The risks documented within, and the outcomes of, your Practice-Wide Risk Assessment (PWRA) – including client-base, geographic factors, services provided and distribution channels. Please see Section 5 for further information);
- The number of partners or staff your practice has;
- The number of offices your practice has and where they are located (including whether your practice has overseas offices);
- Your client demographic, including where they are based, and services provided to them;
- The risk-profile, nature and complexity of work your practice undertakes;
- The volume and value of the work the practice undertakes; or
- The level of visibility and control that senior management has over operational client matters – this may be considered in light of layers of management hierarchy.

9.2 Appointing an individual as the officer responsible for the practice's compliance with the Regulations

Please see Section 4 for guidance relating to the appointment of a Money Laundering Compliance Officer.

9.3 Establishing an independent audit function

The purpose of an independent audit function is to examine, evaluate and make recommendations regarding the adequacy and effectiveness of the practice's anti-money laundering and counter-terrorist financing policies, controls, and procedures (PCPs). Independent audit should not be confused with requirements under R19(3)(e) – the ongoing monitoring and management of compliance with policies, controls and procedures.

9.3.1 Internal or external auditor?

The person/s conducting the audit may not necessarily be external to the practice but must be independent of the function being reviewed.

They should:

- Be independent of the work areas being audited e.g. not the MLRO/MLCO, members of the compliance team or the team that did the original work;
- Have the requisite skills and knowledge in audit and AML/TF in order to be able to adequately carry out their duties.
- Have the authority to access all relevant material (including file materials) to be able to evaluate and report on the adequacy and effectiveness of the PCPs.
- Make recommendations about the PCPs and file remediation if required (in applying these changes, file remediation should retain records of the file pre- and post-the remediation work);
- Monitor the practice's implementation of those recommendations.
- Have direct access/report findings directly to the practice's Senior Management; and
- Where audit is conducted by an internal partner/member of staff, they must be prepared to make an internal report to the MLRO should they have knowledge/reasonable suspicion that a matter has involved the Proceeds of Crime.

Where a practice seeks the services of an external auditor/consultant – they should be satisfied regarding the specific AML/financial crime knowledge, skillset and experience of that person/organisation, to ensure the adequacy and effectiveness of the audit undertaken

Sampling of client/matter files should be undertaken on a risk-based approach - in accordance with the risks identified, and the outcomes of, the PWRA. Sample sizes must be sufficient to demonstrate effective assurance of the practice's PCPs, across all locations, client/matter types.

9.3.2 How often should an independent audit be conducted?

You should take a risk-based approach to determining the frequency of an independent audit. It may be appropriate to undertake audits at regular intervals, e.g., annually. You should consider whether an audit is required based on the time elapsed and the changes to the practice's risk profile, structure and services provided since the last audit.

This is particularly relevant should a practice take-over or merge with another business.

For those areas/clients or matters which pose the highest risks (as per your risk assessments) you should consider undertaking a targeted audit of these areas, on a more frequent basis than the wider practice.

Practices should keep a record of all audits and make this available to their supervisors as requested – this should include

- The scope of the audit and sampling basis used.
- The records audited, what was checked and by whom.
- The findings and recommended actions of the audit.
- Records of senior management/Board discussions regarding the findings of the audit; and
- The practice's response and implementation of actions (and any reasoning for not implementing those recommendations.

9.4 Screening relevant employees prior to, and during their employment

On appointment	**Skills, knowledge and expertise**	• Qualification checks (seeing original certificates or verified copies) particularly in relation to AML/risk management • Test of knowledge/skills as pertaining to role, particularly in relation to AML/risk management • Validating practising status via the relevant register applicable regulator.
	Conduct and integrity	• Taking up references. • Checking criminal history via Disclosure and Barring Service, Disclosure Scotland, Access Northern Ireland or equivalent • Finance or credit check • Checking disciplinary history via their regulator. • Adverse media checks via search engines. • E-verification, if available.
During employment (annually)	**Skills, knowledge and expertise**	• Annual competence declaration. • Appraisal procedure with recorded outcome recorded. • Review of any AML related training or qualifications undertaken through the course of the preceding year.
	Conduct and integrity	• Adverse checks via search engines. • Checking disciplinary history via the relevant register applicable regulator. • Electronic identification and verification, if available.

The above is not an exhaustive or definitive list and a practice should consider what screening checks are appropriate for them. Checks must be in relation and relevant to the individual's ability to carry out their functions effectively and in compliance with firm's obligations under the Regulations. All checks that may be done on appointment may be appropriate to recheck during employment on a risk sensitive basis.

Practices should be aware that relevant employees will include the MLRO/Nominated Officer and specialist compliance staff – but may also extend to other partners/staff responsible for risk assessments, client due diligence or other AML related controls.

Screening must be carried out both before the appointment is made and during the course of the appointment.

The screening and the amount of verification of information provided should be proportionate to the individual’s role in the business, and the level of independent authority and decision-making involved in the role.

A 'relevant employee’ in the context of screening is someone whose work is relevant to your practice's compliance with the Regulations or who is otherwise capable of contributing to:

- the identification or mitigation of money laundering and terrorist financing risks to which your practice is subject, or
- the prevention and detection of money laundering and terrorist financing in relation to your practice.

An inclusive approach should be adopted to screening, as it will provide assurance that staff of a practice can adequately perform their duties and thus help a practice protect itself. This should also provide the benefit of allowing a practice to more fluidly transfer staff internally.

As in other matters, practices should ensure that any information collected for the purposes of screening, are held securely and in line with data protection legislation.

10. Record Keeping & Data Protection

Compliance Principles

Universal - applies across all Compliance Principles

10.1 General Comments

All practices (including sole practitioners) must be able to demonstrate to their supervisor that they have adopted a risk-based approach to the management of AML/TF risk within their businesses. In practice this means retaining documents and records to demonstrate this. Retaining accurate and comprehensive records is also important for facilitating cooperation with law enforcement and potentially defending yourself against criminal prosecution.

While many aspects of the Regulations are about protecting your practice from being used for money laundering, the primary intent of this section is to help you to protect your practice against action from your supervisors or law enforcement.

If in doubt, write it down.

In trying to apply a risk-based approach, it may occasionally be unclear as to what the correct course of action is. In such cases, you should always record the issues you considered in arriving at a decision.

This section outlines these documents and sets out the specific conditions for their retention.

Beyond the specific documents mentioned, you should retain records of anything that can help you demonstrate compliance with the Regulations to your supervisor. This may include recording any comments or considerations which have been made while considering and completing these documents.

These requirements should be integrated with the general data protection procedures of your practice and not run contrary to them. This includes any data-sharing agreement you may have with other practices.

This section also considers data protection legislation, but for more detailed information on data protections see this guidance on the requirements of GDPR.

Practices must have clearly documented policies, controls and procedures (PCPs) which include procedures relating to record keeping and related data protection requirements.

Risk Assessments
Customer Due Diligence and Enhanced Due Diligence
Policies, Controls and Procedures
Training
Internal Controls
Record Keeping
Reliance
Data Protection

Areas of focus for record keeping in PCPs

10.2 Record keeping policy

Regulation 19 (PCPs) requires you to maintain, in writing, PCPs to mitigate ML/TF risks.

You must regularly review these PCPs and maintain a record in writing of:

- any changes made as a result of the review; and
- the steps taken to communicate those PCPs, or any changes to them, within the practice.

These PCPs must address reliance and record keeping.

If the practice already has a data protection/retention policy, you must ensure that it complies with these requirements.

10.3 CDD Records

Regulation 40(2) requires you to keep the following in relation to CDD:

- a copy of any documents and information obtained by the relevant person to satisfy the requirements in R28, R29 and R33 to R37 (CDD/EDD/SDD);
- sufficient supporting records (the original documents or copies) in respect of a transaction (whether or not it is an occasional transaction) which is the subject of CDD or ongoing monitoring to enable the transaction to be reconstructed.

The records that you must keep include those relating to:

- identity verification;
- Client/matter risk assessments;
- ongoing monitoring of the business relationship;
- enhanced due diligence measures; and
- additional information for Politically Exposed Persons: approval from senior management, enhanced due diligence undertaken (including source of wealth checks) and enhanced monitoring.

Depending on the size and sophistication of your practice's record storage procedures, you may wish to:

- scan CDD materials and hold it electronically with a statement that the original has been seen;
- take photocopies of CDD material and hold it in hard copy with a statement that the original has been seen;
- accept certified copies of CDD material and hold them in hard copy; and
- keep electronic or hard copies of the results of any electronic identity or verification checks or screening undertaken

R28(16) requires you to be able to demonstrate to your supervisory authority that the extent of the measures that you have taken to satisfy requirements under this regulation are appropriate in view of the risks of money laundering and terrorist financing. Keeping appropriate records of your decisions, at the time that CDD was conducted, will help you to demonstrate that you have applied a risk-based approach in a reasonable and proportionate manner.

Consistency of record keeping is particularly important in areas that produce higher volumes of information, such as client and matter risk assessments and CDD/EDD. Consistency in these areas ensure that your practice can find and readily interpret information when required.

You should also consider the requirements of other applicable regulators, particularly in relation to cross border transactions and working in areas which may be subject to oversight by overseas regulators.

10.4 Retention period for CDD records (R40)

You must retain the records for five years beginning on the date on which you know, or have reasonable grounds to believe:

(a) that an occasional transaction is complete; or
(b) that the business relationship has come to an end for records relating to:
  (i) any transaction which occurs as part of a business relationship, or
  (ii) CDD measures taken in connection with that relationship.

You are not required to retain the records relating to a transaction which occurred as part of a business relationship for more than 10 years.

On expiry of this period, you must delete any personal data, unless:

- you are required to retain it by another enactment or rule made by your regulator;
- you are required to retain the data for the purposes of any court proceedings; or
- you have reasonable grounds for believing that the records containing personal data that needs to be retained for the purposes of legal proceedings.

Many practices will wish to retain the complete file of papers, including CDD records, for a period exceeding the five years specified in Regulation 40(3). For example, your practice’s retention policy may specify longer retention times to take account of the expiry of limitation periods for potential negligence actions against the practice. If there is any variation on the period prescribed in R40(3), the client’s consent must be obtained. This consent clause may

be contained in your engagement letter or terms of business and should be signed or otherwise acknowledged by the client.

10.5 Sharing CDD information with other parts of a group

R20(1)(b) requires you to maintain PCPs for data protection on sharing of information within a group about customers, customer accounts and transactions. The use of CDD information held by other parts of the same organisation is permissible. Where one part/branch/subsidiary of the same UK organisation seeks to use CDD held by another part, this should be clearly documented and recorded on file, and the underlying information must be readily and easily accessible by the part of the organisation seeking to rely on it.

Where one part of the organisation ceases to have a relationship with a client, CDD information should be kept and transferred to any other part of the business which continues that relationship.

Where CDD information is held by the practice in other jurisdictions, and the UK branch/practice seeks to use this information, care should be taken by the UK branch/practice that information held meets the necessary requirements under the Regulations. No foreign data protection limitations should hinder access to this information by the UK practice, or by UK law enforcement agencies upon valid request. Should such limitations be in place, the UK branch/practice cannot use this information and should themselves conduct appropriate CDD.

Where the practice undertakes multiple transactions for a specific client, you do not need to keep duplicate CDD records in each file. You can hold information in a central file. This approach may help to ensure:

- Accuracy and consistency of CDD information about each client;
- Ease of record deletion in line with your retention policy;
- Ease of reference and accessibility for MLCO/MLRO or other partners/members of staff who may need to use the information in the course of business; and
- Ease of reference and accessibility of information in respect of law enforcement or supervisory enquiries.

10.6 Reliance

R40(6) says that where another relevant person relies on you under R39 for the completion of CDD measures, you must keep the relevant documents as specified in R40(3) and (4) and immediately make available information and documents set out in R40(7) to (9).

Reliance is covered further in Section 6.

10.7 Other records that you must keep

10.7.1 Risk Assessments

R18(4) requires you to keep an up-to-date record in writing of all the steps you have taken to identify and assess the risks of money laundering and terrorist financing which your practice is subject to. This is the case for your Practice Wide Risk Assessment and any client or matter risk assessments you undertake unless your supervisory authority notifies you in writing that such a record is not required.

Under R28(12) the way in which you comply with CDD requirements must reflect your assessment of the level of risk arising in a particular case and your practice-wide risk assessment under R18. Therefore, under R28(16) you must be able to provide the risk assessment, the information on which that risk assessment was based and your records to your supervisory authority on request.

You should also retain dated records of firm wide risk assessments and policies, procedures and controls, both to be able to understand the development of your compliance approach and to be able to evidence this to your supervisor.

10.7.2 PCPs

R19, R21 and R24 require you to maintain, in addition to a record keeping policy, a record in writing of PCPs relating to:

- risk management practices;
- internal controls (including screening of employees, disclosures to the nominated officer and independent audits);
- CDD;
- reliance;
- screening of relevant employees. (appropriate to the size and nature of your practice)
- the monitoring and management of compliance with PCPs (e.g., records of MLRO reports to senior management and records of any deliberations/discussions/actions undertaken); and
- AML training.

10.7.3 Disclosures to the MLRO

You should keep comprehensive records of suspicions and disclosures because disclosure of a suspicious activity is a defence to criminal proceedings. Such records may include notes of:

- concerns raised by staff;
- ongoing monitoring undertaken;
- discussions with the MLRO regarding concerns;
- advice sought and received regarding concerns;
- copies of any disclosures made;
- conversations with the NCA, law enforcement agencies, insurers and supervisory authorities regarding disclosures made;
- why the concerns did not amount to a suspicion and a disclosure was not made to the MLRO; or
- decisions not to make a report to the NCA, which may be important for the MLRO to justify his or her position to law enforcement agencies.

You should ensure these are held securely and you should avoid retaining them on the client and/or matter file in such a way that they are freely accessible.

10.8 Other Considerations

If the practice undertakes internal re-organisation, or is involved in acquisition, mergers or divestments, it is important that all records remain easily retrievable and accessible, both during and after such structural changes.

10.9 Security

There is a balance to be struck between ensuring your practice handles data responsibly while meeting the requirements in the Regulations and ensuring those that need access to information, can have it.

You should ensure that records are held securely to avoid being inappropriately disclosed to a client or anyone else, and to avoid possible offences of tipping off or prejudicing an investigation. This may be achieved by maintaining controlled access to information to those that need it to meet their responsibilities. For example, if files are held electronically, you may use appropriate passwords and limited access rights in order to limit who has access to information.

10.10 Data protection

Under **R41(1)**, any personal data that you obtain for the purposes of the Regulations may only be processed for the purposes of preventing money laundering or terrorist financing.

The Data Protection Act 2018 applies to you. It allows clients or others to make subject access requests for data held by you. Such requests could cover any disclosures made.

Each subject access request must be considered on its own merits in determining whether, in a particular case, the disclosure of a suspicion report is likely to prejudice an investigation and, consequently, constitute a tipping-off offence. Schedule 2, part 1, sub-section 2 of the Data Protection Act 2018 states that you do not need to provide personal data where disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders. This ‘crime and taxation’ exception would apply where granting access would amount to tipping off. This may extend to suspicions that have only been reported internally within the practice.

Prior to the Data Protection Act 2018, this crime and taxation exception was contained within section 29 of the Data Protection Act 1998. The Information Commissioner issued guidance on section 29 exceptions but, at the time of publishing this guidance, has not updated the guidance since the Data Protection Act 2018 became law. There is a statement on the ICO website stating that the Information Commissioner considers this guidance, as well as others, to still be useful.

If you decide that the crime and taxation exception applies, you should document the steps you took to make this assessment in order to respond to any enquiries by the Information Commissioner. In determining whether the exception applies, it is legitimate to take account of the fact that although the disclosure does not provide clear evidence of criminal conduct, when viewed in isolation, it might ultimately form part of a larger jigsaw of evidence in relation to a particular crime.

Under R41(3**)** you cannot use personal information which you obtain for the purposes of complying with the Regulations for any other purpose unless you are authorised to do so under another piece of legislation, or you have the person's consent. Any consent given needs to be easily rescindable by the person and you should highlight this to the person in question including explaining how they would contact you to withdraw consent.

In addition, you are required to provide new clients with the information specified in section 44 of the Data Protection Act 2018 and a statement that any personal data received from the

client will only be processed for the purposes of preventing money laundering or terrorist financing and any other purposes to which they have consented.

You should consider whether your practice should seek specialist advice in order to comply with your data protection responsibilities.

11. Suspicious Activity Reporting

Compliance principles

29. The practice must have procedures setting out how, and in what circumstances an internal disclosure should be submitted to the Nominated Officer (MLRO)

11.1 General comments

The suspicious activity reporting (SAR) regime for money laundering and terrorist financing is administered by the United Kingdom Financial Intelligence Unit (UKFIU) which sits within the National Crime Agency (NCA). The NCA is a law enforcement body which networks with other law enforcement agencies and is responsible for dealing with serious and organised crime within the UK. The UKFIU receives, processes and, where necessary, triages SARs within law enforcement.

The intelligence that law enforcement receives from SARs is vital to tackling crime and to gaining an insight into current and emerging threats to the UK. Legal practices have a key role in providing quality intelligence where they come across suspicious activity.

The SARs regime should not be used defensively, for example to get permission to continue with a transaction where you have been unable to complete CDD but should instead be used to provide quality information that can prevent and disrupt criminal activities.

11.2 Application

All persons within the regulated sector have obligations under POCA and the Terrorism Act 2000 (TACT), to make disclosures of suspicions of money laundering, terrorist financing and terrorist property offences. Money Laundering Reporting Officers (MLROs) have specific additional obligations. Any individual working within the regulated sector must make an internal disclosure to their MLRO if they know or suspect or have reason to know or suspect money laundering or terrorist financing is taking place.

In addition, any person outside the regulated sector may make a SAR about suspected money laundering or terrorist financing.

Everyone should consider whether the client or the practice is at risk of having committed any of the principal offences under sections 327 to 329 of POCA and sections 15-18 of TACT. The duty to report suspicions via a SAR to the NCA are important, but practices should always be vigilant against committing all relevant POCA offences.

11.3 What is a SAR?

A SAR is the name given to a disclosure to the NCA under either POCA or the Terrorism Act.

11.4 Internal processes for identifying and reporting suspicious activity

Practices in the regulated sector must appoint a MLRO. If you are a sole practitioner, you are the MLRO by default. Upon appointing an MLRO, you must inform your supervisory authority within 14 days. See Section 4 for guidance as to the selection and responsibilities of the MLRO.

You should have a process for staff to make the MLRO aware if they have knowledge or a suspicion of money laundering. You may find it helpful to have a standard internal disclosure form for employees to use to notify the MLRO if they come across suspicious activity. As the MLRO, you should consider the information provided, ask further questions if necessary and consider whether you have a knowledge or suspicion of money laundering or terrorist financing that would, subject to privilege, require a SAR to be submitted.

11.5 When to submit a SAR

You must submit a SAR:

- if you know, suspect or have reasonable grounds for knowing or suspecting money laundering or terrorist financing where that information has come to you from work in the regulated sector (subject to privilege); or
- if you are proposing to engage in a prohibited act under sections 327 to 329 of POCA and require a defence against money laundering.

You must submit the SAR as soon as is practical after you have formed this knowledge or suspicion.

You should also consider whether there may be a case of attempted fraud. Subject to privilege and confidentiality, if you find a clear case of fraud you should alert Action Fraud.

Further guidance on what constitutes suspicion and more detail on the relevant offences is set out in Sections 16 and 17.

11.6 Other notifications

If the SAR is in relation to an internal breach you may also have a requirement to report to your supervisor where you may have breached your regulatory requirements. You should check with your supervisor whether you have an obligation to notify them where you have formed a knowledge or suspicion of money laundering or terrorist financing involving your practice or another regulated practice.

11.7 If you decide not to submit a SAR

If the MLRO decides not to submit a SAR after receiving an internal disclosure, for example because the information does not meet the threshold for suspicion, your MLRO should make sure that they have documented the reasons for their decision and keep records of this along with the original internal disclosure. This will help you demonstrate compliance with

your obligations or could help you to submit a SAR further down the line if you do develop a suspicion.

11.8 How to submit a SAR

11.8.1 SARs online

You should use SARs online wherever possible. This securely encrypted system provided by the NCA allows you to:

- register your practice and relevant contact persons.
- submit a SAR at any time; and
- receive e-mail confirmations of each SAR submitted.

You can register with the NCA here.

11.8.2 Post or fax

SARs can still be submitted in hard copy, although they should be typed and on the preferred form. You will not receive acknowledgement of any SARs sent this way. Where you require consent/DAML you should send by fax as opposed to by post. The NCA encourages you to use the SARs online system wherever possible.

11.9 Information to include

The NCA has provided information on completing the preferred SARs form and FAQs on good practice. This information can be found here.

To speed up consideration of your SAR, it is important to use the correct NCA glossary codes for each reason for suspicion in your report.

The UKFIU periodically provides updated glossary codes and reporting routes and it is best to check the NCA website for the latest information. The latest glossary codes are available here.

Many of the glossary codes may not apply unless you have a suspicion criminal property relates to a specific predicate offence. The UKFIU has agreed to establish an analytical code (a subset of glossary codes) for “technical” breaches that a legal practice may encounter in transactional work. The code (0589-LS) may be used if the kind of criminal property identified relates to minor, technical regulatory offences that are unlikely to be pursued by law enforcement (for example the breach of a tree preservation order).

A good quality SAR can help prioritise urgent cases and investigations and provide intelligence to feed into typologies and identify trends. Missing or inaccurate information reduces the overall effectiveness of the SAR. It can also have a negative impact on identifying the subjects correctly. If your SAR is deficient, or does not contain the requisite information, the UKFIU may send you further correspondence, either closing the matter or seeking additional clarification.

You should include the information below in your SAR, where known. If you do not know crucial information, for example an individual’s name, you should state “unknown” and repeat that this is unknown in relevant sections throughout the SAR.

Subject identifiers, e.g.

- Full name.
- Date of birth.
- Address(es).
- Account numbers.
- Occupation.
- National Insurance Number(s).
- Passport or other relevant documentation numbers.
- Identify other party/parties involved in the criminal conduct or dealing with the criminal property, including their dates of birth and addresses where appropriate and known;
- Suspected criminal behaviour;
- Glossary code(s); and
- Clear descriptions of reasons for suspicion.

11.10 Seeking consent (Defence Against Money Laundering)

The NCA can provide a defence against money laundering (DAML) charges or terrorist financing, commonly known as “consent”. It is important to remember that a granted consent from the NCA does not:

- oblige the reporter to carry out the prohibited act;
- legitimise the funds;
- override private rights of an individual;
- override or replace regulatory requirements e.g., CDD; and
- prevent law enforcement investigating the subject.

You only receive consent to continue working on a matter to the extent to which you asked for it. So, it is vital that you clearly outline all the remaining steps in the transaction that could be a prohibited act. When specifying acts for which you are seeking consent, be careful to include anything that may amount to aiding and abetting the client.

If you are seeking consent, it is important to specify whether you are seeking it for yourself, for your client, or both. Your request should make clear who is seeking consent for each prohibited act.

11.10.1 Required information for NCA to make DAML decision

In addition to the information outlined above, it is important to both tick the consent box and use the code for DAML SARs. This indicates to the NCA that the SAR requires immediate attention. Use XXS99XX if you are seeking consent to deal with property valued more than £3,000 and XXGVTXX for sums less than £3,000. You should include any other relevant glossary codes.

You also need to provide:

- Clear description of your reason for suspicion.
- A description of the potential criminal property, including its value; and
- The prohibited act you seek to undertake involving the criminal property. It is advisable to use the terminology “prohibited act” when describing any proposals for dealing with the property.

The prohibited act is the key difference between a SAR and a DAML SAR. For example, moving money from a client account back to a client where you suspect they may have gained it via unlawful means.

An example of a "reason for suspicion" may be:

Glossary Code: ""XX S99XX, XXPROPXX"

"I am submitting this SAR as the client is purchasing a property and I have concerns relating to the origin of the funds coming from overseas transactions. The reason for my money laundering suspicions are that…"

You should also consider adding other useful information such as previous SAR reference numbers if they relate to the client/matter.

A submission should also conclude with any intended next steps - e.g., exiting relationship, monitoring events etc.

11.10.2 What happens after I submit a DAML SAR?

Once you submit a SAR, the NCA has seven working days, known as the "notice period" starting the day after the SAR is submitted to look at the SAR and ask for more information if necessary.

If consent is refused, you will enter a moratorium period of a further 31 calendar days.
If you need consent sooner, you should clearly state the reasons for the urgency in the initial report. Within the notice and moratorium period you must not undertake a prohibited act. However, this will not prevent you taking other actions on the file, such as writing letters, conducting searches etc. You cannot seek status updates for a DAML unless there is a life-threatening situation or there is a potential for significant harm – as this may divert NCA resources away from other situations of this type and fast-tracking high priority SARs could be delayed. The UKFIU have seven days to update you on your DAML and unnecessary requests for progress checks slows down the whole process for all SAR regime stakeholders.

If the NCA does not respond in the 7-day period, you may consider that you have what is known as "deemed consent" (s335(2) of POCA.)

The NCA may also send you one of the following letters:

- Letter C - Closure for not meeting standards criteria. If significant information is missing the NCA may close the case without consultation. When a case is closed you may resubmit a new request if you choose to do so;
- Letter D - Request for more information or to clarify required information; or
- Letter E - Closure no response in specified time frame/ unsatisfactory answer in response to letter D: Having made requests for further information, if nothing is received in writing within two days, the UKFIU will consider closing the case.

11.11 Tipping off

You must not say anything about an internal disclosure or SAR which could prejudice an investigation. If you do so, you could be guilty of an offence under POCA s333A or TACT s39. When considering if you can discuss with your client that you have submitted a SAR

about them you will need to fully consider the sections on tipping off and prejudicing investigations in Sections 16 and 17.

A legal professional will not commit a tipping off offence under section 333A if the disclosure is to a client and it is made for the purpose of dissuading the client from engaging in conduct amounting to an offence (as per section 333D(2)). .

It can be extremely challenging to explain delays to clients while waiting for a response from the NCA. You must not complete the prohibited act while you are awaiting a response. This underlines the importance of making a SAR as soon as possible. As highlighted above, you may still be able to take some actions provided those actions do not of themselves involve a prohibited act.

You should note that protection from civil liability exists in this situation, arising from POCA S338(4a) which states “Where an authorised disclosure is made in good faith, no civil liability arises in respect of the disclosure on the part of the person by or on whose behalf it is made”.

You may discuss the SAR if doing so would not prejudice an investigation, although you should take caution in doing so. POCA also sets out some additional situations where you may disclose the contents of the SAR. Please refer to the sections on tipping off in sections 16 and 17 of this guidance.

11.12 Extensions of the moratorium period

The Criminal Finances Act 2017 made important changes to the moratorium period under POCA. Section 336A of the amended POCA enables the moratorium period to be extended by court order and section 336C provides for an automatic extension of the moratorium period in certain cases.

The moratorium period allows law enforcement agencies to gather evidence to determine whether further action, such as restraint of the funds, should take place.
The NCA may require further information to be able to undertake proper analysis and make an informed decision on whether to investigate.

11.12.1 Section 336A – court’s power to extend moratorium period

The court (Crown Court in England, Wales and Northern Ireland and the Sheriff Court in Scotland) may only grant an extension of the moratorium period upon an application by a senior officer if it is satisfied that:

- an investigation is being carried out in relation to a relevant SAR but has not been completed,
- the investigation is being conducted diligently and expeditiously;
- further time is needed for conducting the investigation; and
- it is reasonable in all the circumstances for the moratorium period to be extended.

The application must be made by the senior officer before the end of the moratorium period. The court may extend the moratorium period by a further 31 days, i.e., the total moratorium period at this stage may be up to a maximum of 62 days. The length of the extension should be based on the four requirements set out above.

The court may hear further applications to extend the moratorium period (for further 31-day periods) provided that the total number of extensions does not exceed a period of 186 days

over and above the initial 31-day moratorium period. In total this means that the moratorium period can be a maximum of 217 days.

11.12.2 Power of the court to exclude and withhold information from interested persons

The court may exclude an interested person (or anybody representing that person) from any part of a hearing to extend the moratorium period. The Court may also order on application that specified information is withheld from an interested person (or anybody representing that person). The court must exclude any interested person from an application to withhold specified information.

An interested person is either the person who made the SAR or any other person who appears to the senior officer to have an interest in the relevant property. The first category is straightforward but the second could in effect be the client of the practice or any other third party who may have an interest in the underlying property.

The court may withhold the specified information only if it is satisfied that there are reasonable grounds to believe that a SAR would lead to the following:

- evidence of an offence would be interfered with or harmed;
- the gathering of information about the possible offence would be interfered with;
- a person would be interfered with or physically injured;
- the recovery of property under the Act would be hindered; or
- national security would be put at risk.

In practice this means that a person that has made a SAR may be excluded from participating in the hearing of the application to extend the moratorium period.

A possible difficulty here is whether they can sensibly either take instructions from their client (see risks of tipping off below) or take their own action to minimise the risks of a lengthy moratorium period with the risks of tipping off that may bring, given they may not have access to all of the information. You should carefully assess the risks of continuing to take instructions in these circumstances and ensure that any decision is taken with the knowledge of relevant individuals in your practice (e.g., the MLRO and/or MLCO.)

11.12.3 Risks of tipping off in the moratorium period

Once you are on notice of an application to extend the moratorium period, you may inform your client of the existence of the application to extend the moratorium period without committing the tipping off offence. However, you are permitted to disclose "only such information as is necessary for the purposes of notifying the customer or client that an application… has been made" and no more than that. In effect the risks of tipping off are still present as you must not disclose the content of the SAR to the client, or even the reason for your suspicion.

You should be careful in dealing with clients and third parties to make sure that you do not tell them anything about a SAR which may prejudice an investigation. If you are seeking to challenge an application to extend time, then you should also consider whether you may properly do so without taking instructions and generally whether it would be in the best interests of your client to do so.

11.12.4 Section 336C – Automatic extension of the moratorium period

If an application is made under section 336A and the initial 31-day moratorium period would end before that application is heard by the court, then the moratorium period is automatically extended to the date the court determines the application. Also, if an appeal is made against a decision to extend the period and the moratorium period ends before that appeal is heard, then the moratorium period is automatically extended to the date when the appeal is heard. However, the maximum period of any such automatic extension is a period of 31 days from the date when the period would otherwise end.

If an application is made under section 336A and is refused and if the period would otherwise end before the end of 5 days after that hearing, then the period will be extended for a further 5 days from the hearing date. This is presumably a safeguard for the investigating authority to take any further action (such as a restraint order) before the period again expires.

11.13 Contacting the NCA/UKFIU

For DAML enquiries, all contact with the UKFIU DAML Team is via email: DAML@nca.gov.uk

For queries regarding SAR Online/general enquiries you can contact the UKFIU helpdesk by phone on 0207 238 8282 and select option 2 or 3, or by email at ukfiusars@nca.gov.uk.

11.14 Confidentiality of SARs

The NCA is required to treat your SARs confidentially. Where information from a SAR is disclosed for the purposes of law enforcement, care is taken to ensure that the identity of the reporter and their practice is not disclosed to other persons.

If you have specific concerns regarding your safety if you make a SAR, you should raise this with the NCA either in the report or through the helpdesk. If you have concerns about your immediate safety following the making of a SAR, you should contact your local police.

If you fear the confidentiality of a SAR you made has been breached, call the SARs confidentiality breach line on 0800 234 6657.

11.15 Sharing of information within the regulated sector and joint disclosure reports

The Criminal Finances Act 2017 amended POCA to introduce sections 339ZB-G to provide a gateway for sharing information between persons and entities in the regulated sector on a voluntary basis and making joint disclosure reports (super SARs). At present these information sharing provisions have only been commenced for financial and credit institutions and not legal professionals.

The provisions seek to encourage the sharing of information across the private and public sectors to combat money laundering by providing protection for what would otherwise be a breach of confidentiality if certain conditions are fulfilled.

Where information is requested from one regulated person by another on a voluntary basis there are requirements imposed to notify the NCA. After information has been shared, a joint disclosure report can be made to the NCA on behalf of the parties both disclosing and receiving the information, a so called ‘super SAR’. Making either a required notification or a

joint disclosure report will be treated as satisfying the requirements of sections 330 and 331 to make a disclosure in the regulated sector.

Note, however, that when you are advising on a proposed transaction, you may submit a SAR on behalf of your firm and your client, subject always to an analysis of the tipping off provisions.

The Home Office has published a circular with further detail on information sharing within the regulated sector under sections 339ZB-339ZG.

12. Other duties

12.1 General Comments

Compliance with the Regulations, generally falls under a few headings, including assessing risk, undertaking due diligence, training staff etc. There are a handful of further duties that may arise due to a practice being in scope of the Regulations.

These are discussed here and mainly concern complying with the requirement to register certain entities and other duties that arise from the existence of such registers (e.g., reporting discrepancies.)

12.2 Money Laundering Regulations Part 5 Requirements - Overview

You must comply with Part 5 of the Regulations if:

- your practice is a UK body corporate; or
- you (as an individual or an organisation) accept an engagement as a trustee (i.e., as opposed to acting for a trustee) of a relevant trust.

12.3 Obligations on UK body corporates

Under R42(2)(a) a UK body corporate is defined as 'a body corporate which is incorporated or formed under the laws of the UK or a part of the UK'. This includes but is not limited to:

- listed and unlisted companies;
- limited liability partnerships; and
- Scottish limited partnerships.

Under R43(1), if your practice is a body corporate and it enters into a relevant transaction or forms a business relationship with another person to whom the Regulations apply then you must provide that person with the following information on request:

- your name, registered number, registered office and principal place of business;
- your board of directors, or members of your equivalent management body;
- the senior persons responsible for your operations;
- the law to which you are subject;
- your legal owners;
- your beneficial owners; and
- your articles of association or other governing documents.

The obligation to provide this information also applies to your clients who are UK body corporates when they enter relevant transactions or form a business relationship with your practice, which may assist you in your conduct of CDD.

If the identity of individuals or the above information changes during the course of the business relationship, then you must notify the other person within 14 days of the date on which you or the relevant body corporate became aware of the change.

12.4 Obligations of trustees of trusts with a UK Tax Consequence

The Regulations impose obligations on trustees of 'relevant trusts' to maintain accurate and up to date written records relating to the trust's beneficial owners and potential beneficiaries and provide certain information about those beneficial owners and potential beneficiaries to relevant persons and law enforcement authorities on request. The trustees must also provide this information to HMRC through the Trust Registration Service (TRS) each tax year in which the trustees incur a liability to UK tax in relation to trust income or assets. The information on the Trust Register will be available to law enforcement agencies in the UK and EEA member states.

A relevant trust is:

- a UK express trust (i.e., if all the trustees are resident in the UK or if one or more of the trustees is UK resident and the settlor was resident and domiciled in the UK when the trust was set up or (at any time) when the settlor added funds;
- a non-UK express trust (i.e., if it is not a UK trust and it receives UK source income or has UK assets on which it is liable to pay a UK tax); or
- any other non-UK express trust, that is not a trust listed in Schedule 3A (excluded trusts) and whose trustees (in their capacity as such) acquire an interest in land in the United Kingdom (i.e., appear on any of the three relevant UK land registries) or enter into a business relationship with a relevant person, where at least one of those trustees is resident in the United Kingdom and the trust is not an EEA registered trust

An EEA registered trust is a trust whose beneficial ownership information is required, by Article 31.3a of the fourth money laundering directive, to be held in a central register set up by an EEA state other than the United Kingdom.

A taxable relevant trust arises when the trustees of a relevant trust have incurred a liability to UK tax in relation to trust income or assets in a given tax year.

Where you act (including occasionally) as a trustee of a taxable relevant trust you will need to maintain written records and provide the information specified in the Regulations to HMRC annually and to relevant persons with whom you enter into relevant transactions or business relationships and law enforcement authorities on request, the information specified in the Regulations.

A trustee or settlor is resident in the UK if it is a UK body corporate or, if the trustee is an individual, he or she is resident in the UK for the purposes of one or more of the below-mentioned UK taxes.

12.4.1 Which trusts must be registered?

All taxable relevant trusts must be registered.

A taxable relevant trust is a UK express trust or a non-UK express trust which has UK source income or UK assets which the trustees are liable, even if only occasionally, to one or more of the following UK taxes in relation to trust income or assets: Income Tax, Capital Gains Tax, Inheritance Tax, Stamp Duty Land Tax, Land and Buildings Transaction Tax or Stamp Duty Reserve Tax.

Bare trusts (a trust in which the beneficiary has an absolute right to the capital and assets within the trust and income thereby generated) and implied trusts (a trust which arises by operation of law, so a resulting trust or a constructive trust) are not relevant trusts and are therefore not subject to Part 5 of the Regulations.

12.4.2 Which beneficial owners do the trustees need to note and record?

The trustees of a relevant trust are obliged to maintain accurate and up to date written records of all the trust's beneficial owners, who will include its:

- settlor.
- trustees.
- actual or potential beneficiaries.
- any other individual who has control over the trust which may include a protector or protectors; and
- any other potential individual (note, not entity) beneficiaries referred to in a document from the settlor, such as a letter of wishes, relating to the trust.

The concept of individuals who have 'control' over the trust is defined in Regulation 6(2) and encompasses individuals who have a power (exercisable alone or jointly) under the trust instrument or by law to:

- dispose of, advance, lend, invest, pay or apply trust property.
- vary or terminate the trust.
- add or remove a person as a beneficiary or to or from a class of beneficiaries.
- appoint or remove trustees or give another individual control over the trust; or
- direct, withhold consent to or veto the exercise of a power mentioned in sub-paragraph 5.3.1 to 5.3.7 above.

12.4.3 What information must the trustees maintain in relation to each beneficial owner, potential beneficiary and the trust itself?

Where the beneficial owner or potential beneficiary is an individual (but note, not where they are a class), the trustees must note and record:

- the individual's full name.
- the individual's national insurance number or unique taxpayer reference, if any.
- the individual's date of birth; and
- the nature of the individual's role in relation to the trust.

If the individual does not have a national insurance number or unique taxpayer reference, you should record the individual's usual residential address. If that address is not in the UK, the individual's passport number or identification card number should be recorded, with the country of issue and the expiry date of the passport or identification card. If the individual does not have a passport or identification card, the number, country of issue and expiry date of any equivalent form of identification.

Where the beneficial owner is a corporate body, the trustees must note and record:

- if applicable, the register of companies in which the legal entity is entered (including details of the EEA state or third country in which it is registered), and its registration number in that register; and
- the nature of the entity's role in relation to the trust.

The trustees must also note and record the following information in relation to the trust:

- the name of the trust.
- the date on which the trust was set up.
- a statement of accounts for the trust, describing the trust assets.
- identifying the value of each category of the trust assets at the date on which
- the information is first provided to HMRC (including the address of any property held by the trust).
- the country where the trust is considered to be resident for tax purposes.
- the place where the trust is administered.
- a contact address for the trust; and
- the name of any advisers who are being paid to provide legal, financial, tax or other advice to the trustees in relation to the register requirements.

The details of trust assets have to be based on market value at the date on which the asset(s) was placed in the trust by the settlor, when the settlement was first created. To keep administrative burdens on trustees to a minimum HMRC are not expecting any formal valuation but they would expect trustees to provide an accurate estimate of the market value of the assets. If trustees are registering a trust where the value of assets were notified to HMRC previously through either a 41G form or SA900 tax returns then trustees should complete the “Other Asset” field using the term – “Already notified”, leaving all other asset fields marked as “£1”. The details of trust assets have to be provided only once, at the first point of registration.

12.4.4 When does the information need to be obtained and updated for taxable trusts?

The information for taxable relevant trusts must be provided—
(a) on or before 31st January after the tax year in which the trustees were first liable to pay any UK taxes, in the case of a trust which is set up before 6th April 2021.
(b) on or before 10th March 2022, in the case of a trust which is set up after 5th April 2021 where the trustees become liable to pay UK taxes before 9th February 2022.
(c) within 30 days of the trustees becoming liable to pay UK taxes, in any other case.

Information provided in relation to beneficial owners should be current at the date the register is updated and not as at the tax year which triggered the registration. There are certain obligations on trustees in the Regulations to provide third parties with the records and update third parties of a change to the records, which they hold on beneficial owners and potential beneficial owners, within 14 days.

12.4.5 Associated obligation on the trustees to provide information to a relevant person

Where a trustee of a relevant trust is acting as a trustee and enters into a transaction or forms a business relationship with a relevant person, they must inform that relevant person they are acting as trustee. They must also provide that relevant person with information identifying the beneficial owners of the trust and any other person named in a letter of wishes on request.

Regulation 44(3) imposes an obligation on the trustees to notify the relevant person of any change in the identity of the beneficial owners and potential beneficiaries (including persons named in letters of wishes, which may be revised informally and frequently) within 14 days of the date on which any one of the trustees became aware of the relevant change.

12.4.6 Obligation on trustees to provide records to any law enforcement authority

Aside from the obligation to provide HMRC with information on the 31 January following the end of each tax year, the trustees of a relevant trust are also obliged by Regulation 44(5) to provide information about the beneficial owners and potential beneficiaries of the trust which they have recorded, directly and 'on request' to any law enforcement authority in compliance with the deadline set by the law enforcement authority (listed in Regulation 44(10). The trustees of a relevant trust may be approached by law enforcement at any point.

12.4.7 How long do the records need to be maintained?

Where the trustees are professional trustees (i.e., being paid to act as trustees), which is likely to be the case if you or your practice is acting as a trustee, they must retain the records referred to above for a period of five years after the date on which the final distribution is made under the trust.

They must then delete them unless each named beneficial owner and potential beneficiary in the records, consents to longer retention or where longer retention is required by law or for the purposes of court proceedings.

Please note that this may result in your practice having one retention period for its CDD records, including where it acts in relation to a trust for trustees, and a different retention period for records which it is required to hold when it acts as a trustee.

12.4.8 What information do trustees need to provide to HMRC for the register and when?

The trustees of a taxable relevant trust need to provide all the information which they must record on the trust and its beneficial owners and potential beneficiaries as set out above to HMRC.

Trustees should note that the register-reporting obligation only arises if the trustees incurred a liability to pay any of the specified UK taxes in relation to trust income or assets in the preceding tax year. So, a trustee of a non-UK trust which only generates a UK tax liability in the form of a ten-yearly inheritance tax charge need only report to HMRC on or before the 31 January which falls after the tax year in which the inheritance tax charge falls due (in each case).

Trustees that submit the trust tax return will be asked to confirm in Q20 of the return whether they have registered or updated the details of their trust on the TRS.

12.4.9 How will relevant information be provided to HMRC?

The TRS is an online register and allows trustees to submit information about their taxable relevant trust online. For further information on how to register a trust on the TRS, trustees should visit www.gov.uk.

Trustees will also be obliged to make a 'no change' declaration to HMRC annually on or before the 31 January which falls after any tax year in which the trustees are liable to pay any of the above-mentioned UK taxes if there has been no change to the information provided to HMRC.

12.4.10 With whom can HMRC share the information on the register?

HMRC is obliged to share the trust data with any UK law enforcement authority. The following organisations are listed as UK law enforcement authorities in the Regulations:

- Financial Conduct Authority (FCA).
- National Crime Agency (NCA).
- the police forces maintained under section 2 of the Police Act 1996(a).
- the Police of the Metropolis and for the City of London.
- the Police Services of Scotland and Northern Ireland; and
- the Serious Fraud Office (SFO).

12.4.11 Duties arising from the register of beneficial owners of taxable relevant trusts

If you or your practice acts as (as opposed to for) a trustee of a taxable relevant trust, pursuant to R44 of the Regulations you will need to maintain accurate and up to date records of all beneficial owners and potential beneficiaries of the trust. If your practice is also acting for the trustee(s) and has applied CDD, this may require you to collect extra information.

If you form a business relationship in your role as trustee with a relevant person, which could be an advisory relationship with your practice (if it is subject to the Regulations), you must inform the relevant person that you are acting as a trustee and, on request, provide the relevant person with information identifying the trust's beneficial owners and potential beneficiaries.

That obligation lies on (external) trustees of relevant trusts who enter into transactions in relation to which you or your practice are required to apply CDD or who form a business relationship with you or your practice (if you are subject to the Regulations). This should assist you in your compliance with your CDD obligations and is another reason why it makes sense to extend your CDD in relation to a relevant trust's beneficial owners to cover potential beneficiaries.

Otherwise, from a reputational risk and advisory perspective, as law enforcement authorities may gain access to information not only about the trust's beneficial owners as defined in R6(1) but also the names of those individuals who are referred to in any document from the settlor, such as a letter of wishes relating to the trust, it is prudent to note such wider information in your CDD records where you act for any client in relation to a relevant trust, and, indeed where you act in relation to any trust.

12.5 Obligations of trustees of trusts without a UK Tax Consequence

12.5.1 Types of trust

Trusts that do not meet the definition of a taxable relevant trust also have obligations.

Type A - a UK trust which is an express trust and is not an EEA registered trust or a trust listed in Schedule 3A that is not a taxable relevant trust

Type B - a non-UK trust which has at least one trustee resident in the United Kingdom, is an express trust and is not an EEA registered trust or a trust listed in Schedule 3A that is not a taxable relevant trust

Type C - a non-UK trust which is an express trust and is not a trust listed in Schedule 3A, where none of the trustees are resident in the United Kingdom and those trustees, in their capacity as such, acquire an interest in land in the United Kingdom that is not a taxable relevant trust.

Exempted trust types can be found here. .

12.5.2 For individuals

Any beneficial owner or named potential beneficiary must provide the following:

- the individual's full name;
- the individual's month and year of birth;
- the individual's country of residence;
- the individual's nationality; and
- the nature and extent of the individual's beneficial interest.

The above information must be provided—

- on or before 10th March 2022, in the case of a trust which first falls in scope of the above before 9th February 2022; or
- in any other case, within 30 days of the trust being set up, or, if later, within 30 days of the trust first falling in the above scope.

- unless the beneficiaries have not yet been determined, (e.g., because the beneficiary is a class) in which case the information does not need to be provided until the beneficiaries have been determined.

12.5.3 For legal entities

If the beneficial owner is a legal entity, they must provide the following information:

- the legal entity's corporate or firm name;
- the registered or principal office of the legal entity; and
- the nature of the entity's role in relation to the trust.

If Type A and Type B have a controlling interest in a third country entity, they must provide:

- the third country entity's corporate or firm name;
- the country or territory by whose law the third country entity is governed; and
- the registered or principal office of the third country entity.

and if they subsequently acquire an interest in a third country entity, they have 30 days to provide this information. If any of the information provided changes, there is a 30-day window to update the register.

12.6 Reporting of Discrepancies on Registers

Before establishing a business relationship with a:

- company (registered or unregistered as defined in the Unregistered Companies Regulations 2009(1));
- Limited Liability Partnership; or
- Scottish Partnership;

- a practice must collect proof of registration (e.g., via the client) or an excerpt from the relevant register.

If the firm finds a discrepancy between information relating to the beneficial ownership of the company which it collects as above, and information which becomes available to it whilst carrying out its duties under the ML Regulations (during its onboarding process), the discrepancy must be reported to Companies House (R30A(3))

Practices that encounter such discrepancies while fulfilling their AML duties, must report them, but it is not a requirement for practices to actively seek out such discrepancies.

This responsibility to report does not apply where the information is subject to Legal Professional Privilege.

Discrepancies only have to be reported when establishing a new business relationship. Relevant persons do not have to review the records of existing customers, or report during CDD refreshes.

Discrepancies should be reported to Companies House (via the online reporting tool available on the Companies House website) or in the case of trusts to HMRC as soon as reasonably possible. A business relationship can be established prior to a discrepancy being reported.

We would interpret as soon “as reasonably possible” to allow practices enough time to report the discrepancy to the client, with the understanding that the client could quickly amend the discrepancy, thus negating the need to notify the registrar. Any hesitation or resistance by the client in this regard would hasten the need to report the discrepancy.

Furthermore, in the interpretation of what is a reportable discrepancy, you may apply a test of whether the discrepancy is material.

In order for it to meet this test, it needs to indicate a factual difference, so a simple typo, or a difference in the extent of the information would not meet this test and would not need to be reported.

For example, if a register listing had the first name and surname of the individual correct but included only the first letter for their middle name as opposed to the full name, this would not be a material discrepancy, and would not need to be reported.

Similarly, if a first name were spelled both John and Jon or Leah and Lea across the register and documents, these discrepancies would not need to be reported.

Where you conclude that a discrepancy does not require a report to be made you should document that as part of your CDD record and/or client/matter risk assessment.

If you are using reliance on another entity to undertake CDD on your behalf, you can also use this reliance arrangement for them to report discrepancies on your behalf. Also, as with CDD, you can outsource this function to a service provider though you will remain responsible for your firm's compliance.
Further information regarding the duty to report discrepancies can be found here

13.Legal Professional Privilege

13.1 Introduction & Application

This chapter is relevant to any lawyer[2] considering whether to make a disclosure to the NCA under POCA.

The first principles of Legal Professional Privilege (LPP) recognise the importance of the right of an individual to claim and maintain the confidentiality of their communications with a lawyer for the purpose of obtaining legal advice and representation. As such, LPP is "*a fundamental human right long established in the common law*"[3]. Its centrality to the professional relationship between lawyer and client is recognised throughout the world.[4]

However, aspects of the application of the law in this area can be complex and the consequence of the lawyer making the wrong decision as to its application can be personally, and professionally, significant. Lawyers should be careful to determine the basis on which their client may make a claim to LPP based on the relevant qualification of the lawyer concerned and, also, the context of the exchange. Although LPP is usually understood as a common law protection afforded to clients of barristers, solicitors, the Fellows of the Chartered Institute of Legal Executives (CILEX)[5], and foreign lawyers[6] LPP may also be conferred by statute[7] (sometimes only for limited purposes), as in the case of

[2] The term "lawyer" is used throughout this note to refer to legal professionals as recognised in the Legal Service Act 2007.
[3] See comments by Lord Hoffmann in *R. (on the Application of Morgan Grenfell & Co Ltd) v Special Commissioner of Income Tax* [2002] 1 AC 563.
[4] See, for example, United Nations *Basic Principles on the Role of Lawyers* (1990), the International Bar Association *Core Principles of the Legal Profession* (2018) and the Council of Bars and Law Societies of Europe *Charter of Core Principles of the European Legal Profession and Code of Conduct for European Lawyers* (2018). Note, also, the right of the client to the protection of LPP is also a fundamental human right both at common law and under Article 6 (right to a fair trial) and Article 8 (respect for family and private life) under the European Convention on Human Rights (ECHR).
[5] See comments by Lord Neuberger in *R.(on the application of Prudential plc and another) v Special Commissioner of Income Tax [2013] UKSC* 1 at paragraph 29 as to the ambit of such protection which, he states, *"includes members of the Bar, the Law Society, and the Chartered Institute of Legal Executives (CILEX) (and, by extension, foreign lawyers). That is plain from a number of sources, which speak with a consistent voice."*
[6] In *PJSC Tatnef v Bogolyubov and others* [2020] EWHC 2437 (Comm) Mrs Justice Moulder confirmed in relation to foreign lawyers that *"The only requirement in order for legal advice privilege to attach is that they should be acting in the capacity or function of a lawyer or as expressed by Lord Neuberger in Prudential at [19], it should relate to: "communications passing between a client and its lawyers, acting in their professional capacity, in connection with the provision of legal advice."*
[7] Statutory extension in this area is often framed in terms that the relevant professional had been acting "in like manner" as "the client's solicitor" such as in s.190 Legal Services Act 2007 in the context of litigation.

licensed conveyancers[8] patent[9] and registered trademark attorneys[10]. The extent to which LPP attaches to a notary's records has not been the subject of a legal decision in England and Wales and is an evolving area of law. Notaries should therefore consider seeking specific legal advice based on the particular circumstances of a given situation if it appears LPP may apply. [11] In addition, there may also be circumstances in which a client may claim litigation privilege (see discussion below) which does not require a party to the communication to be a lawyer or other legal professional.[12]

13.1.1 POCA & LPP

Sections 327 - 329, 330 and 332 of POCA contain provisions for disclosure of information to be made to the NCA. Further, a recent amendment, Sections 339ZB-G, allows for the voluntary sharing of confidential information to both the NCA, and to other persons carrying on business in the regulated sector when the disclosure may assist in determining any matters in relation to a suspicion of money laundering activity.

Legal professionals also have a duty of full disclosure to their clients. However, sections 333A and 342 of POCA prohibit disclosure of information in circumstances where a SAR has been made and/or where it would prejudice an existing or proposed investigation.

It is, therefore, important to understand the interplay between LPP and the disclosure obligations under POCA.

13.1.2 Why a decision-making framework is needed

Whilst the first principles are relatively straightforward to articulate, each situation turns on its own particular facts and context[13]. LPP is a complex area of law and subject to change. An understanding of LPP and how it is being applied is central to the decision as to whether to make a disclosure under the POCA[14]. It is not enough to assume that an exchange must be covered by LPP; there must be an active assessment as to its application.

This complexity in definition is compounded by the inclusion of the narrowly defined statutory "privileged circumstances" exemption under s330, which is sometimes confused with common law LPP. The lawyer is under a duty to both defend LPP whilst, in the context of AML/CTF, being alert to any suspicion or knowledge of money laundering that may displace this primary duty. Given the potential vulnerability of the lawyer when making such an assessment and, potentially, the need to establish a defence to a subsequent non-disclosure offence, the precise steps taken by the professional to establish whether LPP applies are critical.

The chapter examines the tension between the professional duties of the lawyer and the provisions of POCA in marginal cases. Similar tensions also arise with respect to the

---

[8] See s.33 Administration of Justice Act 1985.

[9] Copyright Designs and Patents Act 1988 s 280.

[10] Trademarks Act 1994 s 87

[11] You should also consult relevant guidance issued by your regulator relating to the nature and effect of legal professional privilege for your specific legal qualification.

[12] LPP is the right of the client, not the lawyer and, consequently, protects an unrepresented person – see *R. (on the application of Kelly) v Warley Magistrates' Court* [2007] EWHC 1836 (Admin); 1 Cr. App. R. 14 per Laws, L.J., at 18.

[13] It is not possible to provide a detailed analysis of LPP in this note. For detailed analysis see Bankim Thanki QC et al *The Law of Privilege* (3rd Edition) (Oxford University Press, 2018) and Colin Passmore *Privilege* (4th edition) (Sweet & Maxwell, 2019).

[14] See *FATF Guidance for a Risk Based Approach: Legal Professionals* (June 2019) p11.

Terrorism Act as to when LPP applies and prevents disclosure under the relevant legislation. A systematic decision-making process, based on case law and statute, will help the lawyer to demonstrate compliance with all relevant professional and regulatory obligations, not just those under POCA. This chapter aims to provide a practical framework to support the decision-making process of the lawyer as they determine whether, in the context of the mandatory reporting obligations under POCA, a particular document, or conversation, is subject to LPP. You will find it helpful to read the guidance note together with the decision making template in paragraph 13.8.1.

It is not, however, a substitute for a detailed review of all case law and legislation relevant to a specific case.

The application of legal professional privilege is often complex and fact sensitive.

If you are in any doubt as to whether legal professional privilege applies in the context of the case in which you act, you should seek independent legal advice as part of your decision-making process.

Seeking legal assistance in this manner, or assistance from your Money Laundering Reporting Officer, does not constitute a breach of your retainer with the client, the rules of professional conduct or the provisions of the Proceeds of Crime Act 2002 or the Money Laundering Regulations (as amended)."

This chapter should be read in conjunction with Chapter 11 of this guidance (Suspicious Activity Reporting). As stated above, if you are still in doubt as to your position, you should seek independent legal advice.

13.2 What is Legal Professional Privilege?

LPP is a privilege against disclosure, ensuring clients know that certain communications with legal professionals cannot be disclosed. LPP protects the personal right of the client to refuse to give evidence about a discussion with their lawyer, or to withhold a document from production, on the basis that the exchange is subject to LPP.

LPP arises in recognition of the client's fundamental human right to be candid with their legal adviser[15], without fear of later disclosure of their communications to their prejudice. It is an absolute right, protected both by the common law and by human rights obligations and cannot be overridden by any other interest, although it can be waived (by the client alone) or, abrogated by the clear terms or the necessary implications of a specific statutory provision.[16]

[15] See Lord Taylor's discussion of the absolute nature of LPP *in R v Derby Magistrates' Court Ex Parte B* [1996] 1 A.C. 487 at 540.

[16] See *Bowman v Fels* [2005] EWCA Civ 226 para 87 *"much stronger language would have been required if s 328 could be interpreted as bearing the necessary implications that legal professional privilege was to be overridden."*

The importance of LPP to the rule of law was described by Lord Scott in *Three Rivers District Council v Governor and Company of the Bank of England (No 6)* in the following terms,

> *"….. in the complex world in which we live there are a multitude of reasons why individuals, whether humble or powerful, or corporations, whether large or small, may need to seek the advice or assistance of lawyers in connection with their affairs; they recognise that the seeking and giving of this advice so that the clients may achieve an orderly arrangement of their affairs is strongly in the public interest; they recognise that in order for the advice to bring about that desirable result it is essential that the full and complete facts are placed before the lawyers who are to give it; and they recognise that unless the clients can be assured that what they tell their lawyers will not be disclosed by the lawyers without their (the clients') consent, there will be cases in which the requisite candour will be absent. It is obviously true that in very many cases clients would have no inhibitions in providing their lawyers with all the facts and information the lawyers might need whether or not there were the absolute assurance of non-disclosure that the present law of privilege provides. But the dicta to which I have referred all have in common the idea that it is necessary in our society, a society in which the restraining and controlling framework is built upon a belief in the rule of law, that communications between clients and lawyers, whereby the clients are hoping for the assistance of the lawyers' legal skills in the management of their (the clients') affairs, should be secure against the possibility of any scrutiny from others, whether the police, the executive, business competitors, inquisitive busy-bodies or anyone else (see also paras. 15.8 to 15.10 of Adrian Zuckerman's Civil Procedure where the author refers to the rationale underlying legal advice privilege as "the rule of law rationale"). I, for my part, subscribe to this idea. It justifies, in my opinion, the retention of legal advice privilege in our law, notwithstanding that as a result cases may sometimes have to be decided in ignorance of relevant probative material."*[17]

However, LPP does not extend to everything legal professionals have a duty to keep confidential. LPP protects only those confidential communications that fall within the definition of LPP, which is a "single integral privilege" (*Three Rivers 6*). However, within this definition, two essential types of LPP are recognised, legal advice privilege (LAP) and litigation privilege, and both have different characteristics in their scope and application as discussed below[18] at 13.10.1

A legal professional is obliged, professionally, at common law and, often, contractually within the retainer, to keep the affairs of clients confidential and to ensure that all staff do likewise. The obligations extend to all matters revealed to a legal professional, from whatever source, by a client, or someone acting on the client's behalf.[19]

---

[17] See *Three Rivers District Council v Governor and Company of the Bank of England (No 6)* [2004] UKHL 48 AT 36; [2003] 1 A.C. AT 508.

[18] In addition to legal advice privilege and litigation privilege, there are other types of privilege, such as joint and common interest privilege, without prejudice communications and the privilege against self-incrimination, which are nevertheless significant.

[19] See, for instance, the helpful commentary in the *SRA Guidance Note: Confidentiality of Client Information* (25 November 2019) which states*, "The duty of confidentiality applies to information about your client's affairs irrespective of the source of the information. It continues despite the end of the retainer or the death of the client when the right to confidentiality passes to the client's personal representatives.*

As a general rule, there are certain exceptional circumstances in which a legal professional's general obligations of confidence may be overridden, for example by a court order for disclosure.

However, certain types of confidential communications can never be disclosed unless statute permits this expressly or by necessary implication[20] or some very limited exceptions apply. Such communications are those protected by LPP. When LPP attaches to a communication:

- The client may waive their right. It is their privilege to waive.
- A statute, in clear and unambiguous terms may abrogate that right to the extent that it can be overridden.
- Finally, the document may have been "prepared for, or in connection with, a nefarious purpose"[21]

13.3 Definition of LPP

. On first principles, once LPP is established, it is absolute. The only issue is whether it has attached at all or, having attached, been specifically abrogated by statute, waived by the client or an exemption applies, such as the furtherance of a criminal purpose exemption (see below). As stated above, two essential types of LPP are recognised at common law: legal advice privilege (LAP) and litigation privilege.

13.3.1 Legal Advice Privilege (LAP)

Principle

Confidentiality will attach to all information given to you, by your client or a third party, in connection with the retainer in which you or your firm are instructed. Should you have information unrelated to the retainer this may not be covered by your duty." https://www.sra.org.uk/solicitors/guidance/confidentiality-client-information/

[20] See the comments of Lord Hobhouse on the meaning of "necessary implication" in *R (Morgan Grenfell) v Special Commissioners of Income Tax* 1 AC 563 *"It is accepted that the statute does not contain any express words that abrogate the taxpayer's common law right to rely upon legal professional privilege. The question therefore becomes whether there is a necessary implication to that effect. A necessary implication is not the same as a reasonable implication as was pointed out by Lord Hutton in B v DPP [2000] 2 AC at 481. A necessary implication is one which necessarily follows from the express provisions of the statute construed in their context. It distinguishes between what it would have been sensible or reasonable for Parliament to have included or what Parliament would, if it had thought about it, probably have included and what it is clear that the express language of the statute shows that the statute must have included. A necessary implication is a matter of express language and logic not interpretation."*

[21] See comments of Lord Neuberger in *R v Prudential SCIT* [2013] UKSC 1 at para 17. Scottish lawyers should refer to *Micosta S.A. v Shetland Islands Council* 1983 SLT 483 and the comments of Lord President Emslie at p.485 – the privilege is superseded where fraud or some other illegal act is alleged, and the lawyer has been directly concerned in carrying out the transaction in issue.

Communications, whether written or oral, between a legal professional (acting in their capacity as a legal professional) and a client/the client's agent for the purpose of that communication, are privileged if they are both:

- confidential; and
- for the dominant purpose of seeking legal advice and legal assistance from a legal professional or providing it to a client.

Scope

Communications are not privileged merely because a client is speaking or writing to you. The protection applies only to those communications which directly seek or provide advice (or are part of what the Court of Appeal in *Balabel v Air India* called the "continuum of communications"[22] resulting from seeking that advice) or are given in a legal context, that involve the legal professional using their legal skills and which are directly related to the performance of the legal professional's professional duties. The Court of Appeal summarised the key points in *Balabel* as follows:

> "…once a legal context is established, LAP applies, not just to those communications which expressly seek or give legal advice, but also to the "continuum of communications" between a lawyer and client aimed at "keeping both informed so that advice may be sought and given as required".[23]

Advice within a transaction

All communications between a legal professional and his or her client relating to a transaction in which the legal professional has been instructed for the purpose of obtaining legal advice are covered by advice privilege, notwithstanding that they do not contain advice on matters of law and construction, provided that they are directly related to the performance by the legal professional of their professional duty as legal adviser of his or her client. [*Three Rivers District Council and others v the Bank of England [2004] UKHL 48 at 111*]

This means that where you are providing legal advice in a transactional matter (such as a conveyance) the advice privilege will cover all:

- communications with,
- instructions from, and
- advice given to

the client, including any working papers and drafts prepared, if they are directly related to your performance of your professional duties as a legal adviser in providing legal advice. However, there is a limitation in that the fruits of that advice, such as a draft contract, lease, or conveyance will not be covered by LPP[24] unless draft would reveal, or provide an indication, as to the nature of the legal advice itself. [Fruits of advice limitation?]

---

[22] See comments in *Balabel v Air India* [1988] Ch 317 at page 330D-331A

[23] See Hickinbottom, L.J., in *CAA v R (Jet2.Com)* [2020] EWCA Civ 35 at Para 68. See also the summary at para 69.

[24] Note the comments of Watkins, L J on the status of what he described as "conveyancing matter". The court noted the absence of any authority on the point, but doubted that *"any was needed for the proposition that the document known as the conveyance is not clothed with privilege and I do not see why conveyancing matter, as I have called it, can validly be said to be, seeing that in my opinion in common sense it cannot be*

It is important to keep in mind four principles when deciding whether legal advice privilege applies:

14. The retainer of the lawyer must be reviewed. When a lawyer is consulted by a client, there is likely to be a relevant legal context defined in the retainer letter or terms of engagement. Whilst it is not conclusive, it does give a steer as to the nature of the legal context and the exchanges between lawyer and client for the purpose of legal advice.

15. As a result of the decision in *Three Rivers* (No 5) it is necessary to be clear as to the identity of the corporate client (i.e., clarify which employees are considered to be 'the client') to trigger the claim to LPP.

16. The definition of legal advice is drawn in quite a wide frame and, as established in *Balabel v Air India*, it extends to "what should reasonably and sensibly be done in a relevant legal context." [25] In such a context, most exchanges, passing between client and lawyer will include advice on an issue from a legal perspective. That includes, as Taylor L.J. pointed out in Balabel 'Where information is passed by the solicitor or client to the other as part of the continuum aimed at keeping each other both informed so that advice may be sought and given as required, privilege will attach'.

17. The precise document, or the oral exchange, should be reviewed, not in isolation but in in light of the relevant legal context. This approach was reiterated recently as follows: "In considering whether a document is covered by LAP, the breadth of the concepts of legal advice and continuum of communications must be taken into account"[26] There will always be a problem in the "marginal cases where the answer is not easy,[27]" and where the relevant legal context is not clear.

13.3.2 Litigation privilege

Principle

This privilege[28], which is wider than legal advice privilege since it extends to communications with third parties, protects confidential communications made after litigation has started, or when it is reasonably in prospect, between any of the following:

- a legal professional and a client.
- a legal professional and an agent, whether or not that agent is a legal professional; or
- a legal professional and a third party.[29]

---

called advice consisting as it does of records of the financing of the purchase of, in this case, a house." See *R v Inner London Crown Court ex p. Baines & Baines* [1988] QB 579.

[25] *Balabel v Air India* [1988] 1 Ch 317 Taylor LJ

[26] *CAA v The Queen on the Application of Jet 2.com Limited* [2020] EWCA 35 at para 69

[27] *Three Rivers (No 6) [2004] UKHL 48* per Lord Scott at para 46

[28] In Scotland, the broadly equivalent concept is privilege *post litem motam*.

[29] See e.g., Lord Carswell in *Three Rivers 6*, para 102 [2004] UKHL 48 describing *"communications between parties or their solicitors and third parties"*

- a client and a third party.

These communications must be for the sole or dominant purpose of litigation, for any of the following:

- for seeking or giving advice in relation to it.
- for obtaining evidence to be used in it; or
- for obtaining information leading to obtaining such evidence

13.3.3 Important points to consider across Legal Advice and Litigation Privilege

An original document not brought into existence for these privileged purposes and so not already privileged, very rarely becomes privileged merely by being given to a legal professional for advice or other privileged purpose. See *CAA v R(Jet2.com)* at para100 (vii).

It is important to note that where a communication, although not itself created for the purpose of seeking or providing legal advice, might realistically disclose either the advice sought or given, that communication may nevertheless be privileged: CAA v R (Jet2.com) at para 107. (for example, a summary of legal advice made for a board meeting).

Further, in connection with LAP, where you have a corporate client, communication between you and the employees of a corporate client may not be protected by LPP if the employee cannot be considered to be 'the client' for the purposes of the retainer. As such, some employees will be clients, while others will not. [*Three Rivers District Council v the Governor and Company of the Bank of England (no 5) [2003] QB 1556*] and more recently, *Director of the Serious Fraud Office v Eurasian Natural Resources Corporation Limited* [2018] EWCA Civ 2006. In a corporate context, particularly where in-house lawyers are involved, the privilege attached to a communication between lawyer and client may be inadvertently lost if dissemination occurs internally between a lawyer and those who would not be regarded as 'the client'. This is especially the case where the dissemination is widespread and by e-mail or other forms of electronic communication.

It is not a breach of LPP to discuss a matter with your nominated officer for the purposes of receiving advice on whether to make a disclosure.

13.4 Crime/fraud or iniquity exception

LPP protects advice you give to a client on avoiding committing a crime [*Bullivant v Att-Gen of Victoria [1901]AC 196*] or warning them that proposed actions could attract prosecution [*Butler v Board of Trade [1971] Ch 680*].

LPP does not extend to documents which themselves form part of a criminal or fraudulent act, or communications which take place in order to obtain advice with the intention of carrying out an offence [*R v Cox & Railton (1884) 14 QBD 153*].

The iniquity exception can occur in both a civil context and does not, necessarily, involve the commission of a criminal offence.[30]

For instance, see further examples in *Dubai Aluminium Co Ltd v Al Alawi* [2005] Civ 286 (an attempt to cover up fraud in civil proceedings); *Kuwait Airways Corp v Iraqi Airways Co*

[30] The exception is also engaged where there is an attempt to hide the proceeds of crime.

[2005] EWCA Civ 286 (invented alibi). In BBGP *Managing General Partner Ltd & Brown Global Partners* [2010] EWHC 2176 (Ch), Norris, J stated as follows:

> *"the wrongdoer has gone beyond conduct which merely amounts to a civil wrong: he has indulged in sharp practice, something of an underhand nature where the circumstances required good faith."*

In *Barrowfen v Patel & others* [2020] EWHC 2536 (Ch) the judge[31] stated that

> *"It is well-established that the exception is not confined to crime or fraudulent misrepresentation but extends to fraud "in a relatively wide sense": see Barclays Bank plc v Eustice."*[32]

In *Barrowfen,* alleged breaches of the duties of a director under the Companies Act 2006 came within the iniquity exception,

> "By analogy with BBGP I consider that the iniquity exception is engaged where breaches of sections 172 to 175 and 177 of the Companies Act 2006 are alleged against a director and the allegations involve fraud, dishonesty, bad faith or sharp practice or where the director consciously or deliberately prefers his or her own interests over the interests of the company and does so "under a cloak of secrecy".[33]"

It is irrelevant whether you are aware that you are being used for that purpose [*Banque Keyser Ullman v Skandia [1986] 1 Lloyds Rep 336*].

The crime/fraud exception is, essentially, a negation of LPP rather than an exception to it. LPP simply cannot attach as it is an abuse of the usual professional relationship between lawyer and client.

> *"The deception of the solicitors, and therefore the abuse of the normal solicitor/client relationship, will often be the hallmark of iniquity which negates the privilege."* Popplewell, J *JSC BTA Bank v Ablyazov* [2014] EWHC 2788 (Comm) para 93.

13.4.1 Intention of furthering a criminal purpose

It is not just your client's intention which is relevant for the purpose of ascertaining whether information was communicated for the furtherance of a criminal purpose. It is also sufficient that a third party intends the legal professional/client communication to be made with that purpose (e.g., where the innocent client is being used by a third party) [*R v Central Criminal Court ex p Francis & Francis [1989] 1 AC 346*].

13.4.2 Knowing a transaction constitutes an offence

If you know the transaction that you are working on is a principal offence, you risk committing an offence yourself. In these circumstances, communications relating to such a transaction are not privileged and should be disclosed.

---

[31] See also the comments of Tom Leech QC (sitting as a Chancery Judge) *Barrowfen v Patel & others* [2020] EWHC 2536 (Ch)

[32] *Barrowfen v Patel & others* [2020] EWHC 2536 (Ch) at para 33

[33] *Barrowfen v Patel & others* [2020] EWHC 2536 (Ch) at para 35

13.4.3 Suspecting a transaction constitutes an offence

If you merely suspect a transaction might constitute a money laundering offence, the position is more complex. If the suspicions are correct, communications with the client are not privileged. If the suspicions are unfounded, the communications should remain privileged and are therefore non-disclosable.

If the fraud/crime exception applies, then the exchange cannot be privileged. However, in order to arrive at the fraud/crime exemption, it is necessary to consider the nature of the suspicion. A "vague feeling of unease"[34] or "surmise or conjecture"[35] is insufficient.[36]

13.4.4 Prima facie evidence

If you suspect you are unwittingly being involved by your client in a fraud, the courts require clear evidence before LPP can be displaced [*O'Rourke v Darbishire [1920] AC 581*[37]]. The sufficiency of that evidence depends on the circumstances: it is easier to infer a prima facie case where there is substantial material available to support an inference of fraud. While you may decide yourself if prima facieevidence exists[38], you may also ask the court for directions [*Finers v Miro [1991] 1 W.L.R. 35*].

13.5 Definition of Privileged circumstances – S330 POCA

Quite separately from LPP, POCA recognises another type of communication, one which is received in 'privileged circumstances'. Privileged circumstances under s330 should not be conflated with the common law concept of LPP. Privileged circumstances under s 330 operates merely as an exemption from certain specific provisions of POCA. Although in virtually all cases the communication may also be covered by LPP, it is not necessarily the case. This is, however, a statutory exception with a narrow application It does not have a blanket application.

The privileged circumstances exemptions are found in the following places:

- POCA – section 330 (6)(b), (10) and (11)
- POCA – section 342 (4)
- Terrorism Act – section 19 (5) and (6)
- Terrorism Act – section 21A (8)

Although the wording is not exactly the same in each section, the essential elements of the exemption are:

- you are a professional legal adviser.
- the information or material is communicated to you:

[34] *R v Da Silva* [2006] EWCA Crim 1654
[35] *Bullivant v AG Victoria* [1901] AC 201
[36] [see discussion in Guidance at p xxx]
[37] Longmore, LJ in *Kuwait Airways* commented *that* "Cox and Railton was, of course, a criminal case but it has always been recognised that the fraud exception applies as much to civil cases*, see e.g., O'Rourke v Darbishire [1920] AC 581." Kuwait Airways v Iraqi Airways* [2005] EWCA Civ 286.
[38] The potential for evidential nuance in this area is considerable. See comments in *Addlesee v Dentons (Europe) LLP* [2020] Ch 243

- by your client or their representative in connection with you giving legal advice[39];
- by the client or their representative in connection with them seeking legal advice from you; or
- by any person for the purpose of/in connection with actual or contemplated legal proceedings; and

- the information or material cannot be communicated or given to you with a view to furthering a criminal purpose.

The defence covers 'legal professional advisers' and their employees.

Consider the crime/fraud exception (13.6) when determining what constitutes the furthering of a criminal purpose.

S330(6) operates, essentially, as a defence to the obligation to make a disclosure. Its status is important in the analysis. The section establishes that there is no offence under s 330 if there is a reasonable excuse for failing to make a disclosure. Disclosure is prevented if the material is subject to LPP. Presumably, depending on the facts, failure to interpret s330 correctly could also form a reasonable excuse for failing to make a disclosure under s330(6)(a).

Consequently, given the difficulty in interpretation, it is important to record your decision-making process to rebut any allegation of a failure to make a disclosure under s330. If there is evidence of the formation of a genuine, but mistaken belief that the information was subject to the privileged circumstance exemptions, the legal professional or the professional legal advisor may be able to benefit from the exemption under s 330(6). Originally, s330(6) only applied to legal professionals but has been extended to “relevant professional advisors”. It is important to note, however, that this is a narrow statutory defence and it does not provide any protection in relation to a s327-329 offence.

Finally, section 330(9A) protects the privilege attaching to any disclosure made to a nominated officer for the purposes of obtaining advice about whether a disclosure should be made.

13.6 Differences between privileged circumstances and LPP

The differences between the statutory exception of privileged circumstances under s330(6) POCA and common law LPP have several significant operational ramifications.

13.6.1 Protection of advice

When advice is given or received in circumstances where litigation is neither contemplated nor reasonably in prospect, except in very limited circumstances, communications between you and third parties will not be protected under the advice arm of LPP.

Privileged circumstances, however, exempt communications regarding information communicated by representatives of a client, where it is in connection with you giving legal advice to the client, or the client seeking legal advice from you. This may include communications with:

[39] Note that the 342(4) exception cited above refers to disclosures to clients/third parties, not by them

- a junior employee of a client (if it is reasonable in the circumstances to consider them to be a representative of the client); or
- other professionals who are providing information to you on behalf of the client as part of the transaction.

You should consider the facts of each case when deciding whether or not a person is a representative for the purposes of privileged circumstances. The precise definition of "representative" in this context is, of course, fact sensitive[40].

13.6.2 Losing protection by dissemination

There may be circumstances in which a legal adviser has received information which is subject to legal professional privilege, but which does not fall within the definition of privileged circumstances.

There are occasions in which a lawyer may, whilst retained to represent client A, hold information that is privileged as between client B and their own lawyer. There are occasions in which such information is shared subject to a contractual provision that LPP is not waived. (*Gotha City v Sotheby's (no1)* [1998] 1 WLR 114).

In such circumstances, the legal professional representing client A would not be able to rely on privileged circumstances, but the information might still be subject to LPP, unless the crime/fraud exemption applies.

13.7 The Tension between LPP and Disclosure Obligations under POCA

As indicated above, the fundamental principles of LPP[41] refer to its "absolute" status. Lord Taylor, in *R v Derby Magistrates* stated, *"I am of the opinion that no exception should be allowed to the absolute nature of legal professional privilege, once established."*[42]

There can be complexity in applying LPP its status as a long-established concept backed by a substantial body of case law was highlighted in *R v Derby Magistrates*. Furthermore, although lawyers have disclosure obligations under a number of regimes, it is important to ensure that LPP is respected in relation to all of those regimes.

There is a tension between the disclosure obligations under POCA and the all-encompassing duties of client confidentiality and the duty to protect LPP in connection in circumstances in which there is, unusually, a question as to whether LPP has been established or whether there is an operative exception, such as the iniquity exception, discussed above Further, the burden of making the decision falls on the lawyer with the potential for both regulatory and criminal sanction should the lawyer make the wrong decision. If the lawyer discloses, without good reason, there is a breach of client confidentiality and LPP and a potential claim in damages as well as a small prospect of regulatory sanction. Conversely, a failure to disclose may result in criminal sanction against the lawyer under POCA.

---

[40] see Cotton LJ in *Wheeler v Le Marchant* (1881) 17 Ch.D. 675 at pages 684-5. The judgment is quoted in *Three Rivers 5* [2003] EWCA Civ 474 at para 18 on the meaning of 'representative' in the broader LPP context.

[41] See the comments of Lord Taylor in *R v Derby Magistrates* [1995] UKHL 18 at para 58 *"The principle which runs through all these cases, and the many other cases which were cited, is that a man must be able to consult his lawyer in confidence, since otherwise he might hold back half the truth. The client must be sure that what he tells his lawyer in confidence will never be revealed without his consent. Legal professional privilege is thus much more than an ordinary rule of evidence, limited in its application to the facts of a particular case. It is a fundamental condition on which the administration of justice as a whole rests".*

[42] Lord Taylor in *R v Derby Magistrates* [1995] UKHL 18 at para 65

What follows is a discussion of the tension between the disclosure obligations under POCA and the operation of LPP. It is important, however, not to overstate the nature of such tension, which may only be present in a relatively limited number of cases at the margins.

The first problem for the lawyer is structural. The POCA and its disclosure obligations, is, in large part, based on a financial services framework in which there is a duty of confidentiality but not LPP. LPP brings an added tension to the analysis. It is a tension recognised by the Financial Action Task Force (FATF) as, despite the clarity of a first principles approach, the application of LPP in marginal cases is far from clear.

> *"There may be cases in which these professionals conduct activities that are clearly covered by the legal privilege (i.e., ascertaining the legal position of their client or defending or representing their client in judicial proceedings) alongside activities that are not covered by it. In addition, within a single matter, privilege may attach to some but not all communications and advice."*[43]

The second problem relates to the definition and application of common law LPP which is complex in itself. The decision to disclose is made in a context in which the case law surrounding common law concepts of the nature of legal advice and assistance, relevant legal context, dominant purpose, even the definition of the client, are nuanced.[44] The statutory definition of "privileged circumstances" in s 330(6) POCA is narrow but easy to conflate with LPP. The concept of "suspicion" which triggers the consideration of LPP is problematic; what, exactly is an "irresistible inference" that there is sufficient, perhaps circumstantial evidence, that a suspicion has been triggered[45] The court in *Da Silva* recognised this problem when it stated that

> *"the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice*.[46]

On a practical basis, there is little consideration in the case law of the decision-making process of the lawyer in deciding whether information is, or is not, subject to LPP or provided in privileged circumstances. A stable protocol or framework is of importance to the lawyer who may have to defend their analysis at a future date.

Thirdly, the duty to consider LPP in the context of AML reporting obligations is active rather than passive. The structure of the legislation (a reporting obligation and subject to an exception or an operative defence) points to a need actively to consider whether LPP applies, rather than simply assume that it must do so. This active consideration was highlighted in a commentary on LPP and professional secrecy by FATF, which stated:

"In situations where legal professionals are claiming legal professional privilege or professional secrecy, they must be satisfied that the information is protected by the privilege/professional secrecy and the relevant rules."[47]

---

[43] *FATF Guidance for A Risk Based Approach: Legal Professionals* (June 2019) p10

[44] *"…. Legal professional privilege is an established concept. As a non-lawyer, I accept that it is a complicated issue. However, professional legal advisers ought to know whether legal privilege applies; indeed, if they do not, there are people whom they can consult."* Lord Rooker HL Deb 27 May 2002 vol 635 c1087

[45] The term "irresistible inference" as used in *R v Anwoir* [2008] EWCA Crim 1354 in the context of criminal property,

[46] Per Longmore, LJ, *R v Da Silva* [2006] EWCA Crim 1654 at para 16, This decision turned on the interpretation of "suspicion" for the purposes of 93A(1)(a) of the Criminal Justice Act 1988. There is no material difference between the concepts for the purposes of the interpretation of suspicion under POCA,

[47] *FATF Guidance for A Risk Based Approach: Legal Professionals* (June 2019) p11

The duty is discharged by active engagement with the question of when LPP applies and the extent to which there is enough information for the lawyer to be satisfied that it may properly be asserted. Therefore, there must be some tangible evidence that this analysis has been done. It is helpful to record that analysis, but care is required as to circulation and storage of the record to avoid the potential for subsequent unintended disclosure.

Finally, there is a lack of clarity as to whether a genuine, but mistaken belief that LPP applies in a particular circumstance could form a "reasonable excuse" defence[48] in the event of action against the lawyer for failure to make either a required[49] or an authorised disclosure.[50.]

13.8 When do I disclose? – Documenting the decision-making process

The following approach is intended to support the decision-making process and to provide evidence of the lawyer's active engagement with the issue of whether or not to make a disclosure under POCA.

Given the conceptual and operational challenges involved in the decision as to whether to disclose, it is possible only to design a high-level decision-making protocol to support legal professionals through this process, based on an analysis of the case law and available evidence, Each case will turn on its own facts and merits, and it is not possible to be prescriptive. However

1) *What is the nature of the Retainer or Client Engagement?*

In order to determine the question of whether an exchange or document is subject to LPP, it is important to define the precise nature of the engagement or retainer between the legal professional and the client. This forms the first step in the assessment process as to whether a document or conversation is subject to legal professional privilege.[51]

Although not conclusive, the written retainer, and any variation, should provide an indication as to the relevant legal context in which legal advice and assistance is to be given. It should provide clarity as to the identity of the client and the focus of the work in a schedule or annex. Computerised time recording work activity codes, if sufficiently granular, may also provide useful evidence of the way in which the work generated.

2) *Is the claim to LPP based on statute or the common law?*

The precise ambit of the claim to LPP is determined either by the application of common law principles outlined throughout this chapter in the case of solicitors and barristers [and Chartered Legal Executives], by statutory extension for patent attorneys,[52] registered trademark attorneys[53] and licensed conveyancers[54]. The claim to privilege by statutory extension is limited to the activities and context set out in the relevant statute. For most lawyers, the claim will be based on the common law, but there are statutory extensions to some legal professionals. In addition, could there be a claim to "privileged circumstances" under s 330 on a coextensive or independent basis? Note, also, the right of the client to the

---

[48] Law Commission Anti-*money laundering: the SARs regime* (Law Com No 384, 2019)

[49] POCA ss 330, 331 and 332

[50] POCA s327(2)(b), 328, 329(b)

[51] A retainer letter was considered in the context of a claim to LPP in *SAAB v Dangate & Others* [2019] EWHC 1558 at para 217 by way of example. See also commentary on the interplay between retainer letters and LLP obligations in AML/CTF context by Jonathan Fisher QC "Legal Privilege, Reporting Suspicions, and Retainer Letters" Blog Post Friday, 13 April 2018 https://brightlinelaw.co.uk/

[52] CDPA 1988

[53] TMA 1994

[54] LSA 2007 s 190

protection of LPP is also a fundamental human right both at common law and under Article 6 (right to a fair trial) and Article 8 (respect for family and private life) under the European Convention on Human Rights (ECHR).

3) Are the LPP tests satisfied?

Are all elements of either "branch" of LPP fulfilled (legal advice or litigation) relation to the document or exchange being considered?[55] Does the analysis link to the original retainer? Has there been any development in the retainer to the extent that the document or discussion may fall outside the broad protection of LPP and be disclosable? What is the brief or role of the lawyer, beyond the strict definition of the retainer, and the nature of the "relevant legal context" in which the "continuum of communication" has taken place? Furthermore, despite the variation of the retainer, express or implied, is the relevant material nevertheless subject to LPP in a manner not envisaged by the original retainer. Is LPP applicable at all (e.g., is there prima facie evidence of furtherance of crime, fraud or any other conduct capable of satisfying the crime/fraud exception?

(4) Is this a "marginal case" that requires additional scrutiny?[56] If, so activate a "marginal case" protocol

In the vast majority of cases, the position will be clear. There will, however, be marginal cases, especially in transactional work. If so, would an additional view from another lawyer (or counsel) be of assistance. It may also be possible to use s330 (9A) in some circumstances to obtain advice from the MLRO without making a disclosure under POCA.

Record the rationale for any decision. – this will provide evidence of the decision-making process and may, in addition, assist in any consideration of a reasonable excuse defence in the future.

You may find it helpful to complete the template/questionnaire set out below to record the decision-making process.

13.8.1 Decision Template

Question	**Answer**	**Evidence**
What are the **specific terms of your retainer/terms of engagement with the client**? What have you been asked to do for your client?		

[55] *CAA v The Queen on the Application of Jet 2.com Limited* [2020] EWCA 35 at para 69 and the comments of Hickinbottom, L.J., on the application of LAP.

[56] The concept of the "marginal case" which may pose additional problems is recognised in *Three Rivers (No 6)* and, by implication in several guidance notes from FATF. It may also be important in the context of any defence or exception under POCA for the lawyer, or of "reasonable excuse" more generally.

Has the retainer been varied at any stage? Was the variation express or implied?		
How has the retainer developed? What is the nature of the **"relevant legal context"** and the **"continuum of communication"** in relation to the document or conversation?		
What are the specific requirements set out in your **Rules of Professional Conduct** relating to your **professional obligations** relating to **confidential information** and **LPP. Is the right of the client to LPP based on the common law or statute?**		
Is the exchange or the material **confidential**? If so, why?		
On your analysis, does a **particular type of LPP (legal advice or litigation) apply?** If so, why?		
Why do you believe that a **disclosure obligation** may have arisen under the AML legislation?		
Do you have knowledge of/formed a suspicion relating to ML? What is the precise nature of the suspicion? Is there a reasonable basis for the suspicion? Review the relevant test, such as , *R v Da*		

Silva [2006] and *R v Anwoir* [2008]		
Has your **client agreed to waive LPP** in this exchange or document to make a joint disclosure?		
If your client has not agreed to waive privilege, **which exemption applies to displace** the primary duty to uphold **client confidentiality and LPP (statutory abrogation or the crime/fraud exception).**		
Is this a case in which the **"privileged circumstance" exception** applies under s330(6) POCA? Does common law LPP also apply?		
Based on the answers to the questions set out above, is this a **"marginal case"** or is the position unclear for any other reason.		
DECISION 1 **COMMUNICATION IS COVERED BY LPP**	Crime/fraud exception does not apply/no statutory abrogation and cannot make a disclosure without a breach of (i) retainer and (ii) Code of Conduct set out above	Note of retainer and Code.
DECISION 2 **COMMUNICATION RECEIVED IN "PRIVILEGED CIRCUMSTANCES" within POCA**	Crime/fraud exception does not apply/no statutory abrogation and cannot make a disclosure without a breach of (i) retainer and (ii) Code of Conduct set out above. You are exempt from making a disclosure to the NCA.	Note of retainer and Code.

DECISION 3: **COMMUNICATION NOT PRIVILEGED BUT CONFIDENTIAL**	If disclosable under POCA and not covered by LPP, disclosure can be made to avoid a breach of s330.	
DECISION 4: **MARGINAL CASE**	A marginal case could turn in a definitional issue regarding the nature of the document or other communication. Review with MLRO and/or external counsel.	

13.8.2 Summary

If the communication is covered by LPP and the crime/fraud exception does not apply, you cannot make a disclosure under POCA.

If the communication was received in privileged circumstances and the crime/fraud exception does not apply, you are exempt from the relevant provisions of POCA, which includes making a disclosure under POCA

If neither of these situations applies, the communication will may still be confidential. However, the material is disclosable under POCA and can be disclosed, whether as an authorised disclosure, or to avoid breaching section 330. Sections 337 [in force] and 339ZF of POCA permit you to make such a disclosure and provides that you will not be in breach of your professional duty of confidentiality when you do so.

14. Civil Liability

14.1 Introduction

This section considers the relationship between the anti-money laundering regime and potential civil claims in two contexts:

1. The victim of financial crime seeks to recover property through the civil justice system by claiming constructive trusteeship.
2. A client seeks a civil remedy when you have made a required or authorised disclosure under the Proceeds of Crime Act (2002) or 'POCA' or the Terrorism Act, 2000 or 'TACT' i.e., a Suspicious Activity Report (SAR).

14.2 Constructive Trusteeship

You should note that POCA is silent on the issue of compensation for victims. Its aim is to deprive criminals of the benefits of financial crime. Although the Court may order compensation where confiscation proceedings are brought under POCA Part 2, civil law allows victims to make a claim of constructive trusteeship.[57]

Liability for constructive trusteeship could arise from:

- **Knowing receipt:** your interference with trust property or property subject to a fiduciary duty; or
- **Knowing (or dishonest) assistance:** your involvement in a breach of a fiduciary or trust duty.

If you are a constructive trustee, you have a personal liability to account for the value of the property received or the loss resulting from assistance with a breach of trust or fiduciary duty (Lord Millett in *Dubai Aluminium Co Ltd v Salaam* [2002] 3 WLR 1913).

This guidance applies to the law of trusts in England, Wales and Northern Ireland. The recognition of the concept of a constructive trust under Scottish Law is less likely. For further information see paragraphs 2.1-2.8 of the Scottish Law Commission Report on Trust Law (2014).

14.3 Knowing Receipt

Liability for knowing receipt occurs where a person:

a) Receives property in which the claimant has an equitable proprietary interest and the property is received:
   i. In breach of trust; or
   ii. In breach of a fiduciary duty; or
   iii. Legitimately, but then misapplied; and
b) Contrary to that trust or duty, applies the property for their own use and benefit; and
c) The person is at fault.

For example, receiving funds that you apply for your own fees could amount to knowing receipt. However, receiving money as an agent or into the client account as trustee of a bare trust will not amount to knowing receipt as the funds are not received or applied for your own use and/or benefit.

[57] A victim may target a professional advisor in a civil claim as they may be more likely to be able to pay. If you believe that you may have acted as a constructive trustee, you should seek legal advice.

What amounts to fault in this context is not clear. However, the Court of Appeal in *BCCI v Akinele* [2001] Ch. 437 held that the test is whether you have acted unconscionably. The test is subjective and includes actual knowledge and wilful blindness. In that case, the Court stated that:

- You need not have acted dishonestly; it is enough to know that a fiduciary or trust duty has been breached; and
- Your knowledge of the origin of the funds should be such that it was unconscionable for you to retain any benefit.

14.4 Knowing Assistance

You will be personally liable for damages and loss caused if you knowingly assist in a breach of fiduciary or trust duties (*Twinsectra v Yardley* [2002] WLR 802).

The breach does not need to be fraudulent (*Royal Brunei Airlines v Tan* [1995] 2 AC 378) and you do not need to know full details of the trust arrangements or obligations of the trustee/fiduciary. You must:

- Know that the person who you are assisting is not entitled to do what they are doing; or
- Have sufficient grounds to suspect that they are not entitled to do what they are doing.

Knowing assistance also requires that you act dishonestly. The Court of Appeal in Group Seven Ltd & Rheingold Management Incorporated v. (1) Notable Services LLP and (2) Martin Landman [2019] EWCA Civ 614, states that the test of whether your conduct is dishonest is the same test as in the case of Ivey.

The Court stated:

“In the light of Ivey, it must in our view now be treated as settled law that the touchstone of accessory liability for breach of trust or fiduciary duty is indeed dishonesty, as Lord Nicholls so clearly explained in Tan, and that there is no room in the application of that test for the now discredited subjective second limb of the Ghosh test. That is not to say, of course, that the subjective knowledge and state of mind of the defendant are unimportant. On the contrary, the defendant’s actual state of knowledge and belief as to relevant facts forms a crucial part of the first stage of the test of dishonesty set out in Tan. But once the relevant facts have been ascertained, including the defendant’s state of knowledge or belief as to the facts, the standard of appraisal which must then be applied to those facts is a purely objective one. The court has to ask itself what is essentially a jury question: namely whether the defendant’s conduct was honest according to the standards of ordinary decent people”

14.5 Civil Liability and Disclosures to the National Crime Agency (NCA)

14.5.1 While waiting for consent

A client may seek a court order for the return of funds on the basis that you are breaching their retainer.

Case law does not provide a direct authority in this situation, but a ruling by the Court of Appeal[58] relating to banks' obligations may indicate the obligations a court might place on legal professionals. That case held:

a) A bank's contract with the client was suspended while the moratorium period was in place, so the customer had no right to an injunction for the return of monies.
b) As a matter of discretion, the court would not force the bank to commit a crime.
c) The bank could provide a letter to the court as evidence of its suspicion.[59]

14.5.2 Where an application for extending the moratorium period has been made

The period during which a client's funds are unable to be returned to them has been extended by the introduction of extended moratorium periods under the Criminal Finances Act 2017. Where an application to extend is being considered, s333D (other permitted disclosures) might provide a limited exception to the tipping off provisions. Where an application is made to extend the moratorium period under s336A a person does not commit an offence under s333D where:

- The disclosure is made to a customer or a client of the person;
- The customer or client appears to the person making the disclosure to have an interest in the relevant property; and
- The disclosure contains only such information as is necessary for the purposes of notifying the customer or client that the application under 336A has been made.

For more information see the Home Office Circular 008/2018: Criminal Finances Act: extending the moratorium period for suspicious activity reports.

14.5.3 Where the NCA has granted consent (DAML)

Obtaining consent will not necessarily protect you from liability for breach of constructive trust. Where you continue with a transaction you must show:

- Although you had sufficient suspicion to justify disclosure to the NCA, your concerns were not such as to render them accountable on a constructive trustee basis. A court will likely consider that you generally operate in the regulated sector, have an adequate level of awareness and training relating to money laundering, and that you are able to account for decisions to proceed with a transaction; or
- Your suspicions were reduced or removed by subsequent information or investigation.

---

[58] *K Ltd v National Westminster Bank Plc & Ors* [2006] EWCA Civ 1039.

[59] Provision of evidence in these circumstances was permitted under repealed POCA s. 333(2)(b) which provided an exception to the tipping off offences. A similar provision is now found in s. 333D(2).

14.6 Civil liability & SARs

S338(4A) of POCA sets out: “where an authorised disclosure is made in good faith, no civil liability arises in respect of the disclosure on the part of the person by or on whose behalf it is made.”

However, there may be circumstances in which a court will order inspection of a SAR in civil proceedings.

In *Lonsdale v National Westminster Bank* [2018] EWHC 2843 the court considered that an individual may have rights to access a SAR under the Civil Procedure Rules where necessary for the fair disposal of proceedings.

15. Supervision

15.1 General comments

Breaches of obligations under the regulations and other relevant legislation are subject to disciplinary sanctions and criminal penalties.

Law enforcement agencies have the power to take action in relation to breaches of the Regulations, and particularly cases of money laundering and/or terrorist financing. While they may choose to pursue any breach which they may become aware of, their resources are not infinite, and they may prioritise some matters over others.

Though some Anti- Money Laundering (AML) supervisors may have the power to prosecute some matters (e.g., HMRC), Professional Body Supervisors (PBSs), like the members of LSAG generally do not. They use their own rule setting and enforcement powers to enforce compliance with the AML regulations.

Supervisors work closely with regulated practices to encourage compliance and increase understanding of how to effectively mitigate risks.

The possible sanctions for a failure to comply are serious, and supervisory bodies will take appropriate action against non-compliance.

Each supervisor will take a risk-based approach to the supervision of their population, but the Office for Professional Body AML Supervision (OPBAS) acts to ensure a level of consistency across the PBSs. You should consult with your supervisor in order to understand their approach to supervision of your practice and enforcement of the Regulations and have regard to any guidance they may publish.

15.2 Legal Sector Supervisors

The named supervisory authorities for the legal sector are:

- the Chartered Institute of Legal Executives.
- the Council for Licensed Conveyancers.
- the Faculty of Advocates.
- the Faculty Office of the Archbishop of Canterbury.
- the General Council of the Bar.
- the General Council of the Bar of Northern Ireland.
- the Law Society of England and Wales.
- the Law Society of Northern Ireland; and
- the Law Society of Scotland.

The supervisory authority listed in the Regulations for solicitors in England and Wales is the Law Society of England and Wales. This responsibility has been delegated to the Solicitors Regulation Authority (SRA).

The General Council of the Bar is the named supervisory authority for the Bar of England and Wales. It discharges its regulatory functions through the Bar Standards Board.
The Chartered Institute of Legal Executives is the named supervisory authority listed in the Regulations for legal executives in England and Wales. It delegates its regulatory functions to, and they are discharged by CILEx Regulation.

15.3 Other supervisors

Other supervisory authorities may be of relevance to some legal professionals and include:

- The Financial Conduct Authority;
- Her Majesty's Revenue and Customs;
- Association of Accounting Technicians;
- Association of Chartered Certified Accountants;
- Association of International Accountants;
- Association of Taxation Technicians;
- Chartered Institute of Management Accountants;
- Chartered Institute of Taxation;
- Faculty Office of the Archbishop of Canterbury;
- Insolvency Practitioners Association;
- Institute of Certified Bookkeepers;
- Institute of Chartered Accountants in England and Wales;
- Institute of Chartered Accountants in Ireland;
- Institute of Chartered Accountants of Scotland;
- Institute of Financial Accountants; and
- International Association of Bookkeepers.

Occasionally there may be overlap between Legal and other supervisors particularly with Accountancy supervisors, so it is important to understand what activities your practice provides that are regulated and who supervises such activities. It is also important to ensure that you are not providing services without supervision of all activities in scope of the Regulations.

Where a there is a supervisory overlap and a supervisory authority reaches agreement with another supervisor about which is to supervise the legal professional or practice, this agreement will be made known to the legal professional/practice in accordance with R7(3).

In all other cases of supervisory overlap, and where you have questions about AML supervision, you should contact your supervisory authority in the first instance.

15.4 Supervision under the Regulations

R7 sets out the supervisory authorities for the regulated sectors. Where a person in one or more regulated sectors is covered by more than one supervisory authority, either the supervisory authorities may decide between them who is to be the sole supervisor of the person, or they must co-operate in the performance of their duties.

A supervisory authority must:

- identify and assess the international and domestic risks of money laundering and terrorist financing to which its sector is subject.
- monitor effectively the persons it is responsible for.
- take necessary measures to ensure those persons comply with the requirements of the Regulations.
- comply with its obligations under R46(2), which include:

    - adopting a risk-based approach to supervision.
    - ensuring its employees and officers have access to information on money laundering and terrorist financing risks.
    - basing the frequency and intensity of its supervisory activities on the risk profiles it has prepared for its sector.
    - keeping a record of its supervisory actions and reasons for not acting in a particular case; and
    - taking effective measures to encourage its sector to report potential breaches of the Regulations.
- take appropriate measures, in accordance with a risk-based approach, to review practices' risk assessments and policies, controls and procedures.
- report to the NCA any suspicion that a person or practice it is responsible for has engaged in money laundering or terrorist financing.
- make up to date information on money laundering and terrorist financing available to those it supervises.
- co-operate and co-ordinate their activities with other supervisory authorities, HM Treasury and law enforcement authorities; and
- collect certain information about the practices it supervises, and any other information it considers necessary for exercising its supervisory functions.

15.5 Additional Requirements for Supervisors

As a part of the Regulations as amended, a supervisor must also:

- Ensure that the requirements of R26(7) are met by applicants, whether they are a relevant person or not (i.e., whether there is an underlying non-AML regulatory relationship or not);
- Provide a secure reporting channel for people to report potential breaches to it, ensuring the identity of the reporting person is known only to them; and
- Publish an annual report that contains information on
    - measures taken to encourage reporting of actual or potential breaches.
    - number of reports of actual or potential breaches received; and
    - number and description of measures carried out to monitor compliance with the MLR, POCA and TACT.

R49(1)(d) also requires that potential conflicts of interest within the organisation are appropriately handled e.g., via a functional separation of activity areas where appropriate. This is particularly relevant for organisations that have both a representative and supervisory function.

15.6 Enforcement powers under the Regulations

Part 8 of the Regulations gives supervisory authorities a variety of powers for performing their functions under the Regulations.
The powers are:

- R66 power to require information from, and attendance of, relevant and connected persons without a warrant; and
- R71 power to retain documents taken under Regulation 66.

In addition, Part 9 of the Regulations gives the FCA and HMRC powers to impose civil penalties, prohibit an individual from having a management role within a relevant person

and/or seek an injunction restraining the contravention of a relevant requirement under the Regulations.

15.7 Disciplinary action against legal professionals

Conduct which fails to comply with AML/CTF obligations may also be a breach of your professional obligations, for which a supervisor may have additional powers to those mentioned in the above.

Generally speaking, if you are not compliant with the law (i.e., in this instance the Regulations, POCA and TACT) you are likely to be in breach of your regulatory requirements to your supervisor. Often where a supervisor undertakes enforcement action against a practice, it is their own regulatory powers they will use, rather than a power listed in the Regulations.
Contact your supervisor for further information on their approach to AML enforcement.

15.8 Regulations - relevant offences and penalties

Schedule 6 lists a number of relevant requirements, the breach of which is an offence. In addition to the offence of breaching a relevant requirement, the Regulations contain offences of prejudicing investigations and disclosure offences.

15.8.1 Breach of a relevant requirement

The relevant requirements in Schedule 6 that are most likely to be applicable to legal professionals are those imposed under the Regulations listed in the table below.

Regulation	Requirement
18	Risk assessment by a relevant person
19	Policies, controls and procedures
20	Policies, controls and procedures (group level)
21	Internal controls
23	Requirement on authorised persons to inform the FCA
24	Training
25	Directions to a parent organisation from a supervisory authority
26	Acting as a beneficial owner, officer or manager without approval
27	Application of CDD measures
28	Application of CDD measures
30	Timing of verification
31(1)	Requirement to cease transactions where unable to apply CDD measures required by Regulation 28
33(1) and	Obligation to apply enhanced due diligence
(4)-(6)	Enhanced due diligence: politically exposed
35	persons
37	Application of simplified due diligence
39(2) and (4)	Reliance
40(1) and (5)-(7)	Record keeping
41	Data protection
43	Corporate bodies: obligations
44	Trustee obligations
45(2) and (9)	Register of beneficial ownership
56(1) and (5)	Requirement to be registered
57(1) and (4)	Applications for registration
66	Power to require information
69(2)	Entry and inspection without a warrant
70(7)	Entry of premises under warrant
77(2) and (6)	Power to impose civil penalties, suspension and removal of authorisation
78(2) and (5)	Prohibitions

Relevant requirements for which summary conviction may carry a fine and indictment may carry a 2-year custodial or a fine or both

15.8.2 Offence of prejudicing investigations

Under R87 a person commits the offence of prejudicing an investigation if they know or suspect that an officer or proper person is acting in connection with an investigation which is being, or is about to be, conducted, and they:

- make a disclosure which is likely to prejudice the investigation;
- conceal, destroy or dispose of documents relevant to an investigation; or
- cause or permit the falsification, concealment, destruction or disposal of documents relevant to an investigation.

It is not an offence if:

- The person did not know or suspect that the disclosure is likely to prejudice the investigation.
- The disclosure is made in the exercise of a function under, or in compliance with a requirement imposed by, the Regulations, TACT, POCA or any Act relating to criminal conduct or benefit from criminal conduct; or
- The person is a professional legal adviser, and the disclosure is to a client in connection with the giving of legal advice or to any person in connection with legal proceedings or contemplated legal proceedings.

The penalty for an offence under Regulation 87 is:

- On summary conviction:
    - In England or Wales, a fine or a term of imprisonment not exceeding three months or both; and
    - In Scotland or Northern Ireland, a term of imprisonment not exceeding three months, fine not exceeding the statutory maximum or both; and
- On conviction on indictment: a term of imprisonment not exceeding two years or a fine or both.

15.8.3 Information offences

Under R88(1) a person commits an offence if, in supposed compliance with a requirement imposed on them under the Regulations, they knowingly or recklessly make a statement which is false or misleading to a relevant issue.

The penalty for an offence under R88(1) is:

- On summary conviction:
    - In England or Wales, a fine or a term of imprisonment not exceeding three months or both; and
    - In Scotland or Northern Ireland, a term of imprisonment not exceeding three months, a fine not exceeding the statutory maximum or both;
- On conviction on indictment: a term of imprisonment not exceeding two years or a fine or both.

Under R88(3), it is an offence to disclose information in contravention of a relevant requirement. It is a defence for the person to prove that they reasonably believed the disclosure was lawful or that the information had already lawfully been made publicly available.

The penalty for an offence under R88(3) is:

- On summary conviction:
    - In England or Wales, a fine or a term of imprisonment not exceeding three months or both;
    - In Scotland or Northern Ireland, a term of imprisonment not exceeding three months, a fine not exceeding the statutory maximum or both; or
- On conviction on indictment: a term of imprisonment not exceeding two years or a fine or both.

15.9 Joint liability

Offences under the Regulations can be committed by a practice as a whole, whether it is a body corporate, partnership or unincorporated association. However, if it can be shown that the offence was committed with the consent, contrivance or neglect of an officer, partner or member, then both the practice and the individual can be jointly liable.

15.10 Prosecution authorities

The Crown Prosecution Service is a prosecuting authority for offences under POCA, the Terrorism Act and the Regulations.

The Crown Office and Procurator Fiscal Service is a prosecuting authority for offences under POCA, the Terrorism Act and the Regulations.

The Director of Public Prosecutions for Northern Ireland is a prosecuting authority for offences under POCA, the Terrorism Act and the Regulations.

The Revenue and Customs Prosecutions Office is a prosecuting authority for offences under POCA and the Regulations.

The FCA is a prosecuting authority under POCA and the Regulations as a result of section 402 of the Financial Services and Markets Act 2000.

16. Money Laundering Offences

16.1 General overview

Part 7 of the Proceeds of Crime Act 2002 (POCA) is applicable throughout the UK. It creates both a set of substantive money laundering offences (principal offences) and a reporting regime that makes it an offence to fail to disclose knowledge or suspicion of money laundering (failure to disclose offences).

By virtue of the definition of 'criminal property' both **the principal offences and the disclosure obligations apply to the proceeds of all crimes.**

POCA s340(3) states:

Property is criminal property if

- it constitutes a person's benefit from criminal conduct, or it represents such a benefit (in whole or part and whether directly or indirectly); and
- the alleged offender knows or suspects that it constitutes or represents such a benefit.

16.2 Application

POCA applies to all persons (and therefore all legal professionals), although some offences apply only to persons within the regulated sector or to MLROs. The principal money laundering offences under POCA apply to money laundering activity which occurred on or after 24 February 2003. The failure to disclose provisions in s330, s331 and s332 apply where the information on which the knowledge or suspicion is based came to a person on or after that date. In other cases, the previous law applies.

16.3 Principal money laundering offences

16.3.1 General comments

Money laundering offences assume that a prior criminal offence has occurred, generating the criminal property being laundered. The underlying criminality is often known as a "predicate offence." No conviction for the predicate offence is necessary for a person to be prosecuted for a money laundering offence. Under POCA it does not matter where in the world the predicate offence took place, provided it would have constituted an offence if it had occurred in the UK (see also section 6.9).

Be aware that it is also an offence to conspire, incite or attempt to launder the proceeds of crime, or to counsel, aid, abet or procure money laundering.

16.3.2 Section 327 – concealing etc

A person commits an offence if he or she conceals, disguises, converts, or transfers criminal property, or removes criminal property from the UK.
Concealing or disguising criminal property is extremely wide in nature, and includes concealing or disguising its nature, source, location, disposition, movement, ownership or any rights connected with it, and therefore covers a wide range of activities – including mixing criminal funds with legitimate cash flows. The deliberate non-disclosure of facts has also been found to amount to a concealment offence (Clark vs Escanda, 1984).

16.3.3 Section 328 - Arrangements

A person commits an offence if they enter into an arrangement or become concerned in an arrangement which they know or suspect facilitates the acquisition, retention, use or control of criminal property by, or on behalf of another person. Commercial arrangements and professional services are clearly included in this. Examples include transferring ownership of assets/property, the conversion of asset type, or the movement of criminally derived value from one jurisdiction to another

16.3.4 What is an arrangement?

An arrangement is not defined in Part 7 of POCA. The arrangement must exist and have practical effects relating to the acquisition, retention, use or control of property.

There must be a meeting of minds.

Arrangement 'bears the meaning that an ordinary educated man would ascribe to it'. It involves a meeting of the minds and mutuality such that each party would consider itself under a legal or moral obligation to do or not do a certain thing.
Agreement requires that 'parties to it should have communicated with one another … and that as a result … each has intentionally aroused in the other an expectation that he will act in a certain way.' (Diplock LJ Re British Basics Slags Ltd Agreements (1963))

16.3.5 Entering into or becoming concerned in an arrangement

To enter into an arrangement is to become a party to it.

To become concerned in an arrangement suggests a wider practical involvement such as taking steps to put the arrangement into effect.

Both 'entering into', and 'becoming concerned in', describe an act that is the starting point of an involvement in an existing arrangement.

Although the Court did not directly consider the conduct of transactional work, its approach to what constitutes an arrangement under s328 provides some assistance in interpreting how that section applies in those circumstances.

Bowman v Fels (2005) EWCA Civ 226 supports a specific understanding of the concept of entering into or becoming concerned in an arrangement, with respect to transactional work.

In particular:

- entering into or becoming concerned in an arrangement involves an act done at a particular time;

- an offence is only committed once the arrangement is actually made; and
- preparatory or intermediate steps in transactional work which does not itself involve the acquisition, retention, use or control of property will not constitute the making of an arrangement under s328.

If you are doing transactional work and become suspicious, you have to consider:

- whether an arrangement exists and, if so, whether you have entered into or become concerned in it or may do so in the future; or
- if no arrangement exists, whether one may come into existence in the future which you may become concerned in.

16.3.6 What is not an arrangement?

Bowman v Fels (2005) EWCA Civ 226 held that s328 does not cover or affect the ordinary conduct of litigation by legal professionals, including any step taken in litigation from the issue of proceedings and the securing of injunctive relief or a freezing order up to its final disposal by judgment.

Dividing assets in accordance with a judgment, including the handling of the assets which are criminal property, is not an arrangement. Settlements, negotiations, out of court settlements, alternative dispute resolution and tribunal representation are also not arrangements. However, the property will generally still remain criminal property and you may need to consider referring your client for specialist advice regarding possible offences they may commit once they come into possession of the property after completion of the settlement.

A victim of an acquisitive offence who is recovering their property will not be committing an offence under either s328 or s329 of the Act. However, if there is an agreement e.g.in an insolvency scenario, whereby a victim agrees to accept a lower percentage in full settlement of a claim, you may still need to consider s328.

16.3.7 Sham litigation

Sham litigation created for the purposes of money laundering remains relevant to s328. Shams arise where an acquisitive criminal offence is committed, and settlement negotiations or litigation are intentionally fabricated to launder the proceeds of that separate crime.

A sham can also arise if a whole claim or category of loss is fabricated to launder the criminal property. In this case, money laundering for the purposes of POCA cannot occur until after execution of the judgment or completion of the settlement.

16.3.8 Section 329 - acquisition, use or possession

A person commits an offence if he or she acquires, uses or has possession of criminal property with the requisite mental element, discussed below.

16.4 Defences to principal money laundering offences

You will have a defence to a principal money laundering offence if:

- you make an authorised disclosure prior to the offence being committed and you gain appropriate consent/DAML (the consent defence);

- In relation to s329 you will also have a defence if you received adequate consideration for the criminal property (the adequate consideration defence); or
- you intended to make an authorised disclosure but had a reasonable excuse for not doing so (the reasonable excuse defence).

16.4.1 Defence against money laundering (consent defence)

S338 authorises you to make a disclosure as a means of requesting consent for otherwise prohibited acts.

It specifically provides that you can make an authorised disclosure either

- before money laundering has occurred;
- while it is occurring but as soon as you suspect; or
- after it has occurred, if you had good reason for not disclosing earlier and make the disclosure as soon as practicable.

If a disclosure is an authorised disclosure made under section 338 and in good faith, it does not breach any rule which would otherwise restrict it, including professional regulatory requirements relating to confidentiality.
Where your practice has a MLRO, you should make your disclosure to the MLRO. The MLRO will consider your disclosure and decide whether to make an external disclosure to the NCA. If your practice does not have a MLRO, you should make your disclosure directly to the NCA (see Section 11 of this guidance).

If you have a suspicion that a retainer you are acting in will involve dealing with criminal property, you can make an authorised disclosure to the NCA via your MLRO and seek a DAML to undertake the further steps in the retainer which would constitute a money laundering offence.

For further information on how to make an authorised disclosure to the NCA and the process by which consent/DAML is gained, see (Section 11) of this guidance.

16.4.2 Adequate consideration defence

In relation to s329 you will also have a defence if you received adequate consideration for the criminal property (the adequate consideration defence).This defence applies if there was adequate consideration for acquiring, using and possessing the criminal property, unless you know or suspect that those goods or services may help another to carry out criminal conduct.

The Crown Prosecution Service guidance for prosecutors says the defence applies where professional advisors, such as legal professionals or accountants, receive money for or on account of costs, whether from the client or from another person on the client's behalf. Disbursements are also covered. The fees charged must be reasonable, and the defence is not available if the value of the work is significantly less than the money received.

The transfer of funds from client to office account, or vice versa, is covered by the defence. Returning the balance of an account to a client may be a money laundering offence if you know or suspect the money is criminal property. In that case, you must make an authorised disclosure and obtain consent/DAML to deal with the money before you transfer it.

Reaching a matrimonial settlement or an agreement on a retiring partner's interest in a business does not constitute adequate consideration for receipt of criminal property, as in both cases the parties would only be entitled to a share of the legitimately acquired assets of

the marriage or the business. This is particularly important where your client would be receiving the property as part of a settlement which would be exempted from s328 due to the case of *Bowman v Fels*.

The defence is more likely to cover situations where:

- a third party seeks to enforce a debt and is given criminal property in payment for that debt; or
- a person provides goods or services as part of a legitimate arm's length transaction but is paid from a bank account which contains the proceeds of crime.

16.4.3 Reasonable excuse

This defence applies where you intended to make an authorised disclosure but had a reasonable excuse for not doing so.

No offence is committed if there is a reasonable excuse for not making a disclosure, but there is **no judicial guidance on what might constitute a reasonable excuse**.

However, you are prevented from disclosing if your knowledge or suspicion is based on privileged information and legal professional privilege is not excluded by the crime/fraud exception. It is the Legal Sector Affinity Group's view that in such instances you will have a reasonable excuse for not making an authorised disclosure and will not commit a money laundering offence.

There may be other circumstances which could provide a reasonable excuse, but this would initally be for law enforcement to consider prior to any prosecution and ultimately for the court to decide in any subsequent prosecution.

For example:

- if it is clear that a regulator or enforcement authority (in the UK or elsewhere) is already fully aware of the suspected criminal conduct or money laundering and the reporter does not have any additional information which might assist the regulator or enforcement authority;
- if the only information that a reporter would be providing for the purposes of an authorised disclosure or a report under s330 is information entirely within the public domain;
- if all the suspected predicate offending occurs outside the UK and all the suspected money laundering occurs outside the UK and there is otherwise no UK nexus to the suspected criminality; or
- if the criminal activity derives from an administrative offence; for example, one of "strict liability" where no mens rea, or criminal intent, is required.

This is not intended to be an exhaustive list. Moreover, reporters should be aware that it will ultimately be for a court to decide if a reporter's excuse for not making a disclosure report was reasonable. Reporters should clearly document their reasons for concluding that they have a reasonable excuse in any given case and, if in doubt, may wish to seek independent legal advice.

16.5 Failure to disclose offences – money laundering

16.5.1 General comments

The failure to disclose provisions are found in s330, s331 and s332. In all three sections, the phrase ‘knows or suspects’ refers to actual knowledge or suspicion - a subjective test. However, you will also commit an offence if you fail to report when you have reasonable grounds for knowledge or suspicion - an objective test. On this basis, you may be guilty of the offence under s330 or s331 if you should have known or suspected money laundering.

For all failure to disclose offences you must either:

- know the identity of the money launderer or the whereabouts of the laundered property; or
- believe the information on which your suspicion was based may assist in identifying the money launderer or the whereabouts of the laundered property.

16.5.2 Section 330 – failure to disclose: regulated sector

A person commits an offence if:

- they know or suspect, or have reasonable grounds for knowing or suspecting, that another person is engaged in money laundering;
- the information on which their suspicion is based comes in the course of business in the regulated sector; and
- they fail to disclose that knowledge or suspicion, or reasonable grounds for suspicion, as soon as practicable to a MLRO or the NCA.

Under the changes introduced by the Criminal Finances Act 2017, where a practice shares information about a suspicion with another regulated entity, making a required notification or being party to a joint disclosure report will both be treated as satisfying any requirement to disclose.

Delays in disclosure arising from taking legal advice or seeking help may be acceptable provided you act promptly to seek advice.

16.5.3 Section 331 – failure to disclose: MLRO in the regulated sector

A MLRO in the regulated sector commits a separate offence if, as a result of an internal disclosure under s330, he or she knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering and he or she fails to make a disclosure to the NCA as soon as practicable.

16.5.4 Section 332 – failure to disclose: MLRO in the non-regulated sector

An organisation which is not in the regulated sector, may decide on a risk-based approach to set up internal disclosure systems and appoint a person as MLRO to receive internal disclosures.

A MLRO in the non-regulated sector commits an offence if, as a result of an internal disclosure, they know or suspect that another person is engaged in money laundering and fails to make a disclosure as soon as practicable to the NCA.

16.6 Defences to failure to disclose offences

There are three situations in which you have not committed an offence for failing to disclose:

- you have a reasonable excuse;
- you are a professional legal adviser, or a relevant professional adviser and the information came to you in privileged circumstances; or
- you did not receive appropriate training from your employer.

The first defence is the only one which applies to all three failure to disclose offences; the other two defences only apply to persons in the regulated sector who are not MLROs.

All of the failure to disclose sections also reiterate that the offence will not be committed if the property involved in the suspected money laundering is exempted overseas criminal conduct.

16.6.1 Reasonable excuse

Similar to the reasonable excuse defence against the *primary money laundering* offences, no offence in respect of a failure to disclose is committed if there is a reasonable excuse for not making a disclosure. Refer above to the guidance on this point.

16.6.2 Privileged circumstances

No offence is committed if the information or other matter giving rise to suspicion comes to a professional legal adviser or relevant professional advisor in privileged circumstances. You should note that receipt of information in privileged circumstances is not the same as legal professional privilege. It is a creation of POCA designed to comply with the exemptions from reporting set out in the European directives.

Privileged circumstances means information communicated:

- by a client, or a representative of a client, in connection with the giving of legal advice to the client;
- by a client, or by a representative of a client, seeking legal advice from you; or
- by a person in connection with legal proceedings or contemplated legal proceedings.

The exemption will not apply if information is communicated or given to the legal professional with the intention of furthering a criminal purpose and is unlikely to apply in respect of any transactional work undertaken on behalf of a client.

16.6.3 Lack of training

Employees within the regulated sector who have no knowledge or suspicion of money laundering, even though there were reasonable grounds for suspicion, have a defence if they have not received training from their employers. It does not apply where actual knowledge or suspicion exists. Employers may be prosecuted for a breach of the Regulations if they fail to train staff. This defence is not available to MLROs/Nominated Officers.

16.7 POCA Offences – other features

Mental Elements

The three mental elements most relevant to offences under Part 7 of POCA are:

- knowledge;
- suspicion; and
- reasonable grounds for knowledge or suspicion.

The objective standard only applies to offences relating to the regulated sector (s330-s331). The element ‘belief on reasonable grounds’ is also relevant in the specific context of the foreign legal conduct defence. A person will not be guilty of an offence if they know or believe on reasonable grounds that the relevant criminal conduct was exempt overseas conduct.

For the principal offences of money laundering the prosecution must prove that the property involved is criminal property. This means that the prosecution must prove that the property was obtained through criminal conduct and that, at the time of the alleged offence, you knew or suspected that it was.

For the failure to disclose offences, where you are acting in the regulated sector, you must disclose if you have knowledge, suspicion or reasonable grounds for suspicion. If you are not in the regulated sector you will only need to make a disclosure if you have actual, subjective knowledge or suspicion.

These terms for the mental elements in the offences are not defined within POCA. However, case law has provided some guidance on how they should be interpreted.

16.7.1 Knowledge

Knowledge means actual knowledge. There is some suggestion that willfully shutting one's eyes to the truth may amount to knowledge. However, the current general approach from the criminal courts is that nothing less than actual knowledge will suffice. Knowledge can be inferred from surrounding circumstances – for example a failure to ask obvious questions may lead to a jury implying knowledge

For a section 330 offence, knowledge must also come to the practice or member of staff during the course of regulated business. Information that does not arise through these circumstances may not give rise to the requirement to report, although does not preclude the practice/MLRO from doing so.

16.7.2 Suspicion

The term 'suspects' is one which the courts have historically avoided defining; however, because of its importance in English criminal law, some general guidance has been given. In the case of *R v Da Silva* [2007] 1 WLR 303, which was prosecuted under previous money laundering legislation, Longmore LJ stated:

> ‘It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more

> than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.'

There is no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a degree of satisfaction, not necessarily amounting to belief, but at least extending beyond speculation.

The test for whether you hold a suspicion is a highly subjective one.

If you think a transaction is suspicious, you are not expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. You may have noticed something unusual or unexpected and after making enquiries, the facts do not seem normal or make commercial sense. You do not have to have evidence that money laundering is taking place to have suspicion, or have knowledge of the underlying criminality Section 18 of this guidance contains a number of warning signs which may give you a cause for concern; however, whether you have a suspicion is a matter for your own judgment. To help form that judgment, consider talking through the issues with colleagues or contacting your supervisor. Listing causes for concern can also help focus your mind.

If you have not yet formed a suspicion but simply have cause for concern, you may choose to ask the client or others more questions. This choice depends on what you already know, and how easy it is to make enquiries.

If you think your own client is innocent but suspect that another party to a transaction is engaged in money laundering, you may still have to consider referring your client for specialist advice regarding the risk that they may be a party to one of the principal offences.

16.7.3 Reasonable grounds to know or suspect

For legal professionals in the regulated sector an additional objective test may establish the mental element of an offence. It is necessary to ask were there factual circumstances from which an honest and reasonable person, engaged in a business in the regulated sector, should have inferred knowledge or formed the suspicion that another was engaged in money laundering?

MLRO access to good quality CDD information (including the background/circumstances of a particular client/transaction) is key in this situation. This will help establish whether the matter in question is out-with the normal course of business or what might be expected of the client, or what specific further enquiries to make in order to establish whether there are grounds to know or suspect.

A clear and concise rationale for the internal report should be available to the MLRO for consideration. Practices may find it helpful implement a standard internal reporting form for use by staff/partners – outlining the key information necessary to aid the MLRO in determining whether a report should be submitted.

Questions to ask in this context may include the source of funds or source of wealth/assets involved, the amounts/value involved, the intended use/movement/destination of assets, presence of red flags, high risk jurisdictions etc.

Legal Professionals must be able to demonstrate the actions/non-action taken was reasonable given the specific set of circumstances involved in each particular matter. The rationale for the decision taken should be retained by the MLRO.

Consideration must be made to balance the requirement to submit a SAR in a timely manner, and the gathering of further information in order to decide whether a suspicion has been formed.

16.7.4 Jurisdictional scope

You must report suspected money laundering even if your suspicion relates to overseas criminal conduct. Unless you have a reasonable excuse you may also commit a principal money laundering offence if you deal with criminal property derived from a predicate offence committed outside the UK.

This is because the definition of 'criminal conduct' in POCA not only includes all UK crimes, but all conduct which would be criminal if it had occurred in the UK. Similarly, the definition of money laundering, which underpins the failure to report offences, includes the principal offences, related offences and anything that would fall within either of those categories if done in the United Kingdom.

It is unnecessary to know, and is irrelevant, whether the conduct generating the criminal proceeds was unlawful in the jurisdiction where the conduct occurred.

A narrow exception from the application of these principles for conduct that occurs overseas and is legal where it takes place was introduced by the Serious Organised Crime and Police Act 2005 and is known sometimes as the "Spanish Bullfighter" exception. The legal conduct overseas exception applies where a person knows or believes on reasonable grounds that the relevant criminal conduct occurred in a country outside the UK and:

- was not unlawful where it occurred; and
- had it occurred in the United Kingdom would not be punishable by 12 months' imprisonment or more.

16.8 Tipping off Offences

Since 2007, s333A POCA has contained two offences for tipping off. There are also tipping off offences for terrorist property in the Terrorism Act, discussed in Section 17.

16.8.1 Tipping off – in the regulated sector

There are two tipping off offences in s333A of POCA. They apply only to businesses in the regulated sector.

16.8.1.2 Section 333A(1) – disclosing a suspicious activity report (SAR)

It is an offence to disclose to a third person that an internal or external SAR has been made by any person to the police, HM Revenue and Customs, the NCA or a nominated officer, if that disclosure might prejudice any investigation that might be carried out as a result of the SAR. This offence can only be committed:

- *after* a SAR is made or a disclosure is made to the NCA;
- if you know or suspect that by disclosing this information, you are likely to prejudice any investigation related to that SAR; and
- the information upon which the disclosure is based came to you in the course of business in the regulated sector.

16.8.1.3 Section 333A(3) – disclosing an investigation

It is an offence to disclose the fact that an investigation into a money laundering offence is being contemplated or carried out if that disclosure is likely to prejudice that investigation. The offence can only be committed if the information on which the disclosure is based came to the person in the course of business in the regulated sector, and it is known a law enforcement investigation is being contemplated or is underway.

The key point is that you can commit this offence, even when you are unaware that a SAR was submitted.

16.9 Prejudicing an investigation

S342(1) contains an offence to prejudice a confiscation, civil recovery or money laundering investigation, if the person making the disclosure knows or suspects that an investigation is being, or is about to be, conducted. S342(1) applies to those outside the regulated sector as well as those within the regulated sector.

You only commit this offence if you knew or suspected that the disclosure would, or would be likely to, prejudice any investigation.

16.10 Defences

16.10.1 Tipping off

The following disclosures are permitted:

- s333B - disclosures within an undertaking or group, including disclosures to a professional legal adviser or relevant professional adviser;
- s333C - disclosures between institutions, including disclosures from a professional legal adviser to another professional legal adviser;
- s333D - disclosures to your supervisory authority; and
- s333D(2) - disclosures made by professional legal advisers to their clients for the purpose of dissuading them from engaging in criminal conduct.

A person does not commit the main tipping off offence if he or she does not know or suspect that a disclosure is likely to prejudice an investigation.

16.10.2 Section 333B – disclosures within an undertaking or group etc.

It is not an offence if an employee, officer or partner of a practice discloses that a SAR has been made if it is to an employee, officer or partner of the same undertaking.

A legal professional will not commit a tipping off offence if:

- the disclosure is to a professional legal adviser or a relevant professional adviser;
- both the person making the disclosure and the person to whom it is made carry on business in an EEA state or in a country or territory imposing equivalent money laundering requirements; and
- those persons perform their professional activities within different undertakings that share common ownership, management or control.

16.10.3 Section 333C – disclosures between institutions etc.

A legal professional will not commit a tipping off offence if *all* the following criteria are met:

- The disclosure is made to another legal professional in an EEA state, or one with an equivalent AML regime;
- The disclosure relates to a client or former client of both parties, or a transaction involving them both, or the provision of a service involving them both;
- The disclosure is made for the purpose of preventing a money laundering offence; and
- Both parties have equivalent professional duties of confidentiality and protection of personal data.

16.10.4 Section 333D(2) – limited exception for professional legal advisers

A legal professional will not commit a tipping off offence if the disclosure is to a client and it is made for the purpose of dissuading the client from engaging in conduct amounting to an offence. This exception and the tipping off offence in s333A apply to those carrying on activities in the regulated sector.

16.11 Section 342(4) – professional legal adviser exemption

It is a defence to a s342(1) offence that a disclosure is made by a legal adviser to a client, or a client's representative, in connection with the giving of legal advice or to any person in connection with legal proceedings or contemplated legal proceedings.
Such a disclosure will not be exempt if it is made with the intention of furthering a criminal purpose (s342(5)).

16.12 Making enquiries of a client

You should make preliminary enquiries of your client, or a third party, to obtain further information to help you to decide whether you have a suspicion. You may also need to raise questions during a retainer to clarify such issues.

There is nothing in POCA which prevents you making normal enquiries about your client's instructions, and the proposed retainer, in order to remove any concerns and enable the practice to decide whether to take on or continue the retainer.
These enquiries will only be tipping off if:

- you disclose that you have already made a SAR or that a money laundering investigation is being carried out or contemplated; and
- those enquiries are likely to prejudice any subsequent investigation.

It is not tipping-off to include a paragraph about your obligations under the money laundering legislation in your practice's standard client care letter.

17. Terrorist Property Offences

17.1 General comments

Terrorist organisations require funds to plan and carry out attacks, train militants, pay their operatives and promote their ideologies.

Terrorist financing is the provision or collection of funds with the intention of being used to carry out terrorist acts whether by terrorist organisations or by individuals acting alone or in small networks.

Practices should be aware that terrorist financing can involve funds from legitimate or illegitimate sources – ranging from personal donations to the proceeds of criminal activity such as drug dealing, extortion or human trafficking. It may also originate from funds raised via the diversion or exploitation of natural resources.

Concealment of the destination of legitimate funds to be used for criminal purposes is, in effect, money laundering in reverse.

The Terrorism Act 2000 (as amended) (TA) criminalises not only the participation in terrorist activities but also the provision of monetary support for terrorist purposes. Unless stated otherwise, sections mentioned in this Section 17, will refer to sections of the TA.

The UK National Risk Assessment 2020 states:
"The risk of terrorist financing through legal services is low. We continue to assess that legal services are not attractive for terrorist financing and there remains no evidence of these services being abused for terrorist financing purposes".

Practices must still be aware of their risk exposure in the context of the overall business, and within individual client relationships or transactions – and take appropriate steps to mitigate these risks.

17.2 Application

All persons are required to comply with the TA. The principal terrorist property offences in s15–s18 apply to all persons and therefore to all legal professionals. However, the specific offence of failure to disclose and the two tipping off offences apply only to persons in the regulated sector, as defined in Schedule 3A of the TA.

17.3 Section 14 - Definition of Terrorist Property

Terrorist property is defined as:
"money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation), proceeds of the commission of acts of terrorism, and proceeds of acts carried out for the purposes of terrorism".

17.4 Principal terrorist property offences

17.4.1 Section 15 – fundraising

It is an offence to be involved in fundraising if you have knowledge or have reasonable cause to suspect that the money or other property raised may be used for terrorist purposes.

You can commit the offence by:

- inviting others to make contributions;
- receiving contributions; or
- making contributions towards terrorist funding, including making gifts and loans.

It is no defence that the money or other property is a payment for goods and services.

17.4.2 Section 16 – use or possession

It is an offence to use or possess money or other property for terrorist purposes, including when you have reasonable cause to suspect they may be used for these purposes.

17.4.3 Section 17 – arrangements

It is an offence to become involved in an arrangement which makes money or other property available to another if you know or have reasonable cause to suspect it may be used for terrorist purposes.

17.4.4 Section 18 – money laundering

It is an offence to enter into or become concerned in an arrangement facilitating the retention or control of terrorist property by, or on behalf of, another person including, but not limited to the following ways:

- by concealment;
- by removal from the jurisdiction; or
- by transfer to nominees.

It is a defence if you did not know, and had no reasonable cause to suspect, that the arrangement related to terrorist property.

17.5 Defences to principal terrorist property offences

We will refer to defence against terrorist financing SARs as DAML for simplicity.

In 2007, three new defences to the main offences in s15 – s18 were introduced to the TA. These defences are contained in s21ZA – s21ZC, and are as follows:

- **prior consent/DAML defence** – you make a disclosure to an authorised person before becoming involved in a transaction or an arrangement, and the person acts with the consent of an authorised officer. Similarly to POCA there is a 7 working day notice period for the NCA to respond, after which you will have either a response or deemed consent but unlike POCA there is no moratorium period;
- **consent/DAML defence** – you are already involved in a transaction or arrangement and make a disclosure, so long as there is a reasonable excuse for failure to make a disclosure in advance; and
- **reasonable excuse defence** – you intended to make a disclosure but have a reasonable excuse for failing to do so.

Similarly to POCA there is a 7 working day notice period for the NCA to respond, after which you will have either a response or deemed consent but unlike POCA there is no moratorium period.

See Section 11 of this guidance for more information on how to make a disclosure and gaining consent.

There are further defences relating to co-operation with the police in s21. You do not commit an offence under s15-s18 in the following further circumstances:

- you are acting with the express consent of a constable, including civilian staff at the NCA; or
- you disclose your suspicion or belief to a constable or the NCA after you become involved in an arrangement or transaction that concerns money or terrorist property, and you provide the information on which your suspicion or belief is based. You must make this disclosure on your own initiative and as soon as reasonably practicable.

The defence of disclosure to a constable or the NCA is also available to an employee who makes a disclosure about terrorist property offences in accordance with the internal reporting procedures laid down by the practice.

17.6 Failure to disclose offences

17.6.1 Non-regulated sector

S19 provides that anyone, whether they are a MLRO or not, must disclose as soon as reasonably practicable to a constable, or the NCA, if they believe or suspect that another person has committed a terrorist financing offence based on information which came to them in the course of a trade, profession or employment. The test is subjective.

17.6.2 Regulated sector

S21A creates a criminal offence for those in the regulated sector who fail to make a disclosure to either a constable or the practice's MLRO where they know, suspect, or there are reasonable grounds for knowing or suspecting that another person has committed an offence. Since 2007 the offence has also covered the failure to disclose an attempted offence under s15-s18.

17.7 Defences to failure to disclose

The following are defences to failure to disclose offences under both s19 and s21A.

Either:

- you had a reasonable excuse for not making the disclosure; or
- you received the information on which the belief or suspicion is based in privileged circumstances, without an intention of furthering a criminal purpose.

Under s21A a person also has a defence where they are employed or are in partnership with a 'professional legal adviser' to provide assistance and support and they receive information giving rise to the relevant knowledge or suspicion in privileged circumstances.

It is also a defence under s19 if you made an internal report in accordance with your employer's reporting procedures.

17.8 Section 21D tipping off offences: regulated sector

17.8.1 Section 21D(1) – disclosing a suspicious activity report (SAR).

It is an offence to disclose to a third person that a SAR has been made by any person to the police, HMRC, the NCA or a MLRO, if that disclosure might prejudice any investigation that might be carried out as a result of the SAR. This offence can only be committed:

- *after* an internal disclosure has been made or a disclosure has been made to the NCA;
- if you know or suspect that by disclosing this information, you are likely to prejudice any investigation related to that SAR; and
- the information upon which the disclosure is based came to you in the course of business in the regulated sector.

17.8.2 Section 21D(3) – disclosing an investigation*.*

It is an offence to disclose that an investigation into allegations relating to terrorist property offences is being contemplated or carried out if that disclosure is likely to prejudice that investigation. The offence can only be committed if the information on which the disclosure is based came to the person in the course of business in the regulated sector. The key point is that you can commit this offence, even where you are unaware that a SAR was submitted.

17.9 Defences to tipping off

17.9.1 Section 21E – disclosures within an undertaking or group etc

It is not an offence if an employee, officer or partner of a practice discloses that a SAR has been made if the disclosure is to an employee, officer or partner of the same undertaking. A legal professional will also not commit a tipping off offence if a disclosure is made to another legal professional in a different undertaking, provided that the undertakings the parties work in:

- share common ownership, management or control; and
- carry on business in either the UK or an EEA state or a country or territory that imposes money laundering requirements that are equivalent.

17.9.2 Section 21F – other permitted disclosures

A legal professional will not commit a tipping off offence if all the following criteria are met:

- the disclosure is made to another legal professional in the UK or an EEA state, or one having an equivalent AML regime;
- the disclosure relates to a client or former client of both parties, or a transaction involving them both, or the provision of a service involving them both;
- the disclosure is made for the purpose of preventing a terrorist property offence; and
- both parties have equivalent professional duties of confidentiality and protection of personal data.

17.9.3 Section 21G – limited exception for professional legal advisers

A legal professional will not commit a tipping off offence if the disclosure is to a client and it is made for the purpose of dissuading the client from engaging in conduct amounting to an offence. This exception and the tipping off offence in s21D only apply to the regulated sector.

17.10 Making enquiries of a client

You will often make preliminary enquiries of your client, or a third party, to obtain further information to help you to decide whether you have a suspicion. You may also need to raise questions during a retainer to clarify such issues.

These enquiries will only amount to tipping off if you disclose that a suspicious activity report has been made, or that an investigation into allegations relating to terrorist property offences is being carried out or contemplated.

17.11 The offences

Part 1 of the Terrorist Asset-Freezing Act 2010 (the TAFA) contains prohibitions against:

- dealing with the funds or economic resources owned, held or controlled by designated persons;
- making funds or financial services or economic resources available, directly or indirectly to designated persons;
- making funds or financial services or economic resources available to any person for the significant benefit of a designated person; and
- knowingly and intentionally participating in activities that would directly or indirectly circumvent the financial restrictions, enable, or facilitate the commission of any of the above offences.

It is a defence if you did not know nor had any reasonable cause to suspect that you were undertaking a prohibited act with respect to a designated person.

In relation to funds, “deal with” is defined by the legislation as:

- using, altering, moving, allowing access to or transferring;
- dealing with in any other way that would result in any change in volume, amount, location, ownership, possession, character or destination; or
- making any other change that would enable use, including portfolio management.

In relation to economic resources, “deal with” is defined as “using to obtain funds, goods, or services in any way.”

Funds, and economic resources are each defined very broadly in s39 of the TAFA 2010. S40 of the TAFA defines financial services broadly and includes asset management (e.g. trust services) as well as investment advice.

The TAFA applies to persons designated by the UK unilaterally or under Council Regulation 2580/2001. The ISIL (Da'esh) and Al-Qaida (Asset-Freezing) Regulations 2011 (the 2011 Regulations), as amended, create a similar, and parallel regime of offences for persons designated under EC Regulations 881/2002 and 1686/2016.

17.12 Other terrorist property offences (No Deal Brexit; post-implementation period)

In addition to the Terrorism Act offences, the UK has enacted terrorist asset-freezing legislation in part to give effect to international obligations. These terrorist property offences focus on the financial and economic dealings of specific individuals, referred to in the legislation as designated persons.

The Sanctions and Anti-Money Laundering Act 2018 empowers the Secretary of State to make regulations that will enable the terrorist-asset freezing regime to apply in substantially the same way after the United Kingdom leaves the European Union. After Britain leaves the European Union (and any transition period), the Government intends to repeal Part 1 of the Terrorist Asset-Freezing Act 2010 and revoke the 2011 Regulations. The asset-freeze offences will be reproduced across three regulations:

- Counter Terrorism (Sanctions) (EU Exit Regulations) 2019;
- Counter Terrorism (International Sanctions) (EU Exit) Regulations 2019; and
- ISIL (Da'esh) and Al-Qaida (United Nations Sanctions) (EU Exit Regulations) 2019.

17.13 The offences

These regulations contain prohibitions against:

- dealing with the funds or economic resources owned, held or controlled by designated persons;
- making funds or financial services or economic resources available, directly or indirectly to designated persons;
- making funds or financial services or economic resources available to any person for the significant benefit of a designated person; and
- knowingly and intentionally participating in activities that would directly or indirectly circumvent the financial restrictions, enable, or facilitate the commission of any of the above offences.

It is a defence if you did not know nor had any reasonable cause to suspect that you were undertaking a prohibited act with respect to a designated person.

In relation to funds, 'deal with' is defined by the legislation as:

- using, altering, moving, allowing access to or transferring;
- dealing with in any other way that would result in any change in volume, amount, location, ownership, possession, character or destination; or
- making any other change that would enable use of the funds (including portfolio management).

In relation to economic resources, 'deals with' is defined as:

- exchanging or using the resources for funds, goods, or services (including by pledging them as security).

A consolidated list of designated persons is available on the Treasury website.

18. Red Flags and Warning Signs

18.1 General Overview

The Regulations require you to conduct risk assessments, due diligence and ongoing monitoring of your business relationships and take steps to be aware of transactions with heightened money laundering or counter-terrorist financing risks. The Proceeds of Crime Act 2002 requires you to report suspicious transactions.

This section highlights a number of warning signs or “red flags” for legal professionals generally and for those dealing with particular types of work, to further help you assess the AML risks associated with your practice, or risks of a particular client or matter appropriately and also to help you decide whether you have reasons for concern or the basis for a reportable suspicion.

Because money launderers are always developing new techniques, no list of examples can be exhaustive or fully comprehensive; however, below are some key factors which may arise during or after client and retainer acceptance and give you cause for concern.

If you become aware of a red flag, this should prompt to you to ask for additional documentation or ask further questions of your client. For any aspect of an instruction, good questions to ask are, “Does this make sense?” and, “Is the documentation I have consistent with what I am being told and know about the background, nature or circumstances of the client?” If the answer is no, then consider what further information or documentation you require in order to become satisfied. If you cannot be satisfied, you consider your position in terms of proceeding with the relationship or matter, as per r.30., and consider the submission of a suspicious activity report.

The presence of any one red flag does not mean that a client is automatically high risk, that you should not continue with the retainer or that you need to make a Suspicious Activity Report. The presence of red flags must be considered in context; the client may be able to provide a legitimate explanation. For example, a large transaction by an oil company points to high risk, but actually it may be a normal and regular occurrence for that particular client’s industry and business activities, and for your law firm. Remember, it is not “tipping off” to ask for further information as part of your client due diligence process.

If you cannot get the information you need, this may in itself be cause for further concern and lead you to become suspicious.

18.2 Examples of Red Flags

In collating these red flags, reference has been made to The FATF Report on Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals (2013) and The FATF Guidance on Concealment of Beneficial Ownership (July 2018) as well as other, similar pieces of guidance.

18.2.1 The Client

If a client:

- is excessively obstructive, secretive or unwilling to meet you;
- is a Politically Exposed Person (PEP);

- provides false or counterfeited documentation;
- is a business entity which cannot be found on the internet and/or uses an email address with an unusual domain or one more appropriate for an individual such as Hotmail, Gmail, Yahoo etc., especially if the client is otherwise secretive or avoids direct contact;
- is known to have convictions for acquisitive crime /other serious crimes such as human trafficking, illegal arms dealing or narcotics, known to be currently under investigation for acquisitive crime or have known connections with criminals;
- is or is related to or is a known associate of a person listed as being involved or suspected of involvement with terrorist or terrorist financing related activities;
- shows an unusual familiarity with respect to the ordinary standards provided for by the law in the matter of satisfactory customer identification, data entries and suspicious transaction reports;
- is involved in transactions which do not correspond to their normal professional or business activities e.g., a non-profit engaging business services that do not align with its work;
- does not have a suitable knowledge of the nature, object or the purpose of the legal services requested;
- wishes to establish or take over a legal person or entity with a dubious description of the aim, or for a purpose which is not related to their normal professional or commercial activities or their other activities, or for which a license is required, while the client does not have the intention to obtain such a licence;
- frequently changes legal structures and/or managers of legal persons;
- asks for short-cuts or unexplained speed in completing a transaction;
- appears disinterested in the outcome of the retainer and/or the costs incurred e.g., fees, taxes, the loss incurred due to selling at a reduced price or at a discount;
- requires introduction to financial institutions to help secure banking facilities;
- is engaging you from another area or jurisdiction without an obvious reason for doing so;
- is a business that is not normally cash intensive but appears to have substantial amounts of cash;
- is a business that relies heavily on new technologies and so may have inherent vulnerabilities to exploitation by criminals;
- uses financial intermediaries, financial institutions or legal professionals that are not subject to AML/CFT laws and measures and that are not adequately supervised by competent authorities or Professional Body Supervisors.);
- appears to be acting on somebody else's instructions without disclosing the identity of such person;
- requests that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation, which inhibits the legal professionals' ability to perform proper due diligence and risk assessment;
- has no address, or has multiple addresses without legitimate reasons;
- has funds which are disproportionate or inconsistent with their disclosed circumstances and financial position;
- changes their means of payment for a transaction at the last minute and without plausible justification;
- insists, without reasonable explanation, that transactions be undertaken exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity;
- is involved in certain transactions, structures, geographic locations, international activities or other factors that are not consistent with the practice's understanding of the client's business or economic situation;

- is from an industry or sector where there is more risk of ML: oil, arms, precious metals, tobacco products, cultural artefacts, ivory, other items related to protected species, other items of archaeological, historical, cultural and religious significance, or of rare scientific value, legal cannabis industry;
- applies for residence rights or citizenship in a jurisdiction in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities in that jurisdiction;
- is suspected of involvement in falsifying activities for example by use false loans, false invoices, or misleading naming conventions;
- has a business where employee numbers, structure or nature is divergent from the industry norm;
- seeks advice or to implement an arrangement where there are indicators of a tax evasion purpose;
- is suddenly active after a previously dormant period without clear explanation;
- starts or develops an enterprise with unexpected profile or abnormal business cycles or enters into new/emerging markets;
- indicates a wish not to obtain necessary governmental approvals/filings;
- frequently changes professional adviser(s) or members of management;
- is reluctant to provide all the relevant information or legal professionals have reasonable suspicion that the provided information is incorrect or insufficient;
- is a foreign national with no significant dealings in the country in which professional or financial services are sought;
- is conducting transactions which appear strange given an individual's age;
- has previously been prohibited from holding a directorship role in a company or operating as a trust and company service provider;
- is the signatory to company accounts without sufficient explanation;
- conducts financial activities and transactions inconsistent with client profile; or
- has declared income which is inconsistent with the client's assets, transactions, or lifestyle.

If the client is a legal person or legal arrangement and it:

- has demonstrated a long period of inactivity following incorporation, followed by a sudden and unexplained increase in financial activities;
- describes itself as a commercial business but cannot be found on the internet or social business network platforms;
- is registered under a name that does not indicate the activity of the company or the name cannot otherwise be associated with the operations or ownership of the company;
- is registered under a name that indicates that the company performs activities or services that it does not provide;
- is registered under a name that appears to mimic the name of other companies, particularly high-profile multinational corporations;
- is registered at an address that does not match the profile of the company, that cannot be located on internet mapping services or is also listed against numerous other companies or legal arrangements;
- has directors or controlling shareholder(s) who cannot be located or contacted, or do not appear to have an active role in the company;
- has directors, controlling shareholder(s) and/or beneficial owner(s) who are listed against the accounts of other legal persons or arrangements, indicating the use of professional nominees;
- has directors, controlling shareholders who are geographically diverse, without a logical reason;

- have large amounts of minor data corrections or changes in ownership/control on official company registries, without logical reason;
- has authorised numerous signatories without sufficient explanation or business justification;
- regularly sends money to low-tax jurisdictions or international trade or finance centres;
- conducts a large number of transactions with a small number of recipients;
- conducts a small number of high-value transactions with a small number of recipients;
- regularly conducts transactions with international companies without sufficient corporate or trade justification;
- maintains relationships with foreign professional intermediaries in the absence of genuine business transactions in the professional's country of operation;
- receives large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere in a short period of time without commercial justification;
- maintains a bank balance of close to zero, despite frequent incoming and outgoing transactions;
- conducts financial activities and transactions inconsistent with the corporate profile;
- is incorporated/formed in a jurisdiction that does not require companies to report beneficial owners to a central registry;
- operates using accounts opened in countries other than the country in which the company is registered;
- involves multiple shareholders who each hold an ownership interest just below the threshold required to trigger enhanced due diligence measures.

18.2.2 The Parties

- the parties to the transaction are connected without an apparent business reason;
- the ties between the parties of a family, employment, corporate or any other nature generate doubts as to the real nature or reason of the transaction;
- there are multiple appearances of the same parties in transactions over a short period of time;
- the age of the executing parties is unusual for the transaction; there are attempts to disguise the real owner or parties to the transaction;
- the person actually directing the operation is not one of the formal parties to the transaction or their representative;
- the natural person acting as a director or representative does not appear to be a suitable representative.

18.2.3 Source of Funds

The source of funds is unusual due to:

- third party funding either for the transaction or for fees/taxes involved with no apparent connection or legitimate explanation;
- funds received from or sent to a foreign country when there is no apparent connection between the country and the client;
- funds received from or sent to high-risk countries;
- the client is using multiple bank accounts or foreign accounts without good reason;
- private expenditure is funded by a company, business or government;
- use of corporate funds to fund a private individual's expenditure or vice versa;

- selecting the method of payment has been deferred to a date very close to the time of completion, in a jurisdiction where the method of payment is usually included in the contract, without logical explanation;
- an unusually short repayment period has been set without logical explanation;
- mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation;
- the asset is purchased with cash and then rapidly used as collateral for a loan;
- there is a request to change the payment procedures previously agreed upon without logical explanation;
- finance is provided by a lender, either a natural or legal person, other than a credit institution, with no logical explanation or economic justification;
- the collateral being provided for the transaction is currently located in a high-risk country;
- there has been a significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company, with no logical explanation;
- the company receives an injection of capital or assets in kind which is notably high in comparison with the business, size or market value of the company performing, or from a foreign country or with no logical explanation;
- there is an excessively high or low price attached to the securities transferred;
- large financial transactions, especially if requested by recently created companies, where these transactions are not justified by the corporate purpose, the activity of the client or the possible group of companies to which it belongs or other justifiable reasons;
- loans are received from private third parties without any supporting loan agreements, collateral, or regular interest payments;
- use of cash;
- a client deposits funds into your client account but then ends the transaction for no apparent reason;
- a client tells you that the funds are coming from one source and at the last minute the source changes; or
- a client unexpectedly asks you to send money received into your client account back to its source, to the client or to a third party not associated with the transaction.

18.3 The Nature of the Transaction

- Transactions involving jurisdictions with strict bank secrecy and confidentiality rules, without similar money laundering requirements;
- use of shell companies which may be indicated by*:*
    - formal nominees and informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise;
    - address of mass registration;
    - only a post-box address;
    - no real business activities being undertaken;
    - the exclusive transit of transactions with no wealth or income being generated;
    - no personnel (or only a single person as a staff member);
    - lack of payment of taxes, superannuation, retirement fund contributions or social benefits;
    - no physical presence;
- loss-making transactions where the loss is avoidable or readily accepted;

- dealing with money or property where you suspect that either is being transferred to avoid the attention of a trustee in a bankruptcy case, HMRC, or a law enforcement agency;
- transactions which appear to be complex or unusually large;
- unusual patterns of transactions which have no apparent economic purpose;
- transactions are unusual because of their size, nature, frequency or manner of execution;
- significant differences between the declared price and the approximate actual values as judged either by the legal professional or in respect to some reference;
- type of operation being conducted is clearly inconsistent with the size, age, or activity of the legal entity or natural person acting;
- creation of complicated ownership structures;
- involvement of structures with multiple countries where there is no apparent link to the client or transaction;
- incorporation and/or purchase of stock or securities of several companies, enterprises or legal entities within a short period of time with elements in common;
- there is an absence of documentation to support the client's story, previous transactions, or company activities;
- there are several elements in common between a number of transactions in a short period of time;
- back-to-back property transactions (for example, within six months), with rapidly increasing value or purchase price;
- abortive transactions with no concern for the fee level or after receipt of funds;
- the retainer exclusively relates to keeping documents or other goods, holding large deposits of money or otherwise using the client account;
- a lack of sensible commercial/financial/tax or legal reason for the transaction;
- a power of attorney is sought for the administration or disposal of assets under conditions which are unusual;
- investment in immovable property, in the absence of any links with the place where the property is located and/or of any financial advantage from the investment;
- services where legal professionals, effectively acting as financial intermediaries, handle the receipt and transmission of funds through accounts they control in the act of facilitating a business transaction;
- services that allow clients to deposit/transfer funds through the legal professional's trust account that are not tied to a transaction which the legal professional is performing;
- services where the client may request financial transactions to occur outside of the legal professional's trust account;
- services requested by the client for which the legal professional does not have expertise unless the legal professional is referring the request to an appropriately trained professional for advice;
- services that rely heavily on new technologies that may have inherent vulnerabilities to exploitation by criminals, especially those not regulated for AML/CFT;
- transfer of real estate or other high value goods or assets between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason;
- payments received from un-associated or unknown third parties and payments in cash where this would not be a typical method of payment;
- transactions where it is readily apparent to the legal professional that there is inadequate consideration, especially where the client does not provide legitimate reasons for the amount of the consideration;

- administrative arrangements concerning estates where the deceased was known to the legal professional as being a person who had been convicted of crimes that generated proceeds;
- unexplained establishment of unusual provisions in credit arrangements that do not reflect the commercial position between the parties;
- transfer of goods that are inherently difficult to value, where this is not common for the type of client, transaction or the legal professional's normal course of business;
- acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason;
- services where the legal professional acts as a trustee/director that allows the client's identity to remain anonymous; or
- commercial, private or real property transactions or services to be carried out by the client with no apparent legitimate business, economic, tax, family governance, or legal reasons.

18.4 Trusts and Administration of Estates

- Purpose of the trust is unclear (trusts can be used to evade tax and hide criminal property);
- unusual structure or jurisdiction;
- unexplained use of express trusts, and/or incongruous or unexplained relationships between beneficiaries and the settlor;
- settlor was accused or convicted of acquisitive criminal conduct, improperly claimed welfare benefits or had evaded the due payment of tax during their lifetime;
- assets earned or obtained in a high-risk jurisdiction;
- unexplained or incongruous classes of beneficiaries in a trust; or
- discrepancy between the supposed wealth of the settlor and the object of the settlement.

18.5 Property work

18.5.1 Ownership issues

- Properties owned by nominee companies or multiple owners may be used as money laundering vehicles to disguise the true owner and/or confuse the audit trail; or
- sudden or unexplained changes in ownership. (Flipping, involves a property purchase, often using someone else's identity which is then quickly sold for a much higher price to the same buyer using another identity. The proceeds of crime are mixed with mortgage funds for the purchase. This process may be repeated several times.)

18.5.2 Funding Methods

- Transactions that do not involve a mortgage have a higher risk of being fraudulent, though a payment being made through the mainstream banking system is not guaranteed to be clean;
- large payments from private funds, especially if your client has a low income and payments from a number of individuals or sources;
- funds are supplied by a third party; or
- checks on the source of the funding can be more difficult where they involve direct payments between buyers and sellers.

18.5.3 Valuing

- A significant discrepancy between the sale price and what would reasonably be expected for such a property to sell for.

18.5.4 Lender issues

- A client may attempt to mislead a lender client to improperly inflate a mortgage advance – for example, by misrepresenting the borrower's income or because the seller and buyer are conspiring to overstate the sale price. This is mortgage fraud, and the mortgage advance will be the proceeds of crime; or
- loans which are not at arms' length may require particularly close consideration.

18.5.5 Tax issues

- If the purchase price is recorded incorrectly, this may be in an attempt to evade stamp duty (the saving would represent the proceeds of crime.)

18.5.6 Charities

- If registered with the Charity Commission, a charity is likely to be lower risk;
- if you are asked to receive money on the charity's behalf from an individual or a company donor, or a bequest from an estate, be alert to unusual circumstances including large sums of money; or
- there is growing concern about the use of charities for terrorist funding. HM Treasury maintains a consolidated list of individuals and entities to whom you may not provide funds, economic resources, and in relation to terrorism, financial services.

18.6 Company and Commercial Work

18.6.1 Formation of private equity funds

- Generally private equity work will be considered at low risk of money laundering or terrorist financing. Factors which may alter this risk assessment include:

  - where the private equity sponsor or an investor is located in a jurisdiction which is not regulated for money laundering to a standard which is equivalent to the 4th Directive;
  - where the investor is either an individual or an investment vehicle itself; or
  - where the private equity sponsor is seeking to raise funds for the first time.

- Whether an unregulated private entity firm, fund manager or other person involved with the transaction is an appropriate source of information regarding beneficial ownership of the client should be determined on a risk-based approach. Issues to consider include:

  - the profile of the private equity sponsor, fund manager, or such other person; their track record within the private equity sector; or
  - their willingness to explain identification procedures and provide confirmation that all beneficial ownerships have been identified.

18.6.2 Collective investment schemes

The risk associated with a collective investment scheme may be decreased where:

- the scheme is only open to tax-exempt institutional investors;
- investment managers are regulated individuals or entities; or
- a prospectus is issued to invite investment.

Factors which will increase the risks include where:

- the scheme is open to non-tax-exempt investors;
- the scheme or its investors are located in a jurisdiction which is not regulated for money laundering to a standard which is not equivalent to the currently applicable EU directive; or
- neither the scheme nor the investment managers are regulated and do not conduct CDD on the investors.

18.7 Trust and Company Service Providers (TCSPs)

- Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment;
- inexplicable changes in ownership;
- activities of the trust, company or other legal entity are unclear or different from the stated purposes under trust deeds or internal regulations of the company or foundation;
- legal structure has been altered frequently and/or without adequate explanation;
- management of any trustee, company or legal entity appears to be according to instructions of unknown or inappropriate person(s);
- unlikely choice of TCSP without a clear explanation, given the size, location or specialisation of the TCSP;
- use of pooled client accounts or safe custody of client money / assets or bearer shares, without justification;
- situations where advice on the setting up of legal persons or legal arrangements may be misused to obscure ownership or real economic purpose;
- in case of an express trust, an unexplained nature or classes of beneficiaries and acting trustees of such a trust;
- services where TCSPs may in practice represent or assure the client's standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs;
- services that are capable of concealing beneficial ownership from competent authorities;
- services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants than is normal;
- use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason;
- transactions using unusual means of payment;
- postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made;
- successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason;

- power of representation given in unusual conditions and the stated reasons for these conditions are unclear or illogical;
- transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason;
- nominee is being used with no apparent legal, tax, business, economic or other legitimate reason;
- commercial, private or real property transactions or services to be carried out by the trust, company or other legal entity with no apparent legitimate business, economic, tax, family governance, or legal reasons;
- products/services that have inherently provided more anonymity or confidentiality without a legitimate purpose;
- existence of suspicion of fraudulent transactions, or transactions that are improperly accounted for;
- any attempt by the settlor, trustee, company or other legal entity to enter into any fraudulent transaction;
- any attempt by the settlor, trustee, company or other legal entity to enter into any arrangement to fraudulently evade tax in any relevant jurisdiction;
- The customer is both the ordering and beneficiary customer for multiple outgoing international funds transfers;
- The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client;
- The transaction itself:

  - is occurring between two or more parties that are connected without an apparent business or trade rationale;
  - is a business transaction that involves family members of one or more of the parties without a legitimate business rationale;
  - is a repeat transaction between parties over a contracted period of time;
  - is a large or repeat transaction, and the executing customer is a signatory to the account, but is not listed as having a controlling interest in the company or assets;
  - is executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile;
  - as executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile;
  - appears cyclical;
  - involves the two-way transfer of funds between a client and a professional intermediary for similar sums of money;
  - involves two legal persons with similar or identical directors, shareholders or beneficial owners;
  - involves a professional intermediary without due cause or apparent justification;
  - involves complicated transaction routings without sufficient explanation or trade records;
  - involves the transfer of real property from a natural to a legal person in an off-market sale;
  - involves the use of multiple large cash payments to pay down a loan or mortgage;
  - involves a numbered account;
  - involves licensing contracts between corporations owned by the same individual
  - involves the purchase of high-value goods in cash;
  - involves the transfer of (bearer) shares in an off-market sale;
  - loan or mortgage is paid off ahead of schedule, incurring a loss;

- includes contractual agreements with terms that do not make business sense for the parties involved;
- includes contractual agreements with unusual clauses allowing for parties to be shielded from liability but make the majority of profits at the beginning of the deal;
- is transacted via a digital wallet; or

- Unexplained use of powers of attorney or other delegation processes.

18.8 Litigation (generally out of scope but still may be relevant for POCA or TACT)

- Disputes which are settled too easily or in an atypical manner may indicate sham litigation;
- payments on account followed by request for refund; or
- settlement of a debt by credit card, which may be stolen.

18.9 Choice of Lawyer

- The instructions are unusual for your practice or client or where they change unexpectedly without a logical reason;
- the client has changed advisor a number of times or engaged multiple legal advisers without legitimate reason;
- the required service was refused by another professional or the relationship with another professional was terminated;
- effusive praise for you or your firm; or
- willingness to pay more than usual rates.

19. GLOSSARY

Acronym	Meaning
AIM	Alternative Investment Market
AML	Anti- Money Laundering
BACS	Bankers' Automated Clearing System
BOOM	Beneficial Owner, Officer or Manager
CDD	Client Due Diligence
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CTO	Chief Technology Officer
DAML	Defence Against Money Laundering
EDD	Enhanced Due Diligence
EEA	European Economic Area
EID&V	Electronic Identification & Verification
EU	European Union
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
GDPR	General Data Protection Regulation
HMRC	Her Majesty's Revenue & Customs
HMT	Her Majesty's Treasury
HRTC	High Risk Third Country
ID&V	Identification & Verification
IDV	Identity Verification
ISIL	Islamic State of Iraq and the Levant
LLP	Limited Liability Partnership
LSAG	Legal Sector Affinity Group
ML	Money Laundering
ML/TF	Money Laundering/Terrorist Financing
MLCO	Money Laundering Compliance Officer
MLRO	Money Laundering Reporting Officer
NCA	National Crime Agency
OPBAS	Office for Professional Body Anti-Money Laundering Supervision
PCP	Policy, Control, Procedure
PEP	Politically Exposed Person
POCA	Proceeds of Crime Act
PWRA	Practice Wide Risk Assessment
RBA	Risk Based Approach
SAR	Suspicious Activity Report
SDD	Simplified Due Diligence
SFO	Serious Fraud Office
SLP	Scottish Limited Partnership
TACT	Terrorism Act

TF	Terrorist Financing
UBO	Ultimate Beneficial Owner
UK	United Kingdom
UKFIU	United Kingdom Financial Intelligence Unit

Annex I

If you suspect that property involved in a retainer is criminal property, offences under section 327 and section 329 are relatively straightforward to assess. However, an arrangement offence under section 328 may be more complicated, particularly with transactional matters.

Annexes II and III

You may become concerned in the arrangement by, for example, executing or implementing it, which may lead you to commit an offence under the Proceeds of Crime Act or the Terrorism Act (2000).

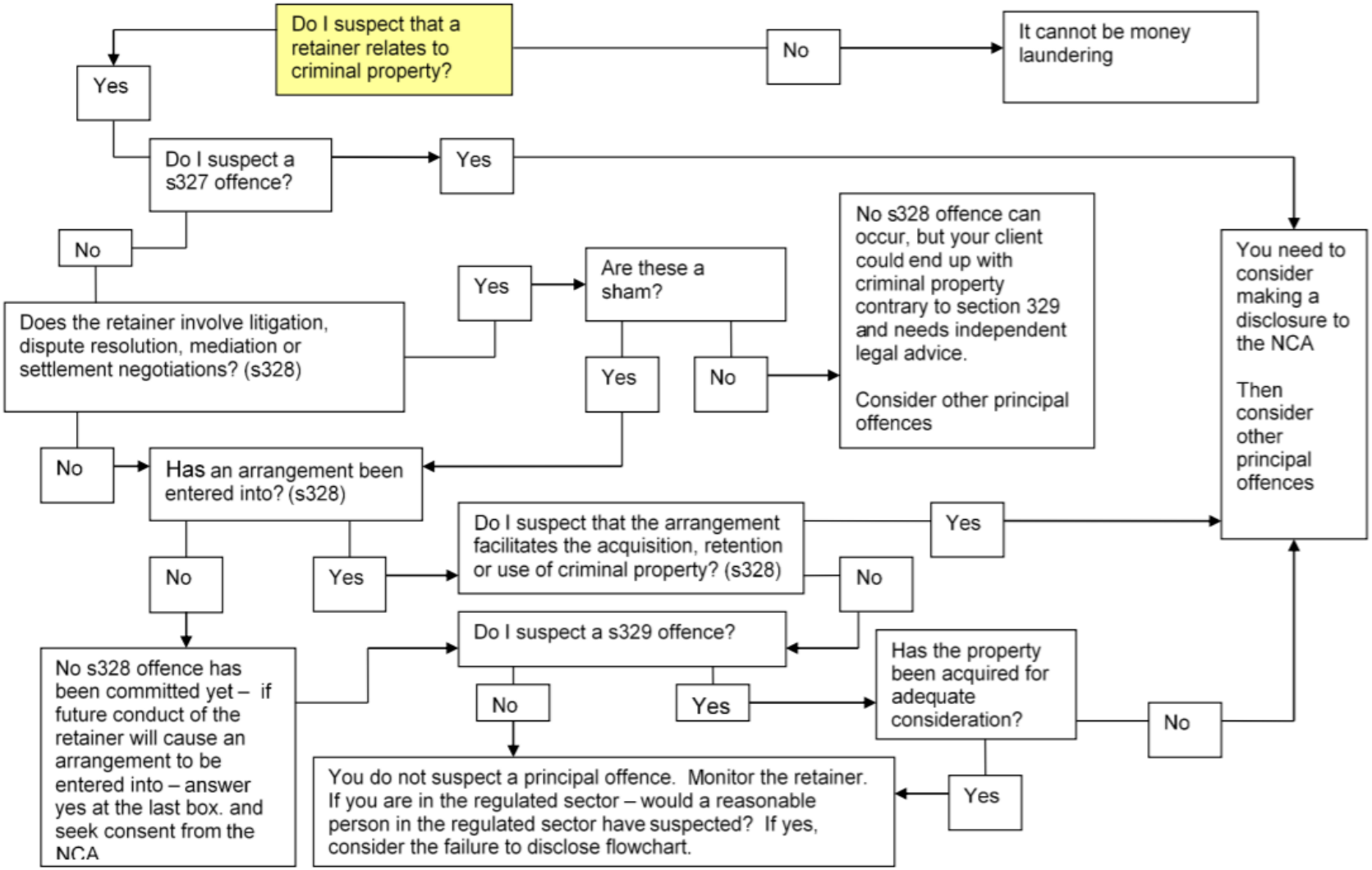
Consider whether you need to make an authorised disclosure to:

- obtain consent/DAML to proceed with the transaction
- provide yourself with a defence to the principal money laundering offences

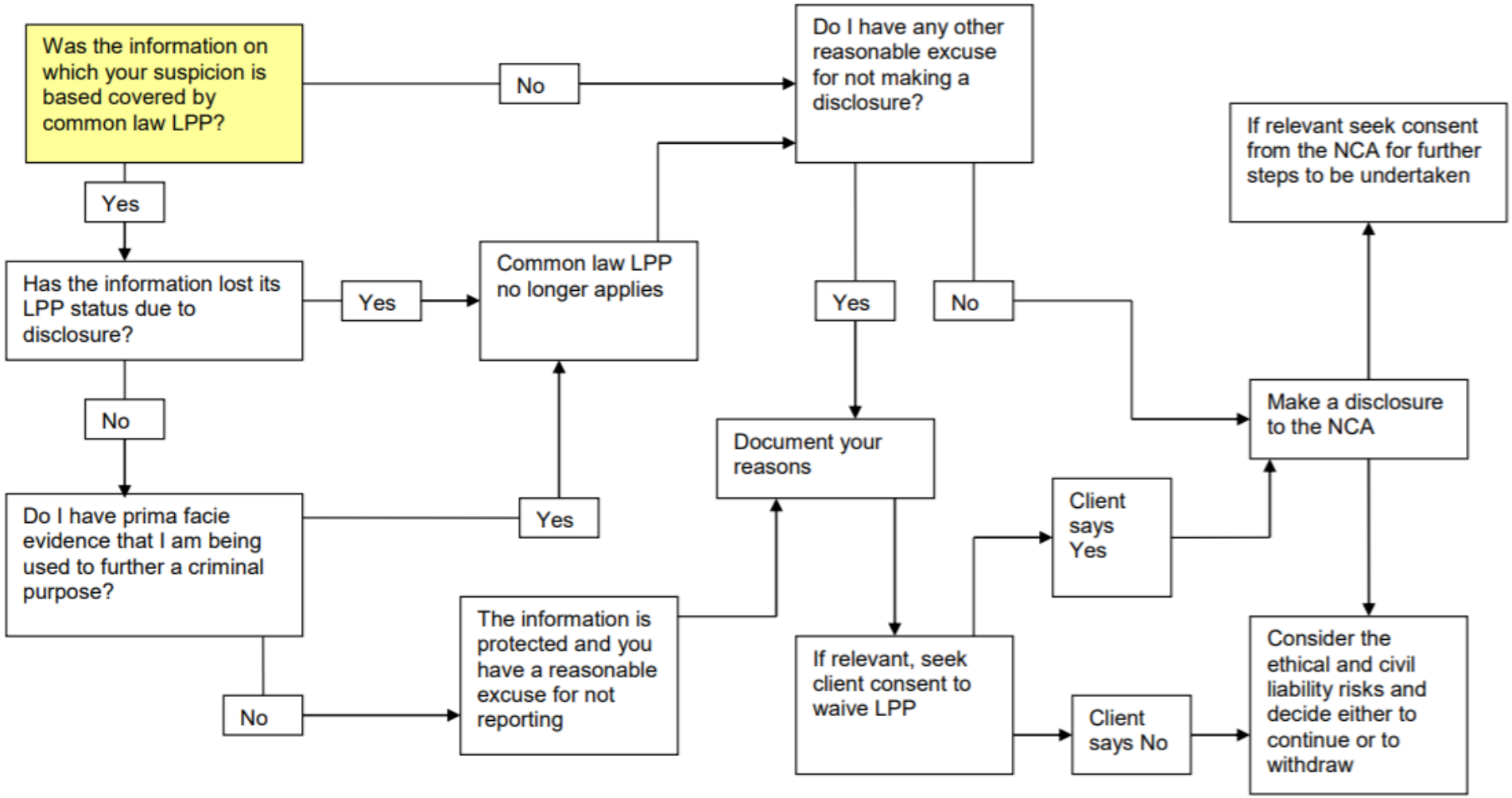
If you are acting within the regulated sector, consider whether you risk committing a failure to disclose offence, if you do not make a disclosure to the NCA.

The following two flowcharts show the issues to consider when deciding whether to make a disclosure to the NCA.

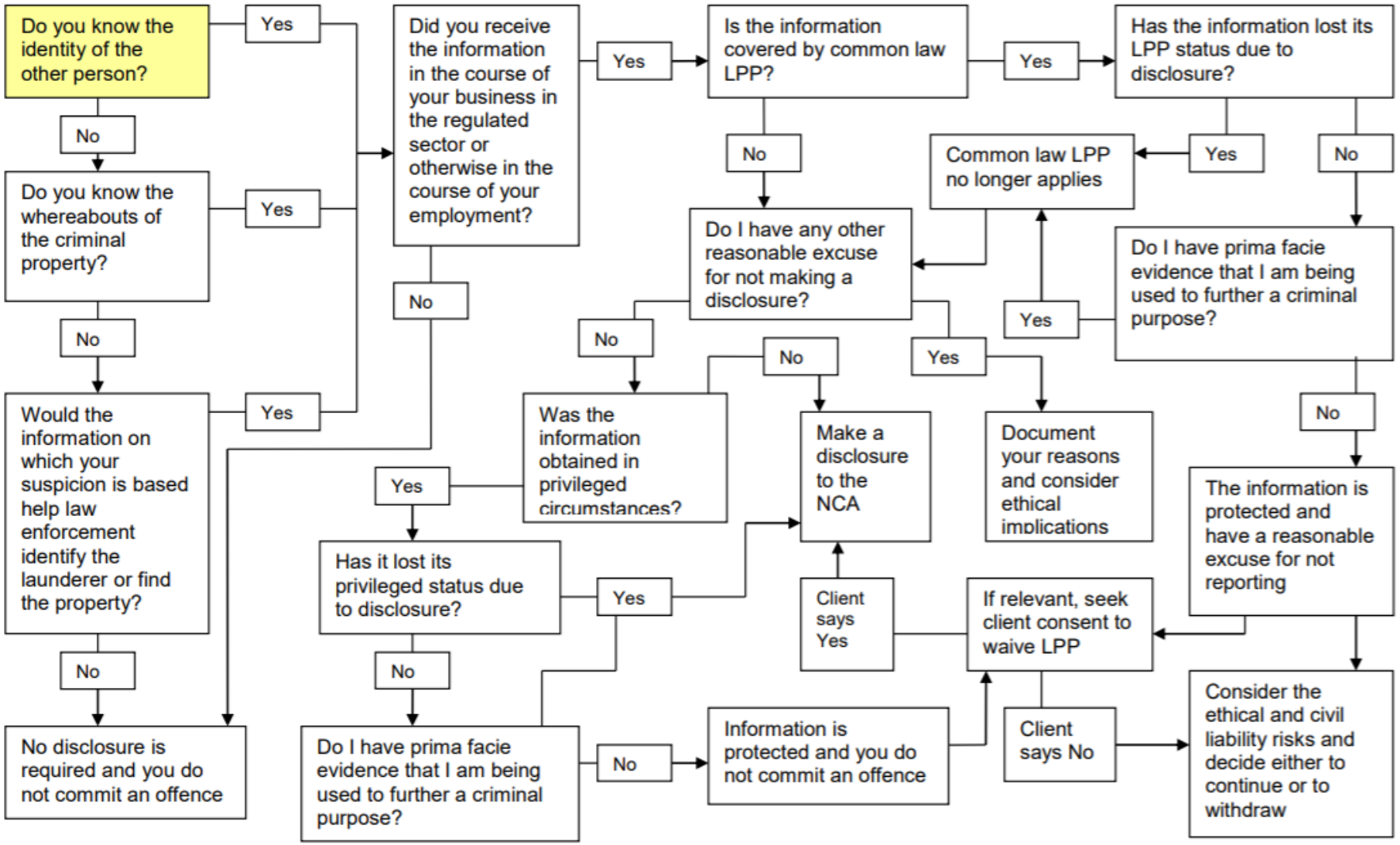
Annex I - flowchart A



Annex II Flowchart B



Annex III Flowchart C



Acknowledgements

Special thanks to:

Jane Jarman, Solicitor and Professor of Law at Nottingham Law School, Nottingham Trent University, for her time, knowledge and expertise in drafting Chapter 13 “Legal Professional Privilege”.

Members of the Law Society of England & Wales Money Laundering Taskforce for their time, knowledge and expertise in undertaking practitioner review, challenge and input across this document.