Legal Sector Affinity Group

Anti-Money Laundering

Guidance for the Legal Sector

September 2017

Contents

Glossary

AIM	Alternative Investment Market
AML / CTF	Anti-money laundering / counter-terrorist
BSB	Bar Standards Board
CDD	Customer due diligence
COLP	Compliance Officer for Legal Practice
DAML	Defence Against Money Laundering
EEA	European Economic Area
FATF	Financial Action Task-force
FCA	Financial Conduct Authority
GRO	General Register Office
HMRC	Her Majesty's Revenue and Customs
IBA	International Bar Association
JMLSG	Joint Money Laundering Steering Group
LLP's	Limited Liability Partnerships
LPP	Legal professional privilege
MLRO	Money Laundering Reporting Officer
PEPs	Politically exposed persons
POCA	Proceeds of Crime Act 2002
Regulations	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
SOCPA	Serious Organised Crime and Police Act 2005
SARs	Suspicious activity reports
SRA	Solicitors Regulation Authority

NCA	National Crime Agency
Terrorism Act	Terrorism Act 2000
Third directive	Third European Money Laundering Directive
4th Directive	Fourth European Money Laundering Directive

Definitions

Beneficial owners	See chapter 4 and 5
Business relationship	A business, professional or commercial relationship between a relevant person and a customer, which is: • connected to the business of the relevant person and • expected by the relevant person at the time when contact is established to have an element of duration. However, if the relevant person is asked to form a company for its customer, the relationship is a business relationship regardless of whether or not the formation of the company is the only transaction carried out for the customer.
Customer due diligence	See chapter 4.
Criminal conduct	Conduct which constitutes an offence in any part of the UK or would constitute an offence in any part of the UK if it occurred there – see s340(2) of POCA.
Criminal property	Property which is, or represents, a person's benefit from criminal conduct, where the alleged offender knows or suspects that it is such – see also the definition of property.
Disclosure	A report made to the NCA under the POCA – also referred to as a suspicious activity report (SAR).

DAML	DAML stands for Defence Against Money Laundering and is a term used by the NCA to refer to 'appropriate consent' to carrying out an activity that may result in a person committing a principal money laundering or terrorist financing offence as contained in Part 7 of POCA and Part 3 of the Terrorism Act.
Independent legal professional	See chapter 1.4.5.
Insolvency practitioner	Any person who acts as an insolvency practitioner within the meaning of section 388 of the Insolvency Act 1986 (as amended) or article 3 of the Insolvency (Northern Ireland) Order 1989 (as amended).
Inter vivos trust	A trust which takes effect while a person is alive.
Legal professional privilege	See chapter 7.4.
Nominated officer	A person nominated within the practice to make disclosures to the NCA under POCA – also referred to as a Money Laundering Reporting Officer (MLRO).
Occasional transaction	A transaction (carried out other than as part of a business relationship) amounting to 15,000 euros or more, whether the transaction is carried out in a single operation or several operations which appear to be linked.
Ongoing monitoring	See chapter 4.6.

Overseas criminal conduct	Conduct which occurs overseas that would be a criminal offence if it occurred in the UK. The definition does not include conduct which occurred overseas where it is known or believed on reasonable grounds that the relevant conduct occurred in a particular country or territory outside the UK, and such conduct was in fact not unlawful under the criminal law then applying in that country or territory. The exemption will not apply to overseas criminal conduct if it would attract a maximum sentence in excess of 12 months' imprisonment were the conduct to have occurred in the UK. Conduct will always be exempt if the overseas conduct is such that it would constitute an offence under the Gaming Act 1968, the Lotteries & Amusements Act 1976 or s23 or s35 of the Financial Services and Markets Act 2000. See s102 of SOCPA.
Politically exposed persons	See chapter 4.12.2.
Practice	An independent legal practitioner's business, whether that business is a law firm or conducted as a sole practitioner. For a barrister the term 'practice' refers to a self-employed professional.
Privileged circumstances	See chapter 6.7.2.
Property	All property whether situated in the UK or abroad, including money, real and personal property, things in action, intangible property and an interest in land or a right in relation to any other property.
Regulated sector	Activities, professions and entities regulated for the purposes of AML/CTF obligations - see chapter 1.

Tax adviser	A practice or sole practitioner who, by way of business, provides advice about the tax affairs of another person, when providing such services.
Terrorist property	Money or other property which is likely to be used for the purposes of terrorism, the proceeds of the commission of acts of terrorism and the proceeds of acts carried out for the purposes of terrorism.

Trust or company service provider	A practice or sole practitioner who by way of business provides any of the following services to other persons -
	• forming companies or other legal persons
	• acting or arranging for another person to act
	  ○ as a director or secretary of a company;
	  ○ as a partner of a partnership; or
	  ○ in a similar position in relation to other legal persons;
	• providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement;
	• acting, or arranging for another person to act, as -
	  ○ a trustee of an express trust or similar legal arrangement; or
	  ○ a nominee shareholder for another person other than a company listed on a regulated market when providing such services

Chapter 1 – Introduction

This draft guidance has been sent to HM Treasury for approval later this year and may be subject to change. Once it has been approved it will be published as final.

1.1 Who should read this guidance?

All independent legal professionals and other staff in a law practice who are involved in anti-money laundering compliance.

As this guidance applies across the entire legal sector the term 'practice' has been used to refer to an independent legal professional's business, whether that business is a law firm or other authorised entity, or is conducted as a sole practitioner, or in a self-employed capacity or operates under another structure. For solicitors, the term 'practice' refers to their firm as a whole and not a practice group within a firm.

1.1.1 Application to barristers and advocates

Barristers and advocates should note that there are areas of this Guidance that will not have application to them, for example where the Guidance refers to undertaking the management of a client's affairs or the handling of client money.

Other sections will apply to some barristers and advocates, but not others. For example, references to the MLRO role and organisational arrangements will not apply to advocates or self-employed barristers who are practising from chambers or as sole practitioners, but will apply to barristers working in private practice in entities, where the MLRO role and the organisational arrangements may be comparable to solicitors' firms.

Where a chapter of the Guidance has only limited or no application to barristers or advocates this is noted at the outset of the relevant chapter.

Barristers should note that BSB Handbook restrictions apply to both barristers and BSB entities; neither are permitted to:

- undertake the management, administration or general conduct of a client's affairs (rS25 for self-employed barristers, rS29 for BSB entities and rS33 for managers and employed barristers of BSB entities);
- receive, control or handle client money apart from that paid by the client to a barrister for their services, save where they are acting as a manager of a body authorised by another approved regulator to undertake reserved legal activities, such as the SRA (rC73 and rS83.5 for BSB entities).

Advocates should note that they are not permitted to receive, control or handle client money when either acting on the instructions of a solicitor or in terms of the Faculty of Advocates' Direct Access Rules.

1.2 What is the issue?

Independent legal professionals are key actors in the business and financial world, facilitating vital transactions that underpin the UK economy. As such, they have a significant role to play in ensuring that their services are not used to further a criminal

purpose. Independent legal professionals must act with integrity and uphold the law, and they must not engage in criminal activity.

Money laundering and terrorist financing are serious threats to society, causing a loss of revenue and endangering life, and fueling other criminal activity.

This guidance aims to assist independent legal professionals to meet their obligations under the UK anti-money laundering and counter-terrorist financing (AML/CTF) regime.

1.3 Definition of money laundering

Money laundering is generally defined as the process by which the proceeds of crime, and the true ownership of those proceeds, are changed so that the proceeds appear to come from a legitimate source. Under POCA, the definition is broader and more subtle. Money laundering can arise from small profits and savings from relatively minor crimes, such as regulatory breaches, minor tax evasion or benefit fraud. A deliberate attempt to obscure the ownership of illegitimate funds is not necessary.

There are three acknowledged phases to money laundering: placement, layering and integration. However, the broader definition of money laundering offences in POCA includes even passive possession of criminal property as money laundering.

1.3.1 Placement

Cash generated from crime is placed in the financial system. This is the point when proceeds of crime are most apparent and at risk of detection. Because banks and financial institutions have developed AML procedures, criminals look for other ways of placing cash within the financial system. Independent legal professionals can be targeted because they and their practices commonly deal with client money.

1.3.2 Layering

Once the proceeds of crime are in the financial system, layering involves obscuring the origins of the proceeds by passing them through complex transactions. These often involve different entities, for example, companies and trusts and can take place in multiple jurisdictions. An independent legal professional may be targeted at this stage and detection can be difficult.

1.3.3 Integration

Once the origin of the funds has been obscured, the criminal is able to make the funds appear to be legitimate funds or assets. They will invest funds in legitimate businesses or other forms of investment, often, for example, using an independent legal professional to buy a property, set up a trust, acquire a company, or even settle litigation, among other activities. This is the most difficult stage at which to detect money laundering.

1.4 Legal framework and other requirements

1.4.1 Financial Action Task Force (FATF)

This was created in 1989 by the G7 Paris summit, building on UN treaties on trafficking of illicit substances in 1988 and on confiscating the proceeds of crime in 1990. In 1990, FATF released their 40 recommendations for fighting money laundering. Between October 2001 and October 2004 it released nine further special recommendations to prevent terrorist funding. The recommendations were again revised in February 2012. The revised recommendations now fully integrate counter-terrorist financing measures with anti-money laundering controls and, among other things, seek to better address new and emerging threats and clarify and strengthen many of the existing obligations, including the laundering of the proceeds of corruption and tax crimes.

1.4.2 European Union directives

1991 – first money laundering directive

The European Commission issued this directive to comply with the FATF recommendations. It applied to financial institutions, and required member states to make money laundering a criminal offence. It was incorporated into UK law via the Criminal Justice Act 1991, the Drug Trafficking Act 1994 and the Money Laundering Regulations 1993.

2001 – second money laundering directive

This directive incorporated the amendments to the FATF recommendations. It extended anti-money laundering obligations to a defined set of activities provided by a number of service professionals, including independent legal professionals, accountants, auditors, tax advisers and real estate agents. It was incorporated into UK law via POCA and the Money Laundering Regulations 2003.

2005 – third money laundering directive

This directive extended due diligence measures to beneficial owners, recognised that such measures can be applied on a risk-based approach, and required enhanced due diligence to be undertaken in certain circumstances. It was incorporated into UK law by the Money Laundering Regulations 2007, the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 (the TACT and POCA Regulations 2007).

2015 - fourth money laundering directive

This directive responded to changes made to the requirements issued by FATF in February 2012 and to a review conducted by the European Commission on the implementation of the third money laundering directive.

There were a number of new developments contained in the 4th Directive. The key ones include the following:

- requirements on regulated entities to have a written risk assessment

- amendments to the way in which simplified due diligence may be applied
- changes to the beneficial ownership provisions
- extension of enhanced due diligence to domestic PEPs
- additional provisions in the legislation focusing on other matters, including changes to the offences that are included for reporting purposes (for example, tax evasion is now included, although many jurisdictions had already incorporated the reporting of tax crimes in their domestic legislation)
- requirements for Member States to maintain registers recording the beneficial owners of companies and trusts which generate tax consequences
- requirements for Member States to take necessary measures to prevent criminals with relevant convictions from holding a management function in, or being the beneficial owner of, an obliged entity

1.4.3 Proceeds of Crime Act 2002 (POCA) Scope

POCA, as amended, establishes a number of money laundering offences including:

- the principal money laundering offences
- the offences of failing to report suspected money laundering
- the offences of tipping off about a money laundering disclosure, tipping off about a money laundering investigation and prejudicing a money laundering investigation

The TACT and POCA Regulations 2007 repealed the section 333 POCA tipping off offence. It has been replaced by section 333A which creates two new offences. Section 342(1) has also been amended to reflect these new offences.

See Chapter 6 for further discussion of the principal money laundering offences.

Application

POCA applies to all persons, although certain offences regarding failure to report and tipping off only apply to persons who are engaged in activities in the regulated sector.

The Proceeds of Crime Act 2002 (Business in the Regulated Sector and Supervisory Authorities) Order 2007 amended the POCA, changing the definition of the regulated sector to bring it into line with the Money Laundering Regulations 2007. These regulations were in turn replaced by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 on 26 June 2017.

Under Schedule 9 of POCA, key activities which may be relevant to independent legal professionals are the provision of the following services by way of business:

- advice about the tax affairs of another person by a practice or sole practitioner
- legal or notarial services involving the participation in financial or real property transactions concerning the buying and selling of real property or business entities

- the managing of client money, securities or other assets
- the opening or management of bank, savings or securities accounts
- the organisation of contributions necessary for the creation, operation or management of companies
- the creation, operation or management of trusts, companies or similar structures.

Chapters 6, 7 and 9 of this guidance provide more details on the obligations of independent legal professionals under POCA.

1.4.4 Terrorism Act 2000

Scope

The Terrorism Act 2000, as amended, established several offences about engaging in or facilitating terrorism and raising or possessing funds for terrorist purposes. It established a list of proscribed organisations that the Secretary of State believes to be involved in terrorism. The TACT and POCA Regulations 2007 entered into force on 26 December 2007 and introduced tipping off offences and defences to the principal terrorist property offences into the Terrorism Act 2000.

Read about these provisions in Chapter 8.

Application

The provisions of the Terrorism Act generally apply to all persons. There is in addition a failure to disclose offence and tipping off offences for those operating within the regulated sector.

The Terrorism Act 2000 (Business in the Regulated Sector and Supervisory Authorities) Order 2007 amended the Terrorism Act to change the definition of the regulated sector to bring it into line with the Money Laundering Regulations 2007. These regulations have since been replaced by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

Chapters 8 and 9 provide more detail on the obligations of independent legal professionals under the Terrorism Act.

1.4.5 The Money Laundering Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations)

Scope

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 repeal and replace the Money Laundering Regulations 2007 and implement the 4th Directive. They set out administrative requirements for the anti-money laundering regime within the regulated sector and outline the scope of CDD.

The Regulations aim to limit the use of professional services for money laundering by requiring professionals to know their clients and to monitor the use of their services by clients.

Application

Regulation 8 states that the Regulations apply to persons acting in the course of businesses carried on in the UK in the following areas:

- credit institutions
- financial institutions
- auditors, insolvency practitioners, external accountants and tax advisers
- independent legal professionals
- trust or company service providers
- estate agents
- high value dealers
- casinos

Independent legal professional

An independent legal professional means a firm or a sole practitioner who by way of business provides legal or notarial services to other persons. It does not include legal professionals employed by a public authority or working in-house.

The Regulations only apply to a legal professional's activities where there is a risk of money laundering occurring. As such, they apply when a legal professional participates in financial or real property transactions concerning:

- buying and selling of real property or business entities
- managing of client money, securities or other assets
- opening or management of bank, savings or securities accounts
- organisation of contributions necessary for the creation, operation or management of companies
- creation, operation or management of trusts, companies, foundations or similar structures

A legal professional is considered to be participating in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction.

The Regulations do not apply to work undertaken by a notary as a public certifying officer where he or she has no substantive role in the underlying transaction. As such, the Regulations do not apply to many aspects of a notary's practice including, for example, the taking of affidavits and declarations, protests, translating, certifying the execution of documents and authentication work in general. Although the Regulations will not apply to work of this nature, notaries are still subject to obligations under the

Notaries Practice Rules 2014 and Code of Practice positively to identify appearing parties and keep records of the means of identification employed.

Activities covered by the Regulations

In terms of the activities covered, you should note that:

- managing client money is more narrowly defined than handling it
- opening or managing a bank account is defined more widely than simply opening a client account. It is likely to cover a legal professional acting as a trustee, attorney or a receiver.

Activities not covered by the Regulations

HM Treasury has confirmed that the following would not generally be viewed as participation in a financial transaction:

- payment on account of costs to a legal professional or payment of a legal professional's bill
- provision of legal advice
- participation in litigation or a form of alternative dispute resolution
- will-writing, although you should consider whether any accompanying taxation advice is covered
- work funded by the Legal Services Commission

If you are uncertain whether the Regulations apply to your work, you should seek legal advice on the individual circumstances of your practice or simply take the broadest possible approach to compliance with the Regulations.

Working elsewhere in the Regulated sector

When deciding whether you are within the regulated sector for the purpose of the Regulations, you also need to consider whether you offer services bringing you within the definitions of a tax adviser, insolvency practitioner, or trust or company service provider.

Under Regulation 11(d) a tax adviser is a firm or sole practitioner who provides advice about tax affairs of other persons, when providing such services.

A trust or company service provider is defined in Regulation 12(2) as firm or sole practitioner who, by way of business provides any of the following services, when providing those services:

- forming companies or other legal persons
- acting, or arranging for another person to act:
    - as a director or secretary of a company;
    - as a partner of a partnership; or
    - in a similar capacity in relation to other legal persons

- providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or legal arrangement
- acting, or arranging for another person to act, as:
    - a trustee of an express trust or similar legal arrangement
    - a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

You must consider the full range of related services, such as tax planning and tax compliance work.

You will also need to consider whether your practice undertakes activities falling within the definition of financial institution, particularly with respect to the list of operations covered by the capital markets directive, as contained in schedule 2 of the Regulations. When considering those operations, you should note that a will is not a designated investment, so storing it is not a safe custody service, and is not covered by the Regulations.

Simply being nominated as a trustee under a will does not amount to being a trust and company service provider, because the trust is not formed until the testator's death.

If you are an independent legal professional within the regulated sector and you also fall within another category, such as work regulated by the Financial Conduct Authority (FCA), this may affect your supervision under these Regulations. You should contact your supervisory authority for advice on any supervisory arrangements that they may have in place with other supervisory authorities.

1.5 Status of this guidance

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

Guidance is issued by the Legal Sector Affinity Group, which comprises the AML Supervisors for the legal sector. You are not required to follow this guidance, but doing so will make it easier to account to oversight bodies for your actions.

This guidance is not legal advice, and does not necessarily provide a defence to complaints of misconduct or inadequate professional service.

However, legal sector regulators will take into account 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.

We are in the process of obtaining approval from HM Treasury for this guidance. Once HM Treasury approval is obtained, 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.

While care has been taken to ensure that this guidance is accurate, up to date and useful, members of the Legal Sector Affinity Group will not accept any legal liability in relation this guidance.

1.6 Terminology in this guidance

Must

A specific requirement in legislation. You must comply, unless there are specific exemptions or defences provided for in relevant legislation.

Should

Outside of a regulatory context, good practice for most situations in the Legal Sector Affinity Group's view.

These may not be the only means of complying with legislative or regulatory requirements and there may be situations where the suggested route is not the best possible route to meet the needs of your client. However, if you do not follow the suggested route, you should be able to justify to oversight bodies why the alternative approach you have taken is appropriate, either for your practice, or in the particular retainer.

May

A non-exhaustive list of options for meeting your obligations or running your practice. Which option you choose is determined by the profile of the individual practice, client or retainer. You may be required to justify why this was an appropriate option to oversight bodies.

Chapter 2 - Risk-based approach

Note: References to client accounts and management of trusts, companies and charities in sections 2.3.2.2, 2.4.2 and 2.4.5 do not apply to barristers or advocates for the reasons set out in section 1.1.1.

2.1 General comments

The possibility of being used to assist with money laundering and terrorist financing poses many risks for the practice of an independent legal professional, including:

- criminal and disciplinary sanctions for the practice and individuals in the practice
- civil action against the practice as a whole, as well as certain individuals
- damage to reputation leading to a loss of business.

These risks must be identified, assessed and mitigated, just as you do for all business risks facing your practice. If you know the risks that you face generally and know your client well and understand your instructions thoroughly, you will be better placed to assess risks and spot suspicious activities.

Adopting a risk-based approach to preventing money laundering means that you focus your resources on the areas of greatest risk. The resulting benefits of this approach include:

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

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 and to make reports of suspicious activities once a suspicion is held. However, the risk-based approach still applies to ongoing monitoring of clients and retainers and this will enable you to identify suspicions.

Money laundering and terrorist financing risks vary across the legal sector and your practice's particular risk-based processes should be lead by an assessment of:

- the activities you undertake,
- the existing professional and ethical rules and regulations to which you are subject, and
- the susceptibility of the activities of your practice to money laundering and terrorist financing in the particular countries in which your practice operates.

2.2 Requirement to undertake and maintain a practice-wide risk assessment

Under Regulation 18(1) an independent legal professional's practice is required to carry out and maintain a documented practice-wide risk assessment to identify and

assess the risk of money laundering and terrorist financing to which the business is subject.

You must:

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

No matter how thorough your risk assessment or how appropriate your controls, some criminals may still succeed in exploiting your practice for criminal purposes. Nevertheless, a comprehensive practice-wide risk assessment combined with appropriate risk-based judgments on individual clients and retainers will enable you to justify your decisions and actions to law enforcement agencies, the courts and your supervisory authority.

2.3 Assessing your practice's risk profile

In carrying out your practice-wide risk assessment you must take into account:

- information on money laundering and terrorist financing risks made available to you by your supervisory authority following their own risk assessment, and
- risk factors relating to:
    - your customers
    - the countries or geographic areas in which your business operates
    - your products or services
    - your transactions, and
    - your delivery channels.

In addition, you should consider the nature of any issues raised in SARs made by your MLRO and consult the key contact in your organisation to understand any risks they may have identified.

Your risk assessment may also include consideration of:

- the UK's National Risk Assessment,
- the EU's Supra-National Risk Assessment
- the FATF Risk-based Approach Guidance for Legal Professionals
- if you provide services in any other jurisdictions, any relevant FATF mutual evaluations, national risk assessments, or publicly available materials in respect of the risks in those jurisdictions; and

- any other material which may be relevant to assess the risk level particular to your practice, for example, press articles highlighting issues that may have arisen in particular jurisdictions.

Having assessed the money laundering and terrorist financing risks your practice faces you should then consider any mitigating factors or reasonable controls that you can implement to manage these risks and reduce their significance to an acceptable level.

2.3.1 Customer risk factors

When assessing risk factors relating to your customers you should consider the demographic of your client base. Factors which may affect the level of risk associated with your client base are set out below.

2.3.1.1 High client turnover v stable client base

Although not determinative, you should take into account the length and strength of your typical client relationships.

If you have long-term and strong relationships with your clients you will be in a better position to identify any potential money laundering issues, which may mean your practice is at a lower risk of being subject to money laundering or terrorist financing (although you should always be mindful of clients that put pressure on you citing their long-standing relationship). Conversely, if you tend to have shorter relationships and a higher client turnover, you may conclude that the lack of a long and strong client relationship means your practice faces greater risk.

2.3.1.2 Clients based in high-risk jurisdictions

Country risk factors should feature prominently in your assessment of the money laundering and terrorist financing risks your practice faces. 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:

- have deficient anti-money laundering legislation, systems and practice
- have high levels of acquisitive crime or higher levels of corruption
- are considered to be 'offshore financial centres' or tax havens
- permit nominee shareholders to appear on the share certificate or register of owners.

The European Commission has been empowered under the 4th Directive to publish a list of 'high risk third countries', contained in Commission Delegated Regulation (EU) 2016/1675. However, you should note that there may be other jurisdictions that present a high risk of money laundering that are not on the European Commission list of 'high risk third countries'.

FATF 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 characterised as countries which have economic or sociological constraints preventing them from implementing AML/CTF measures effectively.

In addition, information is publicly available on bribery and corruption risks and about countries regarded as secrecy jurisdictions (or jurisdictions that permit the use of nominee shareholders).

Online resources you may consult include:

- FATF and HM Treasury statements on unsatisfactory money laundering controls in overseas jurisdictions.
- The International Bar Association's summary of money laundering legislation around the world.
- Transparency International's corruption perception index.

2.3.1.3 Clients in higher risk sectors

Given the wider international focus and extra territorial issues surrounding anti-bribery and corruption laws in some jurisdictions, you should take into consideration the elevated risks attached to certain sectors when carrying out your practice-wide risk assessment.

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/EU sanctions.

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

- public work contracts and construction, including post-conflict reconstruction
- real estate and property development
- the oil and gas industry
- the nuclear industry
- mining (including diamond mining and trading)
- arms manufacturing/supply and the defence industry

Clearly not all work in these sectors will be higher risk but it is essential to be aware of the potential for risk so that you can implement procedures for closer scrutiny on client and matter acceptance.

2.3.1.4 Acting for politically exposed persons (PEPs)

An independent legal professional’s exposure to PEPs is also a major consideration in carrying out your practice-wide risk assessment. A PEP may be a client or a beneficial owner of a client but it is important to consider the type of PEPs that you act for and whether the work to be undertaken will affect your overall risk profile.

PEPs are considered in section 4.12.2.

2.3.1.5 Acting for clients without meeting them

In an increasingly global and technologically advanced environment, it is commonly the case that you will act for clients without meeting them You should include this as a factor when you carry out your practice-wide risk assessment. In addition, you should consider the systems and procedures that you have implemented to mitigate the risks associated with acting for clients you do not meet.

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 must be comfortable that you can mitigate the risks of identity fraud.

2.3.1.6 Clients with high cash turnover businesses

You should consider whether your practice frequently acts for clients who operate or benefit from high cash turnover businesses as these businesses may be appealing to criminals seeking to launder money.

2.3.2 Services and areas of law and geographical location of services provided

In carrying out your practice-wide risk assessment you must consider risks associated with the services you provide, the transactions you participate in and the countries or geographic areas in which you operate.

2.3.2.1 Services and areas of law

Many studies have highlighted that independent legal professionals face the greatest potential risks in the following areas:

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

The involvement of your practice in the sale/purchase of real property, creation of trusts, companies and charities, and management of trusts and companies does not automatically lead to the conclusion that your business is high risk. However, you should consider these areas and consider other risk factors, such as jurisdictional or sector risk, in the context of your business so that you can put in place additional controls where necessary to minimise the risk of money laundering.

Other areas of risk focus more closely on factors which may be more prevalent when considering a particular client or mandate, including unusually complicated transactions. You should consider how you might ensure that your staff can identify the warning signs as part of your risk assessment.

Criminals are constantly developing new techniques, so no list of examples can ever be exhaustive. This section does, however, provide some further guidance on areas of money laundering risk.

2.3.2.2 Client accounts and payments

In carrying out your practice-wide risk assessment you should take into account the risk that criminals may attempt to misuse/abuse your client account. You must ensure that you only use client accounts to hold client money for legitimate transactions where this is incidental to the legal services you supply. Putting the proceeds of crime through your client account can give them the appearance of legitimacy, 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. Therefore, the use of cash may be a warning sign.

Legal professionals should not provide a banking service for their clients.

2.3.2.3 Sale/purchase of real property

Law enforcement authorities believe that the 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.

2.3.2.4 Creation and management of trusts, companies and charities

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.

Shell companies are corporate entities that do not have any business activities or recognisable assets. They may be used for legitimate purposes such as serving as transaction vehicles. 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 be suspicious if a client engages your services only in connection with the routine aspects of forming an entity, without seeking 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 register the engagement of a legal professional to register the company may indicate that the client is seeking to add legitimacy to a shell company.

2.3.2.5 Sham litigation

Litigation may constitute sham litigation if the subject of the dispute is fabricated (there is no actual claim and the litigation is a merely a pretext for transferring the proceeds of crime from one entity to another, possibly through a client account) or if the subject of the litigation is a contract relating to criminal activity that a court would not enforce.

2.3.2.6 Geographical location of services

You should carefully consider the jurisdictions in which you are offering your services and whether there are any particular local issues of which you ought to be aware

which may impact on your risk assessment. Information on jurisdictional issues is set out above in section 2.3.1.2.

2.4 Mitigating factors

This section sets out mitigating factors that you may wish to incorporate into your policies and procedures in order to address the potential threats/areas of risk identified above.

2.4.1 Client demographic risks

- Conduct thorough due diligence taking a risk-based approach and avoiding tick box processes.
- Understand the risks in the jurisdictions in which your clients are based or have their operations and the sectors in which they operate.
- Introduce a means of identifying potentially higher risk issues and do internet-based research on higher risk clients or beneficial owners.
- Probe source of funds in higher risk cases, including where shareholders have no apparent online presence but the transaction value is substantial.

2.4.2 Client accounts/payments

- Ensure that you comply with the client account rules of your regulator.
- Prohibit the use of your client account without the accompanying legal services and include a process to ensure that information about all payments is cross-checked.
- Conduct thorough CDD before taking money on account, including understanding the transaction.
- Avoid disclosing your client account details as far as possible, discourage clients from passing the details on to third parties, ask them to use the account details only for previously agreed purposes and make it clear that electronic transfer of funds is expected. If you need to provide your account details, ask the client where the funds will be coming from. Will it be an account in their name, from the UK or abroad? Consider whether you are prepared to accept funds from any source that you are concerned about.
- Restrict cash payments. Large payments made in actual cash may also be a sign of money laundering. It is good practice to establish a policy of never accepting cash payments above a certain limit either at your office or into your bank account. 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 transaction. If a cash deposit is received, you will need to consider whether you think there is a risk of money laundering taking place and whether it is a circumstance requiring a disclosure to the NCA.
- Accounts staff should monitor whether funds received from clients are from credible sources.

- Ensure appropriate checks are made and the rationale for and size of a transaction and any payments into your accounts by third parties is clearly understood before any third party payments are accepted into the client account. You may not have to make enquiries into every source of funding from other parties. However, you must always be alert to warning signs and in some cases you will need to get more information.
- Where money is accepted into the client account in respect of a transaction or from a client on account and the transaction is aborted, carefully consider the level of risk analysis and CDD conducted at the outset, the legitimacy of the transaction and the parties to it, and the circumstances of the aborted transaction. You should not return funds without considering the need to make a suspicious activity report. Only return funds to the original sender of those funds and not to any other designated person.

2.4.3 Sale/purchase of real property

- Perform thorough CDD checks.
- Keep up-to-date with emerging issues. It may be useful to review resources from law societies or bar associations 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.
- Information overload can be a warning sign. Money launderers may attempt to inundate the legal professional with information to reduce the chances that they spot the issue or to make them convinced of the transaction's legitimacy.

2.4.4 Creation of trusts, companies and charities

- Perform thorough CDD checks. 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, conduct further investigation.
- Seek to understand all aspects of the transaction.

2.4.5 Management of trusts and companies

- Ask whether there is a legal reason or it is it customary to have a legal professional on the board of an entity in the relevant country.
- Perform checks on the entities concerned to minimise the money laundering risk.
- Provide information and/or training, where appropriate, to staff on possible red flags.

2.4.6 Unusual transactions

- Do further due diligence, particularly on source of funds.
- Seek to understand the commercial rationale/reason for the transaction structure.
- Provide training on possible red-flags. See section 3.7 on training requirements and Chapter 12 on money laundering warning signs.

2.5 Assessing individual client and retainer risk

Under Regulation 28(12)(a)(i) and (ii), the way in which you comply with CDD requirements must reflect both your practice-wide risk assessment and your assessment of the level of risk arising in the particular case.

In assessing the level of risk arising in a particular case you must take into account:

- the purpose of the transaction or business relationship,
- the size of the transactions undertaken by the customer and
- the regularity and duration of the business relationship.

You should also consider whether:

- Your client is within a high-risk category, including whether:
    - they are based or conduct their business in high-risk jurisdictions and/or sectors
    - the retainer involves high-risk jurisdictions, or appears to fall outside of the sector in which the client ordinarily operates.
- Extra precautions should be taken when dealing with funds or clients from a particular jurisdiction. This is especially important if the client or funds come from a jurisdiction where the production of drugs, drug trafficking, terrorism or corruption is prevalent.
- In the event you are aware of negative press or information in respect of your client, which gives you cause for concern in relation to money laundering compliance, you may need to consider:
    - the nature and seriousness of any allegations
    - timing of any allegations and whether any steps might have been taken to address previous problems that have arisen and whether any proceeds of crime have been extracted by a fine
    - the level of press coverage and whether the sources of the allegations are reliable or if there is doubt as to their veracity.
- You can be easily satisfied the CDD material for your client is reliable and allows you to identify the client and verify their identity.
- You can be satisfied that you understand their ownership and control structure (particularly if the client or entities in the control structure are based in jurisdictions which permit nominee owners).

- There are concerns about the source of funds or wealth or there are payments to be made by unconnected third parties or payments in cash.
- The retainer involves an area of law or service at higher risk of laundering or terrorist financing.
- Whether the instructions might be considered to be unusual or higher risk, for example:
    - unusually complicated financial or property transactions or transactions where the commercial rationale is unclear
    - instructions on transactional work outside your area of expertise
    - transactions involving various potentially connected private individuals (as clients or as beneficial owners) in higher risk jurisdictions
    - transactions with an unexplained cross-border element

This assessment will help you to consider whether you are comfortable acting in the particular circumstances and, if so, to adjust your internal controls to the appropriate level of risk presented by the individual client or the particular retainer. Different aspects of your CDD controls will meet the different risks posed:

- If you are satisfied that you have verified the client's identity, but the retainer is high risk, you may require fee earners to monitor the transaction more closely, rather than seek further verification of identity.
- If you have concerns about verifying a client's identity, but the retainer is low risk, you may expend greater resources on verification and monitor the transaction in the normal way.

Risk assessment is an ongoing process both for the practice generally and for each client, business relationship and retainer. It is the overall information held by the legal professional gathered while acting for the client that will inform the risk assessment process, rather than sophisticated computer data analysis systems. The better you know your client and understand your instructions, the better placed you will be to assess risks and spot suspicious activities.

Chapter 3 – Systems, policies, procedures and controls

3.1 General comments

Develop and document systems to meet your obligations and risk profile in a risk-based and proportionate manner. Policies and procedures supporting these systems enable staff to apply the systems consistently and demonstrate to supervisors that processes facilitating compliance are in place.

3.2 Application and requirements

Regulation 19 requires the regulated sector to have written policies, controls and procedures (PCPs) in place to mitigate and manage the AML and CTF risks identified in the practice's risk assessment.

These PCPs need to be proportionate to the size and nature of your practice. They must include:

1. PCPs which provide for the identification and scrutiny of matters where:

    - a transaction is complex and unusual and has no apparent economic or legal purpose
    - there is an unusual pattern of transactions and they have no apparent economic or legal purpose
    - there appears to be no apparent economic or legal purpose, or where the commercial rationale is unclear, and a high risk of money laundering is present.

    Legal professionals must carefully consider whether it is appropriate for them to proceed on a matter in the absence of a clear understanding of the nature and purpose of the transaction.

2. Consideration of additional measures to prevent the misuse of products and transactions which favour anonymity.

    It is important that you are able to distinguish between those legal services that you provide and/or transactions in which you act which provide or allow the client a legitimate level of anonymity and those where no good reason for that anonymity has been established and understood.

    Additional measures could include ensuring a better understanding of the background of the transaction and your role in the matter and/or any wider transaction.

3. Consideration of the AML/CTF risk posed to the practice by new technology/legal service delivery methods adopted by the practice.

Effective management of AML and CTF risks are the responsibility of senior management. As such, all PCPs must be approved by senior management.

Those operating in the regulated sector must ensure their PCPs are documented and available to all relevant staff.

You must regularly review and update your PCPs and maintain a written record of any changes you make to them following such a review. You must also maintain a written record of the steps that you have taken to communicate your PCPs, and any changes to your PCPs, to your staff.

It is vital that, where staff make decisions in line with the PCPs identified by the practice, they record their decisions and, where appropriate, the decision-making process either on the client record or matter file.

3.3 Group-wide application

Practices must consider the application of the Regulations to their wider group. Where a practice is a parent undertaking, it must ensure that its PCPs apply to:

1. All subsidiary undertakings, including those located outside the UK, and
2. All branches established outside the UK, which carry out activities that would fall in the regulated sector in the UK.

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

Subsidiaries/branches outside of the EEA: If any of the subsidiary undertakings or branches of a parent undertaking are established in a country outside of the EEA which does not impose requirements to counter money laundering and terrorist financing as strict as those of the United Kingdom, the relevant parent undertaking must ensure that those subsidiary undertakings and branches apply measures equivalent to those required by the UK's implementation of the Regulations, as far as permitted under the law of that country.

In the unlikely event that the law of a country does not permit the application of such equivalent measures by the branch or subsidiary undertaking established in that country, the relevant parent undertaking must:

a) inform its supervisory authority accordingly; and
b) take additional measures to handle the risk of money laundering and terrorist financing effectively, which should be clearly documented.

As with your practice-wide PCPs, you must regularly review and update your group-wide PCPs and maintain a written record of any changes that you make to them following such a review. You must also maintain a written record of the steps that you have taken to communicate your group wide PCPs, and any changes to them, to your staff.

3.4 Areas to cover

Practices must ensure they have PCPs which address:

1. Risk management practices.
2. Internal controls.
3. CDD controls.

4. Reliance and record keeping.
5. Disclosures to the NCA (and decisions not to make disclosures to the NCA).
6. The monitoring and management of compliance with the PCPs.

3.4.1 Risk management practices

Practices must ensure that they have documented their understanding of the key AML/CTF risks that they face.

They should keep a record of the sources used in completing their AML/CTF risk assessment.

It is important that decisions taken in relation to the application of the PCPs are documented. For example, if a decision is taken to adopt extra controls in relation to a client or matter, you should record the reason for the additional controls and the nature of the controls.

In relation to your risk management practices you may also wish to consider:

- the level of personnel permitted to exercise discretion on the risk-based application of the Regulations, and the circumstances under which that discretion may be exercised
- the CDD requirements to be met for simplified, standard and enhanced due diligence
- when outsourcing of CDD obligations or reliance will be permitted, and on what conditions
- how you will restrict work being conducted on a file where CDD has not been completed
- the circumstances in which delayed CDD is permitted
- when cash payments will be accepted
- when payments will be accepted from or made to third parties
- the manner in which disclosures are to be made to the nominated officer.

3.4.2 Internal controls

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'. Factors you may consider when determining whether it is appropriate to apply those controls include:

- The number of staff members 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
- The nature and complexity of work your practice undertakes

- The level of visibility and control that senior management has over client matters

You should consider each of the controls set out in Regulation 21(1) separately and need only apply those which are appropriate having regard to the size and nature of your practice.

The controls referred to in Regulation 21(1) are:

1. Appointing an individual as the officer responsible for the practice's compliance with the Regulations.

   The individual must be either a member of the board of directors (or equivalent management body) or senior management.

   A member of senior management means an officer or employee with sufficient knowledge of your practice's money laundering and terrorist financing risk exposure and sufficient authority to take decisions affecting that risk exposure.

   The requirement to appoint an officer responsible for compliance with the Regulations is additional to the requirement to appoint an MLRO. However, your practice's officer responsible for compliance with the Regulations may also be your MLRO or, if applicable, your Compliance Officer for Legal Practice, provided they are of sufficient seniority.

2. Screening relevant employees prior to and during the course of their employment in relation to their skills and knowledge and their conduct and integrity.

   Screening could mean having regard to:

   - a person's qualifications
   - any regulatory, professional and/or ethical obligations to which the person is subject
   - checking a person's references.

   A 'relevant employee' 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.

3. Establishing an independent audit function to examine, evaluate and make recommendations regarding the adequacy and effectiveness of the practice's PCPs.

   You will need to consider the following factors:

   - The size of your practice. Smaller practices are unlikely to need such a function, assuming that the individuals within the practice feel that they have a good understanding of the clients and matters undertaken.

- The volume of work. Does your practice manage a high volume of work undertaken by relatively junior staff?
- Complexity of the practice and the work undertaken.
- The extent of the PCPs in place to manage the risks identified in your practice's risk assessment.

An independent audit function does not have to be external to the practice but must be independent of the specific function being reviewed. The independent auditor should have the authority to:

- Access all relevant material to be able to evaluate the adequacy and effectiveness of the PCPs.
- Make recommendations in relation to those PCPs.
- Monitor the practice's compliance with its recommendations.

You should take a risk-based approach to determining how frequently an independent audit should take place. An independent audit will not necessarily need to be carried out annually, but should occur following material changes to your practice's risk assessment.

3.4.3 Nominated officers

Regulation 21(3) requires that all practices within the regulated sector must have a nominated officer to receive disclosures under Part 7 of POCA and the Terrorism Act, and to make disclosures to the NCA.

Regulation 21(6) provides that there is no requirement to have a nominated officer in the regulated sector if you are an individual who provides regulated services but do not employ any people or act in association with anyone else.

Practices who do not provide services within the regulated sector should consider appointing a nominated officer, even though it is not required under the Regulations, because POCA and the Terrorism Act still apply. You may also be subject to regulatory requirements to have business management systems facilitating compliance with legal obligations.

You will need to inform your supervisor of the identity of your MLRO and officer responsible for compliance with the Regulations within 14 days of appointment. You will also need to inform your supervisor of any subsequent appointments to either of those positions within 14 days.

Who should be a nominated officer?

Your nominated officer 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. They should also be in a position of sufficient responsibility to enable them to have access to all of your practice's client files and business information, when necessary, to enable them to make the required decisions on the basis of all information held by the practice.

Practices authorised by the FCA will need to obtain the FCA's approval for the appointment of the nominated officer as this is a controlled function under section 59 of the Financial Services and Markets Act 2000.

Role of the nominated officer

Your nominated officer is responsible for ensuring that, when appropriate, the information or other matter leading to knowledge or suspicion, or reasonable grounds for knowledge or suspicion of money laundering is properly disclosed to the relevant authority. The decision to report, or not to report, must not be subject to the consent of anyone else. Your nominated officer will also liaise with the NCA or law enforcement on the issue of whether to proceed with a transaction or what information may be disclosed to clients or third parties.

A range of factors, including the type of practice, its size and structure, may lead to the nominated officer delegating certain duties regarding the practice's AML/CTF obligations. In some large practices, one or more permanent deputies of suitable seniority may be appointed. All practices will need to consider arrangements for temporary cover when the nominated officer is absent.

Responding to enquiries from law enforcement agencies

In accordance with Regulation 21(8), practices 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.

Responses must factor in legal professional privilege, which is not overridden by such requests. Legal professional privilege is covered in more detail in Chapter 7.

3.4.4 Customer due diligence

You are required to have a system outlining the CDD measures to be applied to specific clients. Your risk assessment should record your practice's risk tolerances so that you are able to demonstrate to your supervisor that your CDD measures are appropriate.

Your CDD system may include:

1. When CDD is to be undertaken.
2. Information to be recorded on client identity.
3. Information to be obtained to verify identity, either specifically or providing a range of options with a clear statement of who can exercise their discretion on the level of verification to be undertaken in any particular case.
4. When simplified due diligence may occur.
5. What steps need to be taken for enhanced due diligence.
6. What steps need to be taken to ascertain whether your client is a PEP and subsequent controls that will be put in place.
7. When CDD needs to occur and under what circumstances delayed CDD is permitted.

8. How to conduct CDD on existing clients and how often CDD information will be reviewed to ensure that it is up to date.
9. What ongoing monitoring is required.

For further information on conducing CDD see Chapter 4.

3.4.5 Reliance and Record Keeping

Reliance

Your PCPs must cover reliance, which is discussed further in section 4.4. You should consider including in your PCPs:

- the circumstances in which you consider it appropriate to rely on another regulated person, and
- the steps you will take when relying on another regulated person to satisfy yourself that they have complied fully with the requirements of the Regulations.

Record keeping

Your PCPs should set out how your business complies with the record keeping obligations contained in the Regulations, which are discussed further in section 4.8.

3.4.5 Monitoring Compliance with PCPs

Practices must ensure that they regularly review their risk assessment and PCPs, even if they have determined that the size and nature of the practice is such that an independent audit function is not required.

Monitoring compliance will assist you to assess whether the PCPs that you have implemented are effective in identifying and preventing money laundering and terrorist financing opportunities within your practice. Issues which may be covered in such a review may include:

1. Procedures to be undertaken to monitor compliance, which may involve:
    - random file audits
    - file checklists to be completed before opening or closing a file
    - a nominated officer's log of situations brought to their attention, queries from staff and reports made.
2. Reports to be provided to senior management on compliance.
3. How to rectify lack of compliance, when identified.
4. How lessons learnt will be communicated back to staff and fed back into the risk profile of the practice.

3.5 Disclosures

Practices (except sole practitioners) must have a system clearly setting out the requirements for making a disclosure under POCA and the Terrorism Act. These may include:

- the circumstances in which a disclosure is likely to be required
- how and when information is to be provided to the nominated officer or their deputies
- resources which can be used to resolve difficult issues around making a disclosure
- how and when a disclosure is to be made to the NCA
- how to manage a client when a disclosure is made while waiting for consent/DAML
- the need to be alert to tipping off issues

For details on when a disclosure needs to be made see Chapters 6, 7 and 8. For details on how to make a disclosure see Chapter 9.

3.6 Record keeping

Various records must be kept to comply with the Regulations and defend any allegations against the practice in relation to money laundering and failure to report offences. Your records system must outline what records are to be kept, the form in which they should be kept and for how long they should be kept.

Regulation 40 requires that you keep records of CDD material and supporting evidence and records in respect of the relevant business relationship or occasional transaction. Adapt your standard archiving procedures for these requirements.

3.6.1 CDD material

You may keep either a copy of CDD material, or references to it. Keep it for five years after the business relationship ends or the occasional transaction is completed. At the end of the five year period you must delete any personal data in the record unless:

- you are required to retain records containing personal data under any enactment or rule made by your regulator, or
- you are required to retain records containing personal data for the purposes of any court proceedings, or
- you have the express consent of the person whose data it is.

Consider holding CDD material separately from the client file for each retainer, as it may be needed by different groups in your practice.

Depending on the size and sophistication of your practice's record storage procedures, you may wish to:

- scan the CDD material and hold it electronically

- 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
- keep electronic copies or hard copies of the results of any electronic verification checks
- record reference details of the CDD material sighted.

The option of merely recording reference details may be particularly useful when taking instructions from clients at their home or other locations away from your office. The types of details it would be useful to record include:

- any reference numbers on documents or letters
- any relevant dates, such as issue, expiry or writing
- details of the issuer or writer
- all identity details recorded on the document.

Where you are relied upon by another person under Regulation 39 for the completion of CDD measures, you must keep the relevant documents for five years from the date on which you were relied upon.

3.6.2 Risk assessment notes

Under the Regulation 28(12)(a)(i) and (ii), the way in which you comply with CDD requirements must reflect both your practice-wide risk assessment and your assessment of the level of risk arising in the particular case.

You should consider keeping records of decisions on risk assessment processes of what CDD was undertaken. This does not need to be in significant detail, but merely a note on the CDD file stating the risk level you attributed to a file and why you considered you had sufficient CDD information. For example:

> 'This is a low risk client with no beneficial owners providing medium risk instructions. Standard CDD material was obtained and medium level ongoing monitoring is to occur.'

Such an approach may assist practices to demonstrate they have applied a risk-based approach in a reasonable and proportionate manner. Notes taken at the time are better than justifications provided later.

3.6.3 Supporting evidence and records

You must keep all original documents or copies admissible in court proceedings.

Records of a particular transaction, either as an occasional transaction or within a business relationship, must be kept for five years after the date on which the transaction is completed.

All other documents supporting records must be kept for five years after the completion of the business relationship.

3.6.4 Suspicions and disclosures

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:

- ongoing monitoring undertaken and concerns raised by fee earners and staff
- discussions with the nominated officer regarding concerns
- advice sought and received regarding concerns
- why the concerns did not amount to a suspicion and a disclosure was not made
- copies of any disclosures made
- conversations with the NCA, law enforcement agencies, insurers and supervisory authorities regarding disclosures made
- decisions not to make a report to the NCA which may be important for the nominated officer to justify his or her position to law enforcement agencies.

You should ensure that records are not inappropriately disclosed to the client or third parties to avoid offences of tipping off and prejudicing an investigation, and to maintain a good relationship with your clients. This may be achieved by maintaining a separate file, either for the client or for the practice area.

3.6.5 Data protection

The Data Protection Act 1998 applies to you and the NCA. It allows clients or others to make subject access requests for data held by you. Such requests could cover any disclosures made.

Section 29 of the Data Protection Act 1998 states that you need not provide personal data where disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

HM Treasury and the Information Commissioner have issued guidance which essentially provides that the section 29 exception would apply where granting access would amount to tipping off. This may extend to suspicions only reported internally within the practice.

If you decide that the section 29 exception applies, document steps taken to assess this, to respond to any enquiries by the Information Commissioner.

Under Regulation 41(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 enactment or you have the person's express consent. In addition, you are required to provide new clients with the registrable particulars of your practice within the meaning of section 16 of the Data Protection Act 1998 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.

3.7 Communication and training

Your staff members are the most effective defence against launderers and terrorist financiers who would seek to abuse the services provided by your practice.

Regulation 24 requires that you ensure relevant employees:

- 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, and
- 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.

Professional regulatory requirements may also oblige you to train your staff to a level appropriate to their work and level of responsibility.

3.7.1 Criminal sanctions and defences

Receiving insufficient training is a defence for individual staff members who fail to report a suspicion of money laundering, provided they did not know or suspect money laundering. However, it is not a defence to terrorist funding charges, and leaves your practice vulnerable to sanctions under the Regulations for failing to properly train your staff.

3.7.2 Who should be trained?

When setting up a training and communication system you should consider:

- which staff require training
- what form the training will take
- how often training should take place
- how staff will be kept up-to-date with emerging risk factors for the practice

Assessments of who should receive training should include who deals with clients in areas of practice within the regulated sector, handles funds or otherwise assists with compliance. Consider fee earners, reception staff, administration staff and finance staff, because they will each be differently involved in compliance and so have different training requirements.

Training can take many forms and may include:

- face-to-face training seminars
- completion of online training sessions
- attendance at AML/CTF conferences
- participation in dedicated AML/CTF forums
- review of publications on current AML/CTF issues
- practice or practice group meetings for discussion of AML/CTF issues and risk factors.

Providing an AML/CTF policy manual is useful to raise staff awareness and can be a continual reference source between training sessions.

3.7.3 How often?

You must give your employees relevant training at regular and appropriate intervals. In determining whether your training programme meets this requirement, you should have regard to the practice's risk profile and the level of involvement certain staff have in ensuring compliance.

You should consider retaining evidence of your assessment of training needs and steps taken to meet such needs.

You should also consider:

- criminal sanctions and reputational risks of non-compliance
- developments in the common law
- changing criminal methodologies.

You should take a risk-based approach to determining how often training should take place. Some type of training every two years is preferable.

3.7.4 Communicating with your clients

While not specifically required by the Regulations, we consider it useful for you to tell your client about your AML/CTF obligations. Clients are then generally more willing to provide required information when they see it as a standard requirement.

You may wish to advise your client of the following issues:

- the requirement to conduct CDD to comply with the Regulations
- whether any electronic verification is to be undertaken during the CDD process
- the requirement to report suspicious transactions.

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

Chapter 4 – Customer due diligence

Note: Section 4.12.2.4 (Senior management approval) of this Chapter may not apply to self-employed barristers or advocates who are practising from chambers or as sole practitioners.

4.1 General comments

CDD is required by the Regulations; you are in a better position to identify suspicious transactions if you know your customer and understand the reasoning behind the instructions they give you.

4.2 Application

You must apply CDD on those clients who retain you for services regulated under the Regulations. See section 1.4.5 for further guidance on the scope of the regulated sector.

4.3 CDD in general

4.3.1 When is CDD required?

Regulation 27 requires that you apply CDD when:

- establishing a business relationship
- 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
- you doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.

The distinction between occasional transactions and long-lasting business relationships is relevant to the timing of CDD and the time period for record keeping.

Where an occasional transaction is likely to increase in value or develop into a business relationship, consider conducting CDD early in the retainer to avoid delays later. As relationships change, practices must ensure they are compliant with the relevant standard.

There is no obligation to conduct CDD in accordance with the Regulations for retainers involving non-regulated activities. However, many practices do conduct CDD on all new clients, regardless of the nature of the matter. This enables you to know your client from the outset and clients can be 'passported' easily between a practice's non-regulated and regulated departments.

4.3.2 What is CDD?

Regulation 28 requires that you:

- Identify the client and verify their identity on the basis of documents or information obtained from a reliable source which is independent of the client, 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. This includes taking reasonable measures to understand the ownership and control structure of a legal person, trust, company, foundation or similar legal arrangement.
- Assess and where appropriate obtain information on the purpose and intended nature of the business relationship or occasional transaction.

Identification and verification

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

Verification is obtaining some evidence which supports this claim of identity.

A risk-based approach

Regulation 28(12) provides that when complying with the requirement to take CDD measures, which may differ from case to case, you must reflect:

- the practice's risk assessment required under Regulation 18, and
- your assessment of the level of risk arising in any particular case.

Regulation 28(13) provides that in assessing the risk you must take account of factors including:

- the purpose of a transaction or business relationship
- the size of the assets or of the transactions undertaken
- the regularity and duration of the business relationship.

You cannot avoid conducting CDD, but you can use a risk-based approach to determine the extent and quality of information required and the steps to be taken to meet the requirements.

4.3.3 General Information - methods of verification

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

- obtaining or viewing original documents
- conducting electronic verification
- obtaining information from other regulated persons
- obtaining information from other reliable publicly available sources

Independent source

You need a reliable source to verify your client's identity, which is independent of the client. This can include materials provided by the client, such as a passport.

Consider the cumulative weight of information you have on the client and the risk levels associated with both the client and the retainer.

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 can provide you with such information. Apply the requirements in a risk-based manner to a level at which you are satisfied that you know who the beneficial owner is.

Regulation 28(9) confirms that the register of people with significant control, or confirmation statement, which is published on the Companies House website, may not be solely relied upon for the purpose of identifying the beneficial owner of a company or LLP client. So, in addition, it will be necessary to obtain further verification, for example confirmation from the client that the information is up to date or other documentation confirming the beneficial ownership of the client.

Documents

You should not ignore obvious forgeries, but you are not required to be an expert in forged documents.

Electronic verification

This will confirm only that someone exists, not that your client is the said person. You should consider the risk implications in respect of the particular retainer and be on the alert for information which may suggest that your client is not the person they say they are. You may mitigate risk by corroborating electronic verification with some other CDD material.

When choosing an electronic verification service provider, you should look for a provider who:

- has proof of registration with the Information Commissioner's Office to store personal data
- 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 a wide range of 'alert' data sources
- 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
- allows you to capture and store the information used to verify an identity.

When using electronic verification, you are not required to obtain consent from your client, but they must be informed that this check will take place.

While electronic verification can be a sufficient measure for compliance with money laundering requirements, there may be circumstances where it will not be appropriate.

4.4 Reliance and outsourcing

Reliance has a specific meaning within the Regulations and relates to the process under Regulation 39 where, in certain circumstances, you may rely on another person to conduct CDD for you, subject to their agreement.

Reliance is an important feature of the Regulations as in certain circumstances it may allow relevant persons to avoid unnecessary duplication in complying with their CDD obligations. As well as reducing the regulatory burden on relevant persons, reliance may be in the interests of your client as it can facilitate swift and convenient access to services. For example, if you instruct another legal professional (or other regulated person) on behalf of your client, then allowing that person to rely on the CDD checks you have already undertaken may enable your client to access those services sooner than they otherwise would have.

It is important to note that reliance, as set out in Regulation 39, is not:

- accepting information from others to verify a client's identity when meeting your own CDD obligations, or
- electronic verification, which is outsourcing.

4.4.1 Relying on a third party

In order to rely on another regulated person to apply CDD measures you must:

- Immediately obtain from the other person all the information needed to satisfy the requirement to apply CDD measures in accordance with Regulations 28(2) to (6) and (10)
- 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 customer or its beneficial owner; and
    - require the third party to retain copies of the data and documents in accordance with Regulation 40.
- Obtain evidence to establish that the person relied upon falls into the category of persons who may be relied upon (per Regulation 40(3)).

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 ask what CDD enquiries the other person has undertaken to ensure that they actually comply with the Regulations and the risk-based approach. This is particularly important when relying on a person outside the UK. Before relying on a person outside the UK you should be satisfied that the CDD has been conducted to a standard compatible with

the 4th Directive, taking into account the ability to use different sources of verification and jurisdictional specific factors.

You should ensure that the CDD information provided to you is not out of date, and be aware that the risk assessment of the person you are relying on may not match your own. It may not always be appropriate to rely on another person and you should consider reliance as a risk in itself.

4.4.2 Granting reliance

Another relevant person may seek to rely on the CDD checks you have completed, and this will often 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 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 be concerned that, by granting reliance, there is a risk you may at some point become liable to the party who relies if they suffer a loss as a result of their reliance. However, to address this concern you may wish to consider adopting an exclusion of liability clause as part of the arrangement allowing reliance between you and the other party. An example (and no more) of such a clause is as follows, though you may wish to revise this dependent upon the circumstances.

[insert clause]

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. If you would be breaching such a contract by granting reliance then you should still confirm to the other party that you have in fact completed CDD checks on the client (although this will not constitute granting reliance).

4.4.3 Reliance in the UK

You can only rely on the following persons in the UK:

- a credit or financial institution as defined in Regulation 10
- auditors, insolvency practitioners, external accountants and tax advisers as defined in Regulation 11
- independent legal professionals as defined in Regulation 12
- trust or company service providers as defined in Regulation 12(2)
- estate agents as defined in Regulation 13
- high value dealers as defined in Regulation 14(1)
- casinos as defined in Regulation 14(2)

4.4.4 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 fourth money laundering directive; and
- supervised for compliance with the requirements laid down in the 4th Directive in accordance with section 2 of Chapter VI of that directive

4.4.5 Reliance in other countries

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

- subject to requirements in relation to CDD and record keeping equivalent to those laid down in the 4th Directive; and
- supervised for compliance with those requirements in a manner equivalent to section 2 of Chapter VI of the 4th Directive

4.4.6 High Risk Third Countries

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

- the third person is a branch or majority owned subsidiary of a person established in an EEA state who is subject to the fourth money laundering directive; and
- the branch or subsidiary complies fully with the procedures and policies established for the group under Article 45 of the 4th Directive

The list of countries designated as high risk third countries by the European Commission is contained in Commission Delegated Regulation (EU) 2016/1675.

4.4.7 Passporting clients between jurisdictions

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 is not considered 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 the implementation of the 4th Directive in that jurisdiction. If further information is required, you should ensure that it is obtained and added to the central database. Alternatively, you could ensure that the CDD approval controls for the database are sufficient to ensure that all CDD is compliant.

Other practices may wish to rely on their international office simply to provide a letter of confirmation that CDD requirements have been undertaken with respect to the client. This is 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 4th Directive, or rules having the equivalent effect; and
- 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.

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 will not be reliance, but outsourcing. Outsourcing is permitted under Regulation 39(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 and, if so, undertake appropriate enhanced due diligence measures.

UK-based fee earners will have to undertake their own ongoing monitoring of the retainer, even if the international office is also required to do so.

4.5 Timing

4.5.1 When must CDD be undertaken?

Regulation 30 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 transaction which amounts to 15,000 Euros or more.

Regulation 31 provides that if you are unable to complete CDD in time, you cannot:

- carry out a transaction with or for the client through a bank account
- establish a business relationship or carry out a transaction otherwise than through a bank account.

You must also:

- terminate any existing business relationship
- consider making a disclosure to the NCA.

You cannot seek consent from the NCA to proceed with a transaction where you have been unable to complete CDD measures as required by Regulation 28.

Although you must 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. You should only make a disclosure to the NCA if you have a reportable suspicion or knowledge of money laundering or terrorist financing and the information is not covered by legal professional privilege. Further information on making a disclosure is contained in Chapter 9 and practical examples are contained in Chapter 13.

Regulation 31(2) confirms that you are not prevented from repaying money deposited in the client account, provided that, if a disclosure to NCA is required, because you have the necessary suspicion, you obtain consent/DAML from NCA for the transaction.

4.5.2 Exceptions to the timing requirement

There are several exceptions to the timing requirement and the prohibition on acting for the client.

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

Normal conduct of business

Regulation 30(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 exception does not apply if your matter is an occasional transaction.

Consider your risk profile when assessing which work can be undertaken on a retainer prior to verification being completed. When applying CDD to a trust, or other legal arrangement or 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 (see Regulation 30 (7)).

Do not undertake substantive work, permit funds to be deposited in your practice's client account, property to be transferred or final agreements to be signed before completion of full verification.

If you are unable to conduct full verification of the client and beneficial owners, then the prohibition in Regulation 31 will apply.

Ascertaining legal position

Regulation 31(3) provides that the prohibition in 31(1) does 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.'

The requirement to cease acting and consider making a report to the NCA when you cannot complete CDD does not apply when you are providing legal advice or preparing for or engaging in litigation or alternative dispute resolution.

This exception does not apply to transactional work, so take a cautious approach to the distinction between advice and litigation work, and transactional work.

4.6 Ongoing monitoring

Regulation 28(11) requires that you conduct ongoing monitoring of a business relationship. 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 the risk profile
- 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 General Data Protection Regulation, which will apply in the UK from 25 May 2018.

You are not required to:

- conduct the whole CDD process again every few years
- suspend or terminate a business relationship until you have updated information or documents, as long as you are still satisfied you know who your client is, and keep under review any request you have made for up to date information or documents
- use sophisticated computer analysis packages to review each new retainer for anomalies.

Many practices operate a system of regular review and renewal of CDD as good practice.

Ongoing monitoring will normally be conducted by legal professionals handling the retainer, and involves staying alert to suspicious circumstances which may suggest money laundering, terrorist financing, or the provision of false CDD material. A high degree of professionalism and scrutiny is expected from legal professionals – see *R v Griffiths & Pattison* (2007) CA which confirmed that legal professionals are expected to fulfill these obligations 'up to the hilt'.

For example, you may have acted for a client in preparing a will and purchasing a modest family home. They may then instruct you in the purchase of a holiday home, the value of which appears to be outside the means of the client's financial situation as you had previously been advised in earlier retainers. While you may be satisfied that you still know the identity of your client, as a part of your ongoing monitoring obligations it would be appropriate in such a case to ask about the source of the funds for this purchase. Depending on your client's willingness to provide you with such information and the answer they provide, you will need to consider whether you are satisfied with that response, want further proof of the source of the funds, or need to discuss making a disclosure to the NCA with your nominated officer.

In circumstances where no subsequent action was taken/change effected as a result of the obligation to conduct ongoing monitoring through the lifecycle of a transaction, it is suggested that practices record:

- that they considered this issue,
- that they took no action , and

- the reasons for that decision.

A brief note to this effect should be recorded.

4.7 New instructions from an existing client

In accordance with Regulation 27(9) you must apply CDD to existing clients on a risk-sensitive basis and when you become aware that the circumstances of the existing client have changed.

In determining this, you must take into account:

- 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
- any other matter which may affect your assessment of the money laundering or terrorist financing risk in relation to the client

It is good practice to refresh the CDD if there has been a gap of over three years between instructions. You must update the CDD when you become aware of any changes to the client's identification information. This will include change of name, address or business.

You are not required to undertake a renewal of CDD if there has been no change in the risk profile of the client, the type of work you are undertaking or their personal details.

4.8 Records

Regulation 40 requires you to keep records of your CDD documents and information and sufficient supporting records in respect of a transaction (whether or not an occasional transaction) which is the subject of CDD or ongoing monitoring to enable the transaction to be reconstructed.

This includes information and documentation obtained in connection with source of funds checks and the process of the transaction itself.

You must retain the records for a period of five years beginning on the date on which you knew or had reasonable grounds to believe that the occasional transaction was complete or the business relationship had come to end.

On expiry of this period, you must delete any personal data, unless:

- you are required to retain it by another enactment
- you are retaining the data for the purposes of any court proceedings
- the client has given consent to the retention
- you have reasonable grounds for believing that the records containing personal data need to be retained for the purposes of legal proceedings.

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.

Many practices will wish to retain the complete file of papers, including CDD records, for a period exceeding that which is 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 any variation on the period prescribed in Regulation 40(3), the client's consent must be obtained. This consent clause can be contained in your engagement letter or terms of business and should be signed or acknowledged by the client.

4.9 CDD on clients

Your practice will need to make its own assessment as to what evidence is appropriate to verify the identity of your clients. We outline a number of sources which may help you make that assessment.

4.9.1 Natural persons

A natural person's identity comprises a number of aspects, including their name, current and past addresses, date of birth, place of birth, physical appearance, employment and financial history, and family circumstances. Their identity must be verified in accordance with Regulation 28, on the basis of documents or information obtained from a reliable source which is independent of the client. You should use information or documents from a reliable source.

Evidence of identity can include:

- identity documents such as passports and photocard driving licences
- other forms of confirmation, including assurances from persons within the regulated sector or those in your practice who have dealt with the person for some time.

In most cases of face to face verification, producing a valid passport or photocard identification should enable most clients to meet the AML/CTF identification requirements.

It is good practice to have either:

- one government document which verifies either name and address or name and date of birth
- 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.

Where it is not possible to obtain such documents, consider the reliability of other sources and the risks associated with the client and the retainer. Electronic verification may be sufficient verification on its own as long as the service provider uses multiple sources of data in the verification process.

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, a

record of identification may include a file note of your satisfaction about identity, usually including an address.

UK residents

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

- current signed passport
- birth certificate
- marriage certificate
- current photocard driver's licence
- current EEA member state identity card
- current identity card issued by the Electoral Office for Northern Ireland
- residence permit issued by the Home Office
- firearms certificate or shotgun licence
- photographic registration cards for self-employed individuals and partnerships in the construction industry
- benefit book or original notification letter confirming the right to benefits
- council tax bill
- utility bill or statement, or a certificate from a utilities supplier confirming an arrangement to pay services on pre-payment terms
- a cheque or electronic transfer drawn on an account in the name of the client with a credit or financial institution regulated for the purposes of money laundering
- bank, building society or credit union statement or passbook containing current address
- entry in a local or national telephone directory confirming name and address
- confirmation from an electoral register that a person of that name lives at that address
- a recent original mortgage statement from a recognised lender
- legal professional's letter confirming recent house purchase or land registry confirmation of address
- local council or housing association rent card or tenancy agreement
- HMRC self-assessment statement or tax demand
- house or motor insurance certificate
- record of any home visit made
- statement from a member of the practice or other person in the regulated sector who has known the client for a number of years attesting to their

identity. Bear in mind you may be unable to contact this person to give an assurance supporting that statement at a later date.

Persons not resident in the UK

Where you meet the client you are likely to be able to see the person's passport or national identity card. If you have concerns that the identity document might not be genuine, contact the relevant embassy or consulate.

The client's address may be obtained from:

- an official overseas source
- a reputable directory
- a person regulated 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 overseas address given.

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

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 CDD measures you apply.

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.
- 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 priest, 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.
- 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.

Professionals

Where other professionals use your services in their capacity as a professional rather than a private individual, you may consult their professional directory to confirm the person's name and business address. It will not be necessary to then confirm the person's home address. You may consult directories for foreign professionals, if you are satisfied it is a valid directory, e.g. one produced and maintained by their professional body, and if necessary, you can translate the information unless you already have a sufficient understanding of what it says.

Persons acting on behalf of the client

In accordance with Regulation 28(10) where a person (the representative) purports to act on behalf of your client, you must:

- verify that the representative is authorised to act on your client's behalf
- identify the representative
- verify the identity of the representative on the basis of documents and information from a reliable source which is independent of both the representative and the client.

4.9.2 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 should be sufficient:

- name
- registered address, if any
- trading address

- nature of business.

Other partnerships and unincorporated businesses which are small and have few partners should be treated as private individuals. Where the numbers are larger, they should be treated as private companies.

Where a partnership is made up of regulated professionals, it will 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 the partner instructing you and one other partner, and evidence of the practice's trading address.

For a UK LLP, you should obtain information in accordance with the requirements for companies as outlined below.

4.9.3 Companies

A company is a legal entity in its own right, but conducts its business through representatives. You must identify and verify the existence of the company.

A company's identity comprises its constitution, its business and its legal ownership structure.

Where a company is a well-known household name, you may consider that the level of money laundering and terrorist financing risks are low and apply CDD measures in a manner which is proportionate to that risk.

Where you commence acting for a subsidiary of an existing client, you may have reference to the CDD file for your existing client for verification of details for the subsidiary, provided that the existing client has been identified to the standards of the Regulations.

You will also need to consider the identity of beneficial owners where you cannot apply simplified due diligence.

Public companies listed in the UK

Regulation 28(3) requires that, in all cases, if a client is a corporate body you must obtain and verify:

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

Unless the body corporate is a company listed on a regulated market, you must also take reasonable measures to determine and verify:

- the law to which it is subject and its constitution
- the full names of the board of directors (or equivalent management body) and senior persons responsible for its operations.

In accordance with Regulation 28(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.

The fact that a company's securities are listed on a regulated market is also one of the factors specified in Regulation 37(3) which you must take into account when deciding whether the risk is low and whether to apply simplified due diligence to a particular client. Simplified due diligence can also be applied to a majority-owned subsidiary of such a company.

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 daily newspaper
- information from a reputable electronic verification service provider or online registry.

For a 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
- a note in the parent's or subsidiary's last audited accounts
- information from a reputable electronic verification service provider or online registry
- information from the parent company's published reports, for example, from their website.

The regulated market in the UK is the London Stock Exchange. AIM is not considered a regulated market within the UK, but under the risk-based approach you may feel that the due diligence process for listing on AIM gives you equivalent comfort as to the identity of the company under consideration.

Where further CDD is required for a listed company (i.e. when it is not on a regulated market) obtain relevant particulars of the company's identity.

Verification sources may include:

- a search of the relevant company registry (such as Companies House)
- a copy of the company's certificate of incorporation
- 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. See section 4.6 for further guidance on ongoing monitoring.

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.

You must obtain and verify:

- the name
- the company number or other registration number
- the address of the registered office and principal place of business

You must take reasonable measures to determine and verify:

- the law to which it is subject and its constitution
- the full names of the board of directors(or equivalent management body) and senior persons responsible for its operations.

Sources for verifying corporate identification may include:

- certificate of incorporation
- details from the relevant company registry, confirming details of the company and of the director/s and their address
- filed audited accounts
- information from a reputable electronic verification service provider.

In lower risk cases you may be able to satisfy the requirement to take reasonable steps to determine and verify the law to which the company is subject and its constitution by ensuring that you understand the type of business and transactions the company can engage in.

Regulation 43 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.

Public overseas companies

You must obtain and verify the:

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

You must take reasonable measures to determine and verify the:

- law to which it is subject and its constitution
- full names of the board of directors(or equivalent management body) and senior persons responsible for its operations.

In accordance with Regulation 28(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.

“Regulated market” is defined as follows:

(a) Within the EEA, the meaning given by Article 4.1 (14) of the Markets in Financial Instruments Directive

(b) 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.

(c) Specified disclosure obligations are disclosure requirements consistent with specified articles of:

- The Prospectus Directive [2003/71/EC]
- The Transparency Obligations Directive [2004/109/EC]
- The Market Abuse Regulation [No 596/2014]

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.

Consult the register on the European Securities and Markets Authority website.

Evidence of the company's listed status should be obtained in a manner similar to that for UK public companies. Companies whose listing does not fall within the above requirements should be identified in accordance with the provisions for private companies.

Private and unlisted overseas companies

Obtaining CDD material for these companies can be difficult, particularly regarding beneficial ownership.

You should apply the risk-based approach, looking at the risk of the client generally, the risk of the retainer and the risks presented as a result of the country in which the client is incorporated. Money laundering risks are likely to be lower where the company is incorporated or operating in an EEA state or a country which is a member of FATF.

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

Where you are not obtaining original documentation, you may want to consider on a risk-sensitive basis having the documents certified by a person in the regulated sector or another professional whose identity can be checked by reference to a professional directory.

4.9.4 Other arrangements or bodies

Trusts

Who is the client?

Trusts, including express trusts, do not have legal personality. As such, you cannot take on a trust as your client. When advising in relation to a trust your client may be the either:

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

Determining which of the settlor, the trustee(s), the protector(s) or one or more of the beneficiaries is/are your client(s) will involve an analysis of 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. If your client is represented by an intermediary, ensure that you comply with Regulation 28(10) and identify and verify the intermediary's identity and authority to act on behalf of your underlying client.

Your CDD will also involve identifying and verifying the identity of your settlor client and, if applicable, understanding the settlor's net wealth and the nature and extent of the assets that will be settled on the trust. The information and documents you obtain will depend on whether your client is a natural person or an entity. If the settlor is an entity you will also need to understand its beneficial owner.

When should a trust's beneficial owners be considered?

If you go on to advise a settlor on trust affairs once the trust has been established, and whenever you are instructed by someone involved with an existing trust to advise in relation to it, you will need to extend your CDD to the trust's beneficial owners.

Regulation 28(4)(a) requires a relevant person to identify the beneficial owner 'of a customer' which is beneficially owned by another person. Regulation 6(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 Regulation 6(1).

Does enhanced CDD apply?

UK common law trusts are used extensively in everyday situations and often pose a limited risk of money laundering or terrorist financing. However, trusts are vehicles for holding (often personal) assets because they exist to separate legal and beneficial ownership. Under Regulation 33(6)(a)(iii) you must take into account whether 'the customer is a legal person or legal arrangement that is a vehicle for holding personal assets' as a 'customer risk factor' when you are assessing whether there is a high risk of money laundering or terrorist financing in a particular situation which may oblige you to apply EDD measures.

While you must take this factor into account when deciding whether there is a high risk of money laundering and terrorist financing, you should consider the situation as a whole. Factors that may increase the risk of money laundering or terrorist financing when advising a client in relation to a trust are:

- if the client requests a trust to be used when there seems to be little reason to do so,
- the trust is established in a jurisdiction with limited AML/CTF regulation, or
- there are concerns about the client's net wealth or source of funds which will be contributed to the trust, for example, there are public domain allegations that they may potentially harbour the proceeds of crime.

When assessing whether a situation poses a higher risk of money laundering and terrorist financing you must take into account the risk factors set out in Regulation 33(6). However, as Regulation 33(7) makes clear, the presence of one of these risk factors does not in and of itself mean that a particular situation is high risk. If, having considered the risk factors in Regulation 33(6) and any other relevant warning signs, you determine that a higher risk of money laundering or terrorist financing is present, then you must apply EDD measures.

EDD may also apply because your client or one of the trust's other beneficial owners is established in a high risk third country or a PEP. See section 4.12.2.

Applying EDD measures will involve you understanding:

- your client’s net wealth and, where they have a funding role, their source of funds,
- the amount and nature of the trust assets and
- the background to the trust and purpose for which the trust was set up.

EDD will also involve your applying increased monitoring.

Specific CDD requirements where you are instructed in relation to an existing trust

Bearing the above in mind, where you are instructed in relation to an existing trust, when applying CDD, you may need:

- to obtain and verify the identity of your client (which as above may be the settlor, trustee(s), protector(s) or beneficiary(ies));

- where you act for more than two trustees (or protectors), only to obtain and verify the identity of two trustees (or protectors);
- where you act for several beneficiaries (subject to conflicts issues), to 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);
- if your client (whether the settlor, trustee(s), protector(s) or beneficiary(ies)) is an entity, in each case to identify its beneficial owner;
- where your client has had a trust funding role, to understand your client's net wealth and the source of funds which were contributed (or which were used to acquire assets which were contributed) to the trust;
- to understand the nature and extent of the assets settled on the trust; and
- to 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 you should also identify potential beneficiaries.

Should further CDD be sought if the identified beneficial owner is an entity?

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

The extent of the reasonable 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 investigated. As a trustee has no beneficial interest in the trust assets, you need not, in the absence of any suspicions, identify the ultimate beneficial owner of a professional trustee entity. It may not be necessary to identify the ultimate beneficial owner of an entity beneficiary where it is one of many discretionary beneficiaries.

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

Regulation 6(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.

However, as CDD is a 'snapshot' process, undertaken at commencement of the relevant business relationship, you may wish to 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. This is because 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 Regulation 6(1)(c).

In any event, if you decide not to note individual beneficiaries named in the trust deed or any associated document on the basis that you have assured yourself that their

benefit from the trust has not yet been determined, you should identify any named class of beneficiaries, by its description. For example:

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

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
- 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, on 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.

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

Regulation 6(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.

Regulation 6(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;
- direct, withhold consent to or veto the exercise of one of the above powers.

Regulation 6(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).

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 Regulation 44 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 and onerous 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 Regulation 6(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 likely to be 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.

The information which needs to go on the register in relation to each identified individual is extensive and set out in Chapter 5.

Practical considerations

Applying CDD where you act in relation to an existing trust will usually involve your having sight of the trust deed and, as above, any document which relates to it.

Alternatively, you may be able to rely on assurances from the client or another regulated person who has had an involvement with setting up or managing the trust. However, before doing so, you should note and 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 of the circumstances and is not in itself indicative of a high 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.

Foundations

Foundations may or may not have legal personality. You should investigate whether this is the case (e.g. is the relevant structure incorporated?) and thus whether it is appropriate to take on the foundation as your client or whether, as in the case of a trust, 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, where you act in relation to it, as you would where you act for a client in relation to a trust. Regulation 6(5) provides that 'beneficial owner' in relation to a foundation or other legal arrangement similar to a trust, mean those individuals who hold equivalent or similar positions to the (defined) beneficial owners of trusts.

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
- 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 can be obtained from:

- the Charity Commission of England and Wales.
- the Office of the Scottish Charity Regulator.

- 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 the relevant CDD measures for that business structure. You can also generally get confirmation of their 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.

Due to the increased interest in some charities and not-for-profit organisations from 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.

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, it is preferable to verify the identity of at least two of them. You should consider getting copies of the death certificate, grant of probate or 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.

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

For UK charities, identification details may be verified:

- with reference to the GRO certificate
- through an enquiry to HMRC

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.

Clubs and associations

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

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

- full name
- legal status
- purpose
- any registered address
- 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
- financial statements presented to the annual general meeting
- listing in a local or national telephone directory

Pension funds

Regulation 37 provides that simplified due diligence is permitted where there is a low risk of money laundering or terrorist financing, taking account of the risk assessment for that client/matter and the risk factors referred to in Regulation 37(3).

The risk factors include product and service factors including where the product is a pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

So you will need evidence that the product is such a scheme and so qualifies for simplified due diligence. Such evidence may include:

- a copy of a page showing the name of the scheme from the most recent definitive deed
- a consolidating deed for the scheme, plus any amending deed subsequent to that date, from which you can assess how contributions are made and member's interest assignment rights.

Pension funds or superannuation schemes outside the above definition should be subject to CDD according to their specific business structure.

For information on how to conduct CDD on other funds please see the JMLSG's Guidance.

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 considered.

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
- extract from official government website

Under Regulation 37(3) the fact that the client is a public administration or publicly owned enterprise is one of the factors to take into account 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.

4.10 CDD on a beneficial owner

4.10.1 General comments

When conducting CDD on a client, you will need to identify any beneficial owners within the meaning of Regulation 5. Note that this definition goes beyond the traditional understanding of the meaning of a beneficial owner.

To identify the beneficial owner, obtain at least their name and record any other identifying details which are readily available. You may decide to use records that are publicly available, ask your client for the relevant information or use other sources.

To assess which identity verification measures are needed, consider the client's risk profile, any business structures involved and the proposed transaction.

The key is to understand the ownership and control structure of the client. A prudent approach is best, monitoring changes in instructions, or transactions which suggest that someone is trying to undertake or manipulate a retainer for criminal ends. Simply ticking boxes is unlikely to satisfy the risk-based approach. You must take reasonable

measures to verify the identity of the beneficial owner so you are satisfied that you know who they are.

Appropriate verification measures may include:

- a certificate from your client confirming the identity of the beneficial owner
- a copy of the trust deed, partnership agreement or other such document
- shareholder details from an online registry
- the passport of, or electronic verification on, the individual
- other reliable, publicly available information

It is not enough to rely only on the information contained in a company's register of persons with significant control.

4.10.2 Assessing the risk

Issues you may consider when assessing the risk of a particular case include:

- how well you know your client
- whether your client is a regulated person
- the type of business structure involved in the transaction
- where the business structure is based
- the AML/CTF requirements in the jurisdiction where it is based
- why this business structure is being used in this transaction
- how soon property or funds will be provided to the beneficial owner
- whether/why your client is acting on behalf of someone else

When conducting CDD on beneficial owners within a corporate entity or arrangement, you must:

- understand the ownership and control structure of the client as required by Regulation 5
- identify the specific individuals listed in Regulation 6

The level of understanding required depends on the complexity of the structure and the risks associated with the transaction. For example, it may be sufficient to review the trust deed or partnership arrangement and discuss the issue with your client. In the case of a company, you may obtain a company structure chart from your client directly, their website or their annual reports.

It is vital to understand in what capacity your client is instructing you to ensure that you are identifying the correct beneficial owners.

If for example you are acting for Bank A, which is a corporate entity, to purchase new premises for Bank A, then it would be the shareholders and controllers of Bank A who are the beneficial owners. However, if Bank A is a trustee for XYZ Trust and they have instructed you to sell trust property, then Bank A is instructing you on behalf of the arrangement which is XYZ Trust in their capacity as trustee. The beneficial

owners in that transaction will be those with specified interests in and/or control of the XYZ Trust.

4.10.3 Agency

Regulation 6(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 these cases, it is presumed that the client is himself the beneficial owner, unless the features of the transaction indicate that they are acting on someone else's behalf. So you do not have to proactively search for beneficial owners, but to make enquiries when it appears the client is not the beneficial owner.

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.
- acting as an appointed broker or other agent to conduct a transaction. A 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. 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 may want to obtain further verification of the beneficial owner's identity in line with the suggested CDD methods to be applied to natural persons.

4.10.4 Companies

Regulation 5(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, or
- 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 was 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 Regulation does not apply to a company listed on a regulated market. It does apply to UK limited liability partnerships.

Shareholdings

You should make reasonable and proportionate enquiries to establish whether beneficial owners exist and, where relevant as determined by your risk analysis, verify their identity. These may include:

- getting assurances from the client on the existence and identity of relevant beneficial owners
- getting assurances from other regulated persons more closely involved with the client, particularly in other jurisdictions, on the existence and identity of relevant beneficial owners
- conducting searches on the relevant online registry
- obtaining information from a reputable electronic verification service

You cannot rely solely on the information contained in the company's register of persons with significant control. Where the holder of the requisite level of shareholding of a company is another company, apply the risk-based approach when deciding whether further enquiries should be undertaken.

A proportionate approach

It would be disproportionate 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. You must simply be satisfied that you have an overall understanding of the ownership and control structure of the client company.

Voting rights are those which are currently exercisable and attributed to the company's issued equity share capital.

Companies with capital in the form of bearer shares

These pose a 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 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. This may be achieved by:

- requiring that the shares be held by a regulated person
- getting an assurance that either such a regulated person or the holder of the shares will notify you of any change of records relating to the shares.

Control

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 override internal procedures and control mechanisms.

You should remain alert to anyone with such powers while you are obtaining a general understanding of the ownership and control structure of the corporate entity. Further enquiries are not likely to be necessary. Monitor situations within the retainer where control structures appear to be bypassed and make further enquiries at that time.

4.10.5 Partnerships

Regulation 5(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 Regulation 5(3):

- the property of the entity includes its capital and its profits
- control involves the ability to manage the use of funds or transactions outside of the normal management structure and control mechanisms

You should make reasonable and proportionate enquiries to establish whether beneficial owners exist and, where relevant, verify their identity in a risk-based manner.

Enquiries and verification may be undertaken by:

- receiving assurances from the client on the existence and identity of relevant beneficial owners
- receiving assurance from other regulated persons more closely involved with the client, particularly in other jurisdictions, on the existence and identity of relevant beneficial owners
- reviewing the documentation setting up the partnership such as the partnership agreement or any other profit-sharing agreements

4.10.6 Trusts

See section 4.9.4 above.

4.10.7 Other arrangements and legal entities

Regulation 6(7) provides that where you are dealing with a client who is not a natural person, nor a corporate entity or a trust, then the following individuals are beneficial owners:

- 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 determined, the class or persons in whose main interest the entity or arrangement is set up or operates

- 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 this Regulation.

When applying this Regulation 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 as benefit has yet to be determined
- a class of persons need only be identified by way of 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 involves the ability to manage the use of funds or transactions outside the normal management structure and control mechanisms
- 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

You should make reasonable and proportionate enquiries to establish whether beneficial owners exist and, where relevant, verify their identity in a risk-based manner.

Enquires and verification may be undertaken by:

- asking the client and receiving assurances as to the existence and identity of beneficial owners
- asking other regulated persons more closely involved with the client (particularly in other jurisdictions) and receiving assurances as to the existence and identity of beneficial owners
- reviewing the documentation setting up the entity or arrangement such as its constitution or rules

4.11 Simplified due diligence

Regulation 37 permits simplified due diligence to be undertaken where you determine that the business relationship or transaction presents a low risk of money laundering or terrorist financing taking into account your risk assessment.

4.11.1 What is simplified due diligence?

You have to obtain evidence that the transaction and client or products provided are eligible for simplified due diligence. You will not necessarily need to obtain information on the beneficial owners. You will need to conduct CDD and ongoing monitoring where you suspect money laundering.

4.11.2 Who qualifies for simplified due diligence?

When assessing whether there is a lower risk of money laundering or terrorist financing such that SDD can be applied you must take into account:

- whether the customer is:
    - a public administrator or a publicly owned enterprise
    - an individual resident in a geographical area of lower risk
    - a credit or financial institution which is subject to requirements in national legislation implementing the 4th Directive and supervised for compliance with those requirements in accordance with the 4th Directive
    - a company listed on a regulated market 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 Regulation 37(3)(b)
- geographical 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.

Financial services firms are not required to apply CDD to the third party beneficial owners of pooled accounts held by legal professionals, provided the information on the identity of the beneficial owners is available upon request and the financial services firm's business relationship with the holder of the pooled account presents a low degree of risk.

For further details on the requirements for qualification for simplified due diligence, see Regulation 37.

4.12 Enhanced due diligence

Regulation 33 provides that you will need to apply enhanced due diligence in addition to the CDD measures required in Regulation 28, on a risk-sensitive basis 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 Regulations 17(9) and 47
- the client is a politically exposed person (PEP), or a family member or known close associate of a PEP
- the client or transaction is 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
- wherever the transaction:

    - is complex and unusually large or there is an unusual pattern of transactions, and
    - the transaction or transactions have no apparent economic or legal purpose
- there is any other situation which can present a higher risk of money laundering or terrorist financing

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.

In applying the risk-based approach to the situation you should consider whether it is appropriate to:

- seek further verification of the client or beneficial owner's identity from independent reliable sources
- obtain more detail on the ownership and control structure and financial situation of the client
- request further information on the purpose of the retainer or the source of the funds, and/or
- conduct enhanced ongoing monitoring

4.12.1 Non face-to-face clients

Where a client is a natural person and they are not physically present for identification purposes, you must take this into account when assessing whether there is a high risk of money laundering or terrorist financing and the extent of any EDD measures you should take.

A client who is not a natural person can never be physically present for identification purposes and will only ever be represented by an agent. Although the fact that you do not have face-to-face meetings with the agents of an entity or arrangement is specified as a risk factor under the Regulations, this does not automatically mean that enhanced due diligence must be undertaken. You should consider your risk analysis, the risks associated with the retainer and the client, assess how well standard CDD measures are meeting those risks and decide whether further CDD measures are required.

Ensuring that the first payment in the retainer is through an account opened in the client's name with a credit institution will further help to verify your client's identity.

If such information is not included on the electronic fund transfer, discuss this with the relevant financial or credit institution. Consider taking up the matter with the FCA if the institution refuses to give you written confirmation of the details. Take other steps to verify your client's identity.

4.12.2 Politically exposed persons

PEPs have been a focus of the FATF as there is concern amongst OECD member states that PEPs have used their political position to corruptly enrich themselves.

You should take a risk-based and proportionate approach to identifying PEPs and then applying EDD measure and treat business with PEPs on a case by case basis. When there is a PEP relationship (which, for the purposes of compliance with the Regulations, also includes 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 source of wealth and source of funds which are involved in the business relationship or occasional transaction
- conduct closer ongoing monitoring of the business relationship

You are not required to actively investigate whether beneficial owners of a client are PEPs. However, where you have a beneficial owner who you know to be a PEP, you should consider on a risk-based approach what extra measures, if any, you need to take when dealing with that client.

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 firms supervised by the FCA, but you may take it into account in accordance with Regulation 34(4)(b)(i).

4.12.2.1 Who is a PEP?

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 community institution, an international body, or a state, including the UK:

- 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
- directors, deputy directors and members of the board of equivalent function of an international organisation

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.

In addition to the primary PEPs listed above, a PEP also includes:

- family members of a PEP – spouse, civil partner, children, their spouses or partners, and parents
- 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.

4.12.2.2 How to identify PEPs

You are not required to conduct extensive investigations to establish whether a person is a PEP. Have regard to information that is in your possession or publicly known. Many practices use subscriber services that can run checks against the PEPs databases which they maintain. If your practice regularly encounters PEPs, you should consider a subscription as otherwise it is easy to 'miss' PEPs in your client database including at ultimate beneficial ownership level.

To assess your PEP risk profile, you must take into account your risk assessment carried out under Regulation 18(1), 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.

If the risk of you acquiring a PEP as a client is low, you may simply wish to ask clients whether they fall within any of the PEP categories. Where they say no, you may reasonably assume the individual is not a PEP unless anything else within the retainer, or that you otherwise become aware of, makes you suspect they may be a PEP.

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. You may find that a web-based search engine will be sufficient for these purposes, or you may decide that it is more appropriate to conduct electronic checks through a reputable international electronic verification provider.

Note: The range of PEPs is wide and constantly changing, so electronic verification will not give you 100 per cent certainty. You should remain alert to situations suggesting the client is a PEP. Such situations include:

- receiving funds in the retainer from a government account
- correspondence on official letterhead from the client or a related person
- general conversation with the client or person related to the retainer linking the person to a PEP
- news reports which come 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 may consider on a risk-sensitive basis applying aspects of the enhanced due diligence procedures. Even if an individual does not strictly speaking fall within the above PEP definition but on the basis of your research and understanding of what an individual does, you may also consider it appropriate having regard to the risks to take the steps outlined above.

4.12.2.4 Senior management approval

Regulation 3(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 Regulations also impose a duty on the FCA to provide guidance on PEPs, which must include guidance on who should be treated as coming within the definition of senior management.

For independent legal professionals, senior management may be:

- the head of a practice group
- another partner who is not involved with the particular file
- the partner supervising the particular file
- the nominated officer or, if different, the officer responsible for compliance with the Regulations
- the managing partner.

In any case, it is recommended that you advise those responsible for monitoring risk assessment that a business relationship with a PEP has begun, to help their overall monitoring of the practice's risk profile and compliance.

4.12.2.5 Establishing source of wealth and funds

Generally, this simply involves asking questions of the client about their source of wealth and the source of the funds to be used with each retainer. When you know a person is a PEP, their salary and source of wealth is often publicly available on a register of their interests. This may be relevant for higher risk retainers.

The question of evidencing source of wealth should be addressed on a risk sensitive basis. There is no one size fits all answer to this question; certain evidence may be sufficient in some circumstances, though insufficient in others. When assessing what evidence will be sufficient to address this issue, those who operate under the 2017 Regulations need to take a global view of the risk factors relevant to the situation and *consideration* of the client's source of wealth should be central to this assessment. Whatever actions are taken or not taken, those actions and the reasons for them should be clearly recorded.

In addition, please note that source of funds is different from source of wealth. Source of funds relates to from where the client's funds are received – a UK bank account for example. Source of wealth relates to how the client came to have the funds in question – via inheritance, house sale, or investment windfall for example. Source of wealth is fundamental to money laundering risk assessment. If you are clear about the legitimacy of a client's source of wealth, the risk of money laundering is significantly reduced.

4.12.2.6 Enhanced monitoring

You should ensure that funds paid into your client account by your client come from the account nominated and are for an amount commensurate with the client's known wealth. Ask further questions if they are not.

4.12.3 High risk third countries

You must apply EDD measures in any transaction or business relationship with a person established in a 'high risk third country'. However, this requirement does not apply if:

- the customer is a branch or majority owned subsidiary of an entity which is established in an EEA state and subject to the 4th Directive,
- it complies with the group wide policies established by the entity under Article 45 of the 4th Directive, and
- you do not consider EDD measures to be necessary taking a risk-based approach.

Note that not all countries where there may be a higher risk of money laundering are 'high risk third countries'. 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 4th Directive. The current list of high risk third countries is contained in Commission Delegated Regulation (EU) 2016/1675.

4.12.4 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 take into account the risk factors set out in Regulation 33(6). While you must take these risk factors into account, you should consider the situation as a whole. The presence of one or more risk factors does not in and of itself mean that the situation presents a higher risk of money laundering or terrorist financing.

See Chapters 2 and 12 for factors and warning signs you should consider in determining whether a high risk of money laundering is present in a given case.

4.13 Sanctions and other restrictions

Your CDD measures should, following a risk-based approach, be able to ascertain whether your client is subject to the restrictions or directions listed below.

You should also be able to ascertain whether key beneficial owners or the intended recipient of funds from a transaction you are undertaking are subject to the restrictions or directions listed below, where there is a higher risk of money laundering or terrorist financing.

You should assess each case on its merits. However, examples of higher risk situations may include transactions with:

- complex corporate entities in jurisdictions where there is a high risk of terrorist funding
- persons from jurisdictions which are subject to sanctions

HM Treasury's Asset Freezing Unit maintains a consolidated list of financial restrictions in force in the UK. Access this list, register for updates and obtain further information on financial restrictions.

See paragraph 7.10 for further information on obtaining a licence from HM Treasury to carry out transactions with persons or entities subject to financial restrictions.

4.13.1 Financial restrictions – general

The UK government imposes financial restrictions on persons and entities following their designation by the United Nations and/or European Union. The UK also operates a domestic counter-terrorism regime, where the government decides to impose financial restrictions on certain persons and entities.

Statutory instruments are issued for each financial restriction in force. An order will be made freezing the assets of a person or entity, where a financial restriction is imposed. It is unlawful to make payments to or allow payments to be made to that designated person or entity.

These persons and entities will be on HM Treasury's consolidated list.

4.13.2 Restrictions against Al-Qaida and terrorism

The Al Qaida and Taliban (United Nations Measures) Order 2006 and the Terrorism (United Nations Measures) Order 20091 create specific offences for providing funds or economic resources to terrorists.

Persons or entities designated under these orders will be on HM Treasury's consolidated list.

Chapter 5 – Beneficial ownership information

Note: This Chapter may not apply to barristers, BSB entities or advocates who are prohibited from undertaking the management, administration or general conduct of a client's affairs as set out in section 1.1.1.

5.1 Overview

You will need to 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.

5.2 Obligations on UK body corporates

Under Regulation 42(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:

- listed and unlisted companies
- limited liability partnerships
- Scottish limited partnerships

Under Regulation 43(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 will need to 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 firm, which should 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.

5.3 Obligations of trustees

The Regulations impose obligations on trustees of 'relevant trusts' to maintain accurate and up to date 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 and to HMRC on an annual basis. The information will be included on a register which will be available to HMRC and law enforcement agencies in the UK and EEA states.

A relevant trust is a UK express trust or an offshore express trust which generates UK tax consequences (including trusts which only generate tax consequences occasionally). The definition of relevant trust is further outlined below.

Where you act (including occasionally) as a trustee of a relevant trust you will need to maintain the records and provide 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.

5.3.1 Which trusts are caught?

A relevant trust is a UK express trust or an offshore express trust which is liable, even if only occasionally, to 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 because the trust’s assets or income include some UK source income or UK assets.

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.

A trust is a UK express trust 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 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 above-mentioned UK taxes.

5.3.2 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 records of all the trust’s beneficial owners, who will include its:

- settlor;
- trustees;
- beneficiaries named in the trust deed, once it has been determined they will benefit from the trust, or pending that determination (e.g. in the case of a discretionary trust in relation to which the grant of any beneficial interest has yet to be determined) the class of persons in whose main interest the trust is set up;
- 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.

5.3.3 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 a class), the trustees need to note and record:

- the individual's full name;
- the individual's national insurance number of unique taxpayer reference, if any
- if the individual does not have a national insurance number or unique taxpayer reference, the individual's usual residential address, and if that address is not in the UK, the individual's passport number or identification card number, with the country of issue and the expiry date of the passport or identification card; or 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;
- the individual's date of birth;
- the individual's national insurance number and unique taxpayer reference, if any; and
- the nature of the individual's role in relation to the trust.

Where the beneficial owner (but note, not a potential beneficiary) is a corporate body, the trustees need to note and record:

- the legal entity's corporate or firm name;
- the legal entity's unique taxpayer reference, if any;
- the registered or principal office of the legal entity;
- the legal form of the legal entity and the law by which it is governed;
- 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.

Note the requirement to maintain these records does not extend to the beneficial owners of corporate bodies where a corporate body is a beneficial owner of a relevant trust.

The trustees are also obliged to 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 and 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.

As the statement of accounts specifies a value date which is not the acquisition date, the trustees would appear obliged to obtain market valuations for each category of trust asset year on year.

5.3.4 When does the information need to be obtained and updated?

The obligation on trustees to maintain the records outlined above comes into effect when the Regulations come into force.

The information must be provided to HMRC on or before 31 January 2018 or the next 31 January which falls after the end of the tax year in which the trustees were first liable to pay any of the above specified UK taxes. If they provide information prior to 31 January and they become aware it has changed (save if going to value of the trust assets) they must notify HMRC of the change and the date on which it occurred prior to 31 January. 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.

5.3.5 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 person to whom the Regulations apply they must inform that person they are acting as trustee. They must also provide that 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.

5.3.6 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 each tax year, the trustees 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 as defined in Regulation 44(10).

Although HMRC has informally indicated that it anticipates disclosures for the new register of beneficial owners of taxable relevant trusts to come in during the course of the current tax year, prior to the initial 5 April 2018, it appears possible that trustees could be approached by law enforcement at any point after the Regulations have come into effect.

5.3.7 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 'the person to whom information in a record relates', so each named beneficial owner and potential beneficiary in the relevant records, consents to longer retention or where longer retention is required by an enactment or for the purposes of court proceedings.

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.

5.3.8 What information do trustees need to provide to HMRC for the register and when?

The trustees need to provide all the information which they are obliged to record on the trust and its beneficial owners and potential beneficiaries as set out above to HMRC.

We understand that HMRC is not expecting to receive all information on or immediately after the Regulations coming into force. The first set of information will need to be provided by trustees of relevant trusts on or before 31 January 2018. However, as above, trustees could find themselves on the receiving end of a request for information from a relevant person or UK law enforcement authority at any time after commencement of the Regulations meaning that it would be prudent for trustees to attend to collation of relevant records promptly.

Trustees should note that the register reporting obligation only arises in relation to a preceding tax year in which the relevant trust generates a UK tax consequence. So a trustee of an offshore tax which only generates a UK tax consequence in the form of a ten yearly, reoccurring 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).

This may pose an issue for trustees who also need to submit UK tax returns for the relevant trust annually, in which they will be asked to confirm that information on the register of beneficial owners of taxable relevant trusts is correct, if no register updating requirement has arisen (because the trust did not generate a UK tax consequence) in the particular tax year.

Trustees may need to avoid ticking the relevant box on the online form and instead provide an explanatory note.

5.3.9 How will relevant information be provided to HMRC?

We understand that the register will be online and that information contributions to it by trustees will also need to be made online. It is anticipated that third party software is likely to be commercially available to professional trustees who have extensive amounts of data to transfer to the register online and which will be capable of collating data and 'feeding' it to the register. Guidance on this subject is anticipated from HMRC.

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.

5.3.10 With whom can HMRC share the information on the register?

HMRC is obliged to ensure that any officer of any UK police force and/or the NCA can inspect the register.

It is also obliged to ensure the NCA can use information on the register to respond promptly to a request made by a similar authority or financial intelligence unit in another EEA state.

Chapter 6 – Money laundering offences

6.1 General comments

The Proceeds of Crime Act 2002 (POCA) created a single set of money laundering offences applicable throughout the UK to the proceeds of all crimes. It also creates a disclosure regime, which makes it an offence not to disclose knowledge or suspicion of money laundering, but also permits persons to be given consent in certain circumstances to carry out activities which would otherwise constitute money laundering.

6.2 Application

POCA applies to all legal professionals, although some offences apply only to persons within the regulated sector, or nominated officers.

6.3 Mental elements

The mental elements which are relevant to offences under Part 7 of POCA are:

- knowledge
- suspicion
- reasonable grounds for suspicion

These are the three mental elements in the actual offences, although the third one only applies to offences relating to the regulated sector. There is also the element of belief on reasonable grounds in the foreign conduct defence to the money laundering offences. A person will have a defence to a principal offence if they know or believe on reasonable grounds that the criminal conduct involved was exempt overseas criminal 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; while if you are not in the regulated sector you will only need to consider making a disclosure if you have actual, subjective knowledge or suspicion.

These terms for the mental elements in the offences are not terms of art; they are not defined within POCA and should be given their everyday meaning. However, case law has provided some guidance on how they should be interpreted.

6.3.1 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.

6.3.2 Suspicion

The term 'suspects' is one which the court has 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 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.

Chapter 12 of this guidance contains a number of standard 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.

6.3.3 Reasonable grounds to suspect

The issues here for the legal professional conducting regulated activities are the same as for the mental element of suspicion, except that it is an objective test. 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?

6.4 Principal money laundering offences

6.4.1 General comments

Money laundering offences assume that a criminal offence has occurred in order to generate the criminal property which is now being laundered. This 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.

The principal money laundering offences apply to money laundering activity which occurred on or after 24 February 2003 as a result of the Proceeds of Crime Act 2002 (Commencement No. 4, Transitional Provisions & Savings) Order 2003.

If the money laundering occurred or started before 24 February 2003, the former legislation will apply.

However, if the money laundering took place after 24 February 2003, the conduct giving rise to the criminal property can occur before that date.

When considering the principal money laundering offences, be aware that it is also an offence to conspire or attempt to launder the proceeds of crime, or to counsel, aid, abet or procure money laundering.

6.4.2 Section 327 – concealing

A person commits an offence if he or she conceals, disguises, converts, or transfers criminal property, or removes criminal property from England and Wales, Scotland or Northern Ireland.

Concealing or disguising criminal property includes concealing or disguising its nature, source, location, disposition, movement, ownership or any rights connected with it.

6.4.3 Section 328 - arrangements

A person commits an offence if he or she enters into, or becomes concerned in an arrangement which he knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.

What is an arrangement?

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.

An agreement to make an arrangement will not always be an arrangement. The test is whether the arrangement does in fact, in the present and not the future, have the effect of facilitating the acquisition, retention, use or control of criminal property by or on behalf of another person.

What is not an arrangement?

Bowman v Fels [2005] EWCA Civ 226 held that section 328 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.

Our view, supported by Counsel's opinion, is that dividing assets in accordance with the judgment, including the handling of the assets which are criminal property, is not an arrangement. Further, settlements, negotiations, out of court settlements, alternative dispute resolution and tribunal representation are 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.

The recovery of property by a victim of an acquisitive offence will not be committing an offence under either section 328 or section 329 of the Act.

Sham litigation

Sham litigation created for the purposes of money laundering remains within the ambit of section 328. Our view is that 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.

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 section 328 provides some assistance in interpreting how that section applies in those circumstances.

Our view is that *Bowman v Fels* supports a restricted 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 section 328

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
- if no arrangement exists, whether one may come into existence in the future which you may become concerned in.

6.4.4 Section 329 - acquisition, use or possession

A person commits an offence if he or she acquires, uses or has possession of criminal property.

6.5 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)
- you intended to make an authorised disclosure but had a reasonable excuse for not doing so (the reasonable excuse defence)

In relation to section 329 you will also have a defence if you received adequate consideration for the criminal property (the adequate consideration defence).

6.5.1 Authorised disclosures

Section 338 authorises you to make a disclosure regarding suspicion of money laundering as a defence to the principal money laundering offences.

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
- 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 authorised, it does not breach any rule which would otherwise restrict it, including professional regulatory requirements relating to confidentiality.

Where your practice has a nominated officer, you should make your disclosure to the nominated officer. The nominated officer will consider your disclosure and decide whether to make an external disclosure to the NCA. If your practice does not have a nominated officer, you should make your disclosure directly to the NCA.

Appropriate consent/DAML

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 nominated officer and seek consent/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 Chapter 9 of this guidance.

Reasonable excuse defence

This defence applies where a person intended to make an authorised disclosure before doing a prohibited act, but had a reasonable excuse for not disclosing.

Reasonable excuse has not been defined by the courts, but the scope of the reasonable excuse defence is important for legal professional privilege.

You will have a defence against a principal money laundering offence if you make an authorised disclosure.

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 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 would provide a reasonable excuse. For example:

- if it is clear that a regulator or enforcement authority (in the UK or elsewhere) is already 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, or
- if the only information that a reporter would be providing for the purposes of an authorised disclosure or a report under section 330 is information entirely within the public domain, or
- 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.

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 reporters' excuse for not making an authorised disclosure report under section 330 was a reasonable excuse. 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.

Where you suspect part way through

It is not unusual for a transactional matter to seem legitimate early in the retainer, but to develop in such a way as to arouse suspicion later on. It may be that certain steps have already taken place which you now suspect facilitated money laundering; while further steps are yet to be taken which you also suspect will facilitate further money laundering.

Section 338(2A) provides that you may make an authorised disclosure in these circumstances if:

- at the time the initial steps were taken they were not a money laundering offence because you did not have good reason to know or suspect that the property was criminal property; and
- you make a disclosure of your own initiative as soon as practicable after you first know or suspect that criminal property is involved in the retainer.

In such a case you would make a disclosure seeking consent/DAML for the rest of the transaction to proceed, while fully documenting the reasons why you came to know or suspect that criminal property was involved and why you did not suspect this to be the case previously.

6.5.2 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 section 328 due to the case of *Bowman v Fels*.

The defence is more likely to cover situations where:

- a third party seeks to enforce an arm’s length debt and, unknown to them, is given criminal property in payment for that debt;
- a person provides goods or services as part of a legitimate arm’s length transaction but unknown to them is paid from a bank account which contains the proceeds of crime.

6.6 Failure to disclose offences – money laundering

6.6.1 General comments

The failure to disclose provisions in sections 330, 331 and 332 apply where the information on which the knowledge or suspicion is based came to a person on or after 24 February 2003, or where a person in the regulated sector has reasonable grounds for knowledge or suspicion on or after that date.

If the information came to a person before 24 February 2003, the old law applies.

In all three sections, the phrase ‘knows or suspects’ refers to actual knowledge or suspicion - a subjective test. However, legal professionals and nominated officers in the regulated sector will also commit an offence if they fail to report when they have reasonable grounds for knowledge or suspicion - an objective test. On this basis, they may be guilty of the offence under sections 330 or 331 if they 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

6.6.2 Section 330 – failure to disclose: regulated sector

A person commits an offence if

- he or she knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering, and
- the information on which his suspicion is based comes in the course of business in the regulated sector, and
- he or she fails to disclose that knowledge or suspicion, or reasonable grounds for suspicion, as soon as practicable to a nominated officer or the NCA.

Making a required notification or being party to a joint disclosure report will both be treated as satisfying any requirement to disclose once section 339ZD is in force.

Our view is that delays in disclosure arising from taking legal advice or seeking help may be acceptable provided you act promptly to seek advice.

6.6.3 Section 331 – failure to disclose: nominated officer in the regulated sector

A nominated officer in the regulated sector commits a separate offence if, as a result of an internal disclosure under section 330, he knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering and he fails to disclose as soon as practicable to the NCA.

6.6.4 Section 332 – failure to disclose: nominated officer in the non-regulated sector

An organisation which does not carry out relevant activities and so is not in the regulated sector, may decide on a risk-based approach to set up internal disclosure systems and appoint a person as nominated officer to receive internal disclosures.

A nominated officer in the non-regulated sector commits an offence if, as a result of a disclosure, he knows or suspects that another person is engaged in money laundering and fails to make a disclosure as soon as practicable to the NCA.

For this offence, the test is a subjective one: did you know or suspect in fact?

6.7 Exceptions 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;

- 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 are only specifically provided for persons in the regulated sector who are not nominated officers.

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 derived from exempted overseas criminal conduct.

6.7.1 Reasonable excuse

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 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 would provide a reasonable excuse. For example:

- if it is clear that a regulator or enforcement authority (in the UK or elsewhere) is already 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, or
- if the only information that a reporter would be providing for the purposes of an authorised disclosure or a report under section 330 is information entirely within the public domain, or
- 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.

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 an authorised disclosure report under section 330 was a reasonable excuse. 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.

6.7.2 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, or
- 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.

The Crown Prosecution Service guidance for prosecutors indicates that if a legal professional forms a genuine, but mistaken, belief that the privileged circumstances exemption applies (for example, the client misleads the legal professional and uses the advice received for a criminal purpose) the legal professional will be able to rely on the reasonable excuse defence.

For a further discussion of privileged circumstances see Chapter 7.

6.7.3 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. Employers may be prosecuted for a breach of the Regulations if they fail to train staff.

6.8 Tipping off

The offences of tipping off for money laundering are contained in POCA as amended by the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 (TACT and POCA Regulations 2007).

There are also tipping off offences for terrorist property in the Terrorism Act, as amended by the TACT and POCA Regulations 2007.

6.8.1 Offences

6.8.1.1 Tipping off – in the regulated sector

There are two tipping off offences in section 333A of POCA. They apply only to business in the regulated sector.

Section 333A(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, 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 disclosure to the NCA
- if you know or suspect that by disclosing this information, you are likely to prejudice any investigation related to that SAR

- the information upon which the disclosure is based came to you in the course of business in the regulated sector.

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. The key point is that you can commit this offence, even when you are unaware that a SAR was submitted.

6.8.1.2 Prejudicing an investigation – outside the regulated sector

Section 342(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. Section 342(1) was amended by paragraph 8 of the TACT and POCA Regulations 2007. It only applies to those outside 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.

6.8.2 Defences

6.8.2.1 Tipping off

The following disclosures are permitted:

- Section 333B - disclosures within an undertaking or group, including disclosures to a professional legal adviser or relevant professional adviser;
- Section 333C - disclosures between institutions, including disclosures from a professional legal adviser to another professional legal adviser;
- Section 333D - disclosures to your supervisory authority;
- Section 333D(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 does not know or suspect that a disclosure is likely to prejudice an investigation.

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 a disclosure is made to another legal professional either:

- within a different undertaking, if both parties carry on business in an EEA state; or

- in a country or territory that imposes money laundering requirements equivalent to the EU and both parties share common ownership, management or control.

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.

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 section 333A apply to those carrying on activities in the regulated sector.

6.8.2.2 Prejudicing an investigation

Section 342(4) – professional legal adviser exemption

It is a defence to a section 342(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 (section 342(5)).

6.8.3 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 a SAR has been made or that a money laundering investigation is being carried out or contemplated. The offence of tipping off only applies to the regulated sector.

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.

Chapter 7 – Legal professional privilege

7.1 General comments

Legal professionals are under a duty to keep the affairs of their clients confidential, and the circumstances in which they are able to disclose client communications are strictly limited.

However, sections 327 - 329, 330 and 332 of POCA contain provisions for disclosure of information to be made to the NCA. Sections 339ZB-G [not yet in force] contain further provisions for disclosure of confidential information to both the NCA and to other persons carrying on business in the regulated sector.

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.

This chapter examines the tension between a legal professional's duties and these provisions of POCA. Similar tensions also arise with respect to the Terrorism Act.

This chapter should be read in conjunction with Chapter 6 of this guidance and if you are still in doubt as to your position, you should seek independent legal advice.

7.2 Application

This chapter is relevant to any legal professional considering whether to make a disclosure under POCA.

7.3 Duty of confidentiality

A legal professional is professionally and legally obliged to keep the affairs of clients confidential and to ensure that his 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.

In exceptional circumstances this general obligation of confidence may be overridden. However, certain communications can never be disclosed unless statute permits this either expressly or by necessary implication. Such communications are those protected by legal professional privilege (LPP).

7.4 Legal professional privilege

7.4.1 General overview

LPP is a privilege against disclosure, ensuring clients know that certain documents and information provided to legal professionals cannot be disclosed at all. It recognises the client's fundamental human right to be candid with his legal adviser, without fear of later disclosure to his prejudice. It is an absolute right and cannot be overridden by any other interest.

LPP does not extend to everything that legal professionals have a duty to keep confidential. LPP protects only those confidential communications falling under either of the two heads of privilege – advice privilege or litigation privilege.

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.

7.4.2 Advice privilege

Principle

Communications between a legal professional, acting in his capacity as a legal professional, and a client, are privileged if they are both:

- confidential; and
- for the purpose of seeking legal advice 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 which are given in a legal context, that involve the legal professional using his legal skills and which are directly related to the performance of the legal professional's professional duties [*Passmore on Privilege 2nd edition 2006*].

Case law helps define what advice privilege covers.

Communications subject to advice privilege:

- a solicitor's bill of costs and statement of account [*Chant v Brown (1852) 9 Hare 790*]
- information imparted by prospective clients in advance of a retainer if the communications were made for the purpose of indicating the advice required [*Minster v Priest [1930] AC 558 per Lord Atkin at 584*].

Communications not subject to advice privilege:

- notes of open court proceedings [*Parry v News Group Newspapers (1990) 140 New Law Journal 1719*], as the content of the communication is not confidential;
- conversations, correspondence or meetings with opposing legal professionals [*Parry v News Group Newspapers (1990) 140 New Law Journal 1719*], as the content of the communication is not confidential;
- a client account ledger maintained in relation to the client's money [*Nationwide Building Society v Various Solicitors [1999]P.N.L.R. 53.*];
- an appointments diary or time record on an attendance note, time sheet or fee record relating to a client [*R v Manchester Crown Court, ex p. Rogers [1999] 1 W.L.R. 832*];

- conveyancing documents, as they are not communications [*R v Inner London Crown Court ex p. Baines & Baines [1988] QB 579*].

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 his 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 will mean 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, as long as they are directly related to your performance of your professional duties as a legal adviser.

7.4.3 Litigation privilege

Principle

This privilege, which is wider than advice privilege, protects confidential communications made after litigation has started, or 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.

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

7.4.4 Important points to consider

An original document not brought into existence for these privileged purposes and so not already privileged, does not become privileged merely by being given to a legal professional for advice or other privileged purpose.

Further, 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*]

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.

7.4.5 Crime/fraud 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*]. It is irrelevant whether or not you are aware that you are being used for that purpose [*Banque Keyser Ullman v Skandia [1986] 1 Lloyds Rep 336*].

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*].

Knowing a transaction constitutes an offence

If you know the transaction you're 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.

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.

Prima facie evidence

If you suspect you are unwittingly being involved by your client in a fraud, the courts require prima facie evidence before LPP can be displaced [*O'Rourke v Darbishire [1920] AC 581*]. 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 facie evidence exists, you may also ask the court for directions [*Finers v Miro [1991] 1 W.L.R. 35*].

The Crown Prosecution Service guidance for prosecutors indicates that if a legal professional forms a genuine, but mistaken, belief that the privileged circumstances

exemption (see 7.5 below) applies (for example, the client misleads the legal professional and uses the advice received for a criminal purpose) the legal professional will be able to rely on the reasonable excuse defence. It is likely that a similar approach would be taken with respect to a genuine, but mistaken, belief that LPP applies.

We believe you should not make a disclosure unless you know of prima facie evidence that you are being used in the furtherance of a crime.

7.5 Privileged circumstances

Quite separately from LPP, POCA recognises another type of communication, one which is received in 'privileged circumstances'. This is not the same as LPP, it is merely an exemption from certain provisions of POCA, although in many cases the communication will also be covered by LPP.

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 all these sections, the essential elements of the exemption are:

- you are a professional legal adviser;
- the information or material is communicated to you:
    - by your client or their representative in connection with you giving legal advice;
    - 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. For the position regarding notaries, see section 7.4.1 above.

Consider the crime/fraud exception when determining what constitutes the furthering of a criminal purpose.

Finally, section 330(9A) protects the privilege attaching to any disclosure made to a nominated officer for the purposes of obtaining advice about whether or not a disclosure should be made.

7.6 Differences between privileged circumstances and LPP

7.6.1 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 your giving legal advice to the client, or the client seeking legal advice from you. This may include communications with:

- 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.

7.6.2 Losing protection by dissemination

There may be circumstances in which a legal adviser has communicated to him information which is subject to legal professional privilege, but which does not fall within the definition of privileged circumstances.

For example, a legal professional representing client A may hold or have had communicated to him information which is privileged as between client B and his own legal professional, in circumstances where client A and client B are parties to a transaction, or have some other shared interest.

The sharing of this information may not result in client B's privilege being lost, if it is stipulated that privilege is not waived (Gotha City v Sotheby's (no1) [1998] 1 WLR 114).

Privileged circumstances will not apply because the information was not communicated to client A's legal professional by a client of his in connection with the giving by him of legal advice to that client. However, if it was given to him by any person in connection with legal proceedings or contemplated legal proceedings, privileged circumstances would apply.

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 applied.

7.6.3 Vulnerability to seizure

It is important to correctly identify whether communications are protected by LPP or if they are merely covered by the privileged circumstances exemption. This is because the privileged circumstances exemption exempts you from certain POCA provisions. It does not provide any of the other LPP protections to those communications. Therefore a communication which is only covered by privileged circumstances, not

LPP, will still remain vulnerable to seizure or production under a court order or other such notice from law enforcement agencies.

7.7 When do I disclose?

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 include making a disclosure to the NCA.

If neither of these situations applies, the communication will 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 [not yet in force] 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.

Chapter 8 – Terrorist property offences

8.1 General comments

Terrorist organisations require funds to plan and carry out attacks, train militants, pay their operatives and promote their ideologies. The Terrorism Act 2000 (as amended) criminalises not only the participation in terrorist activities but also the provision of monetary support for terrorist purposes.

8.2 Application

All persons are required to comply with the Terrorism Act. The principal terrorist property offences in sections15 – 18 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.

The definition of business in the regulated sector was amended by the Terrorism Act 2000 (Business in the Regulated Sector and Supervisory Authorities) Order 2007 to reflect changes brought about by the third money laundering directive. There are similar changes to the definition of business in the regulated sector in POCA.

8.3 Principal terrorist property offences

8.3.1 Section 15 – fundraising

It is an offence to be involved in fundraising if you have knowledge or 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.

8.3.2 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.

8.3.3 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.

8.3.4 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
- 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.

Read about arrangements under POCA in Chapter 6.

8.4 Defences to principal terrorist property offences

The TACT and POCA Regulations 2007 of 26 December 2007 introduced three new defences to the main offences in sections15 – 18. These defences are contained in sections 21ZA – 21ZC, 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;
- **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;
- **reasonable excuse defence** – you intended to make a disclosure but have a reasonable excuse for failing to do so. See section 6.7.1 on reasonable excuse.

Read Chapter 9 for more information on how to make a disclosure and gaining consent.

There are further defences relating to co-operation with the police in section 21. You do not commit an offence under sections15-18 in the following further circumstances:

- you are acting with the express consent of a constable, including civilian staff at the NCA;
- 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.

8.5 Failure to disclose offences

8.5.1 Non-regulated sector

Section 19 provides that anyone, whether they are a nominated officer or not, must disclose as soon as reasonably practicable to a constable, or the NCA, if they know 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.

8.5.2 Regulated sector

Section 21A, inserted by the Anti-Terrorism Crime and Security Act 2001, creates a criminal offence for those in the regulated sector who fail to make a disclosure to either a constable or the practice's nominated officer where they know, suspect, or there are reasonable grounds for suspecting that another person has committed an offence. This was further expanded by the TACT and POCA Regulations 2007 to cover failure to disclose an attempted offence under sections 15 -18.

8.6 Defences to failure to disclose

The following are defences to failure to disclose offences under both section 19 and section 21A. 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.

The TACT and POCA Regulations 2007 introduced an additional defence for those in the regulated sector. A person 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.

Read about privileged circumstances in 6.7.2.

It is also a defence under section 19 if you made an internal report in accordance with your employer's reporting procedures.

8.7 Section 21D tipping off offences: regulated sector

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, 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 disclosure to the NCA
- if you know or suspect that by disclosing this information, you are likely to prejudice any investigation related to that SAR

- the information upon which the disclosure is based came to you in the course of business in the regulated sector

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.

8.8 Defences to tipping off

8.8.1 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 an EEA state or a country or territory that imposes equivalent money laundering requirements equivalent to the EU.

8.8.2 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 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 money laundering offence; and
- both parties have equivalent professional duties of confidentiality and protection of personal data.

8.8.3 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 section 21D only apply to the regulated sector.

8.9 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.

8.10 Other terrorist property offences in statutory instruments

8.10.1 The offences

Under The Al Qaida and Taliban (United Nations Measures) Order 2006 you must not:

- deal with the funds or economic resources of designated persons; or
- make funds and economic resources available, directly or indirectly for the benefit of designated persons.

Under the Terrorism (United Nations Measures) Order 2009, you must not:

- deal with the funds or economic resources of a designated person;
- make funds, financial services or economic resources available, directly or indirectly to a designated person; or
- make financial services or economic resources available to any person for the significant benefit of a designated person.

Finally, you must not knowingly and intentionally participate 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 reason 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, including (but not limited to) by selling, hiring or mortgaging the resources.

Financial services are defined broadly and include advisory services such as providing advice on:

- acquisitions; and

- corporate restructuring and strategy.

8.10.2 Obtaining a licence from the Office of Financial Sanctions Implementation (OFSI)

You must not proceed with a transaction without a licence from the OFSI Asset Freezing Unit where a client or the intended recipient of funds from the transaction is identified as a designated person.

You must do all of the following:

- suspend the transaction pending advice from the Asset Freezing Unit;
- contact the Asset Freezing Unit to seek a licence to deal with the funds; and
- consider whether you have a suspicion of money laundering or terrorist financing which requires a report to the NCA

You must not return funds to the designated person without the approval of the Asset Freezing Unit

The Asset Freezing Unit has the power to grant licences exempting certain transactions from the financial restrictions. Requests are considered on a case-by-case basis, to ensure that there is no risk of funds being diverted to terrorism.

Contact the Asset Freezing Unit to request a licence or obtain advice regarding financial restrictions at:

Asset Freezing Unit

Fax	020 7451 7677
Email	ofsi@hmtreasury.gsi.gov.uk
Address	Office of Financial Sanctions Implementation HM Treasury 1 Horse Guards Road London SW1A 2HQ

Chapter 9 – Making a disclosure

9.1 General comments

The disclosure regime for money laundering and terrorist financing is run by the financial intelligence unit within the National Crime Agency (the NCA). The NCA was launched on 7 October 2013 under provisions granted by the Crime and Courts Act 2013. It is a law enforcement body devoted to dealing with organised crime within the UK and networking with other law enforcement agencies to combat global organised crime.

For full details on the NCA and its activities view its website at: http://www.nationalcrimeagency.gov.uk/

9.2 Application

All persons within the regulated sector and nominated officers have obligations under POCA and the Terrorism Act 2000 as amended, to make disclosures of suspicions of money laundering, terrorist financing and terrorist property offences.

In addition, any person may need to make an authorised disclosure about criminal and terrorist property.

All persons are required to make disclosures to the NCA of suspected terrorist financing.

9.3 Suspicious activity reports

9.3.1 What is a SAR?

A suspicious activity report (SAR) is the name given to the making of a disclosure to the NCA under either POCA or the Terrorism Act.

9.3.2 Who discloses?

Where a practice has a nominated officer, either they or their deputy will make the SAR to the NCA.

9.3.3 When?

You must make a SAR as soon as practicable after you have formed a reportable suspicion or know of terrorist financing or money laundering (subject to privilege considerations). Swiftly made SARs avoid delays in fulfilling your client's instructions.

Where a joint disclosure report [not yet in force] is made as a result of a disclosure request, it must be made either within the period specified by the requesting NCA officer, or within 28 days of complying with a request for voluntary disclosure of information from another person in the regulated sector.

9.3.4 How to disclose

Forms

The NCA has issued preferred forms to be completed when making a SAR. We encourage you to use the preferred form to enhance the NCA's ability to assess your SAR quickly.

SARs online

You should use SARs online where you have computer access. This securely encrypted system provided by the NCA allows you to:

- register your practice and relevant contact persons;
- submit a SAR at any time of day; and
- receive e-mail confirmations of each SAR submitted.

You can register with the NCA at https://www.ukciu.gov.uk/(e50jai55ui0x2quvierajr45)/Registration/NewUserRegistrationInfo.aspx

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, not by post.

Hard copy SARs should be sent to:

Fax: 020 7238 8256

Post: UK FIU

PO Box 8000

London SE11 5EN

9.3.5 Information to include

The NCA has provided information on completing the preferred SARs form.

To speed up consideration of your SAR, it is recommended that you use the NCA's glossary of codes for each reason for suspicion section of the report.

Contact your supervisory authority to find out your regulatory number.

9.3.6 Getting consent/DAML from the NCA to proceed

You will often be asking the NCA for consent/DAML to undertake acts which would be prohibited as a principal money laundering offence or a terrorist property offence.

While the NCA has produced information on obtaining consent/DAML, here are a number of key points to remember:

- You only receive consent/DAML 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. For example:

  > We seek consent/DAML to finalise an agreement for sale of property X and to then transfer property X into the name of (purchaser) and, following payment of disbursements, pay the proceeds of the sale of the property to (seller).

- The initial notice period is seven working days after the SAR is made, and if consent/DAML is refused, the initial moratorium period is a further 31 calendar days from the date of refusal. If you need consent/DAML sooner, you should clearly state the reasons for the urgency in the initial report and perhaps contact the NCA to discuss the situation. The NCA can sometimes give consent/DAML in a matter of hours.

- Within the notice and moratorium period you must not do a prohibited act. However, this will not prevent you taking other actions on the file, such as writing letters, conducting searches etc.

- The NCA will contact you by telephone to advise that consent/DAML has been provided and will then send a follow up letter.

9.3.7 Extensions of the moratorium period

The Criminal Finances Act 2017 has made important changes to the moratorium period under POCA. Section 336A of the amended Proceeds of Crime Act 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.

There are occasions where the NCA requires further information to be able to undertake proper analysis and make an informed decision on whether to investigate.

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 disclosure (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.

It will be important for the practice that made the SAR to consider (dependent upon whether the practice is on notice of the application and can participate in the proceedings – see below) these requirements have been satisfied by the applicant. In particular, that the investigation is being conducted diligently and expeditiously and

that further time is needed for the investigation. This will obviously be fact specific in each instance.

A senior officer is defined as follows:

- Director General of the NCA or any other NCA officer authorised by the NCA;
- A police officer of at least the rank of inspector;
- An officer of HM Revenue and Customs;
- An immigration officer;
- A member of staff at the FCA;
- Director of the Serious Fraud Office; or
- An accredited financial investigator.

The application must be made by the senior officer before the initial moratorium period of 31 days expires. 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 amount of the extension should of course be based on the four requirements set out above so the practice should consider not just whether an extension request is justified but also whether the amount of extension requested is reasonable in all of the circumstances.

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.

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 ultimate 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 disclosure would lead to the following:

- evidence of an offence would be interfered with or harmed;
- the gathering of information about the possible commission of an 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.

What this all means in practice is that a person that has made a SAR may be excluded from participating in the hearing of the application to extend the moratorium period. This will obviously hamper the ability of that person to analyse whether the application is reasonable or not. Secondly, the person (even if present in the hearing) may also be prevented from seeing important information on the basis that, if disclosed, to the person it may lead to one of the above prejudicial consequences. A possible difficulty here will be what the person does and does not know and whether they can sensibly either take instructions from its ultimate client (see risks of tipping off below) or take their own action to minimise the risks of a lengthy moratorium period with all the risks of tipping off.

Risks of tipping off

Despite the fact that these amendments allow a maximum moratorium period of 217 days, the Act is silent on the ramifications for potential tipping off of clients. In effect, this means that the tipping off provisions will continue to apply during any extension of the moratorium period. The extensions may be problematic in time critical transactions but in most instances the extensions should be rare and given that they have to be made in 31 day increments are challengeable at different stages.

You will have to be careful however in dealing with clients and third parties and ensuring that no disclosures are made about a SAR which may prejudice any investigation. If you are seeking to challenge an application to extend time, then you should also consider whether it may properly do so without taking instructions and generally whether it would be in the best interests of your ultimate client to do so.

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 from the time when it would otherwise end 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 from the time that it would otherwise end 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 heating 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.

9.3.7 Contacting the NCA/UKFIU

The Financial Intelligence Helpdesk can be contacted on 020 7238 8282. You can contact the NCA on this number for:

- help in submitting a SAR or with the SARs online system;
- help on consent/DAML issues; and

- assessing the risk of tipping off so you know whether disclosing information about a particular SAR would prejudice an investigation.

When contacting the UKFIU please have available your SAR reference number.

General UKFIU matters may be emailed to ukfiusars@nca.x.gsi.gov.uk

Consent/DAML issues can also be addressed by emailing DAML@nca.x.gsi.gov.uk

9.3.8 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.

9.4 Sharing of information within the regulated sector and joint disclosure reports (not yet in force)

Sections 339ZB-G of POCA [not yet in force] introduce a gateway for the sharing of information between persons and entities in the regulated sector on a voluntary basis and for the making of joint disclosure reports (super SARs). 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. The conditions are summarised at 9.4.1 below. However, these provisions do not override legal professional privilege. A legal professional will therefore only be able to share information if legal professional privilege does not apply.

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 (see paragraphs 6.6.2 and 6.6.3).

9.4.1 Conditions

Information to be voluntarily disclosed must have come to a person in the course of business in the regulated sector and may only be disclosed to another person in the sector.

Disclosure must follow a request from either an authorised NCA officer or another regulated person.

A disclosure request must abide by certain formalities. It must state that it is made in connection with AML suspicions; identify the person (if known); describe the

information sought, and; specify the person(s) to whom it is requested the information is disclosed.

If made by another person in the regulated sector a request must also set out the grounds for suspicion or provide information enabling the recipient to decide if the information should be disclosed.

In all cases, the person making the disclosure must be satisfied that disclosing the information may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering.

9.4.2 Required Notification

A required notification must be made to the NCA either when a request is made by one person to another for voluntary disclosure of information, or before a person voluntarily shares information with another following a request to do so by the NCA.

These notifications will satisfy the requirements to make a disclosure under sections 330 and 331 (failure to disclose in the regulated sector).

9.4.3 Joint Disclosure Reports

A joint disclosure report can be made to the NCA by the parties who have given and received information by way of voluntary disclosure. A joint disclosure report will be treated as satisfying the requirements to make a disclosure for the purposes of sections 330 and 331.

The Joint Money Laundering Information Taskforce (JMLIT) was set up in 2016 to facilitate information sharing in the regulated sector and it may be advisable to consider any guidance that they issue following their piloting of these measures. It is anticipated that the NCA will in due course update their guidance on making SARs to accommodate the new provisions.

9.5 Feedback on SARs

The NCA provides some feedback on the value of SARs they have received, although such feedback will always be anonymised to protect the confidentiality of those who submitted it. Feedback is provided:

- in the NCA's 'SARs Annual Report';
- in meetings of the NCA's 'Legal Sector Engagement Group'; and
- In meetings of the NCA's 'SARs Regime Committee'.

Chapter 10 – Enforcement

10.1 General comments

The UK AML/CTF regime is one of the most robust in Europe. Breaches of obligations under the regime are backed by disciplinary and criminal penalties.

Law enforcement agencies and AML supervisors are working co-operatively with regulated professions to assist compliance and increase understanding of how to effectively mitigate risks. However, be in no doubt of the seriousness of the possible sanctions for a failure to comply, nor the willingness of supervisory and enforcement bodies to take appropriate action against non-compliance.

10.2 Supervision under the Regulations

Regulation 7 provides for several bodies to be supervisory authorities for different parts of the regulated sector.

Where a person in the regulated sector is covered by more than one supervisory authority, either the supervisory authorities must decide between them who is to be the sole supervisor of the person, or they must co-operate in the performance of their supervisory 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 for whom it is responsible;
- take necessary measures to ensure those persons comply with the requirements of the Regulations;
- comply with its obligations under Regulation 46(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 operation 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 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 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 the persons 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 persons its supervises, and any other information it considers necessary for exercising its supervisory function.

Supervisory authorities that are also self-regulatory bodies are subject to additional obligations which are set out in Regulation 49.

10.2.1 Legal Sector Supervisors

The named supervisory authorities for the legal sector are:

- the Chartered Institute of Legal Executives;
- the Council for Licenced 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;
- 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 in part 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.

10.2.2 Other supervisors

Other supervisory authorities which may be of relevance to some legal professionals include:

- The Financial Conduct Authority – www.fca.org.uk
- The Insolvency Practitioners Association – www.insolvency-practitioners.org.uk; and
- The Chartered Institute of Taxation – www.tax.org.uk

Where a supervisory authority reaches agreement with another supervisor about who is to supervise the legal professional, this agreement will be made known to the legal professional in accordance with Regulation 7(3).

In all other cases of supervisory overlap, and where you have questions about AML supervision, you should contact your supervisory authority.

The Joint Money Laundering Steering Group (JMLSG) provides guidance to the financial sector which the FCA considers when assessing compliance with AML/CTF obligations.

Read JMLSG's guidance

10.2.3 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:

- Regulation 66: power to require information from, and attendance of, relevant and connected persons without a warrant;
- Regulation 69: power to enter and inspect without a warrant;
- Regulation 70: power to enter a premises under a warrant; and
- Regulation 71: power to retain documents taken under Regulation 66 or 70.

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.

10.3 Disciplinary action against legal professionals

Conduct which fails to comply with AML/CTF obligations may also be a breach of your professional obligations. For further information contact your supervisory authority.

10.4 Offences and penalties

Not complying with AML/CTF obligations puts you at risk of committing criminal offences. Below is a summary of the offences and the relevant penalties. In addition to the principal offences, you could also be charged with offences of conspiracy, attempt, counselling, aiding, abetting or procuring a principal offence, depending on the circumstances.

10.4.1 POCA - relevant offences and penalties

Section	Description	Penalty
327	Conceals, disguises, converts, transfers or removes criminal property	On summary conviction – up to six months' imprisonment or a fine or both On indictment – up to 14 years' imprisonment or a fine or both
328	Arrangements regarding criminal property	
329	Acquires, uses or has possession of criminal property	

330	Failure to disclose knowledge, suspicion or reasonable grounds for suspicion of money laundering – regulated sector	On summary conviction – up to six months' imprisonment or a fine or both On indictment – up to five years' imprisonment or a fine or both
331	Failure to disclose knowledge, suspicion or reasonable grounds for suspicion of money laundering – nominated officer in the regulated sector	
332	Failure to disclose knowledge or suspicion of money laundering – nominated officer in non-regulated sector	
333A	Tipping off – regulated sector	On summary conviction - up to three months' imprisonment or a fine not exceeding level 5 or both. On conviction on indictment- up to two years' imprisonment or a fine or both.
342	Prejudicing an investigation	On indictment – up to five years' imprisonment or a fine or both

10.4.2 Terrorism Act- relevant offences and penalties

Section	**Description**	**Penalty**
15	Fundraising	On summary conviction – up to six months' imprisonment or a fine or both On indictment – up to 14 years' imprisonment or a fine or both
16	Use and possession	
17	Funding arrangements	
18	Money laundering	
19	Failure to disclose	
21A	Failure to disclose – regulated sector	

21	Tipping off –regulated sector	On summary conviction- up to three months' imprisonment or a fine not exceeding level 5 on the standard scale, or both On conviction on indictment- up to two years' imprisonment, or a fine or both

10.4.3 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.

Breach of a relevant requirement

The relevant requirements most likely to be applicable to legal professionals are those imposed under the Regulations listed in the table below. You should consult Schedule 6 and consider whether there are any further relevant requirements that apply to your business.

Regulation	**Description**	**Penalty**
18	Risk assessment by a relevant person	On summary conviction – a fine On indictment – up to two years' imprisonment or a fine or both
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 (4)-(6)	Obligation to apply enhanced due diligence	
35	Enhanced due diligence: politically exposed 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	

Offence of prejudicing investigations

Under Regulation 87 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, or
- They conceal, destroy or dispose of, 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;
    - In Scotland or Northern Ireland, a term of imprisonment not exceeding three months, 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.

Information offences

Under Regulation 88(1) a person commits an offence if, in purported compliance with a requirement imposed on them under the Regulations, they knowingly or recklessly make a statement which is false or misleading in a material particular.

The penalty for an offence under Regulation 88(1) 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.
- On conviction on indictment: a term of imprisonment not exceeding two years or a fine or both.

Under Regulation 88(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 Regulation 88(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.
- On conviction on indictment: a term of imprisonment not exceeding two years or a fine or both.

10.5 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.

10.5 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.

Chapter 11 – Civil liability

11.1 General comments

The Proceeds of Crime Act 2002 aims to deprive wrongdoers of the benefits of crime, not compensate the victims. The civil law provides an opportunity for victims to take action against wrongdoers and those who have assisted them, through a claim for constructive trusteeship. Victims often target the professional adviser in civil claims because they are more likely to be able to pay compensation, often by reason of their professional indemnity cover.

If you believe that you may have acted as a constructive trustee, you should seek legal advice.

11.2 Constructive trusteeship

Constructive trusteeship arises as a result of your interference with trust property or involvement in a breach of fiduciary duty. These are traditionally described respectively as knowing receipt and knowing assistance.

Your liability in either case is personal, an equitable liability to account, not proprietary. A constructive trustee has to restore the value of the property they have received or compensate the claimant for the loss resulting from the assistance with a breach of trust or fiduciary duty. See *Lord Millett in Dubai Aluminium Co Ltd v Salaam* [2002] 3 WLR 1913,1933.

The state of your knowledge is key to this liability. Records of CDD measures undertaken and disclosures or your notes provide evidence of your knowledge and intentions.

11.3 Knowing receipt

Liability for knowing receipt will exist where a person receives property in circumstances where the property is subject to a trust or fiduciary duty and contrary to that trust applies the property for their use and benefit. Considering each element in turn:

11.3.1 Receipt

- You must have received the property in which the claimant has an equitable proprietary interest.
- The property must be received:
    - in breach of trust;
    - in breach of a fiduciary duty, or
    - legitimately, but then misapplied.

11.3.2 For your use and benefit

When you receive money, e.g. as an agent, or, as in the case of a client account, as a trustee of a bare trust, then you are not liable for knowing receipt as it is not received for your use or benefit. You may however still be liable for knowing assistance.

Receiving funds that you apply in satisfaction of your fees will however be beneficial receipt and could amount to knowing receipt.

11.3.3 You must be at fault

What constitutes fault here is the subject of some debate. The Court of Appeal in BCCI v Akinele [2001] Ch.437 held that the test is whether you acted unconscionably. The test is a subjective one which includes actual knowledge and willful blindness. The factors the court identified were that:

1. You need not have acted dishonestly. It is enough to know a fiduciary or trust duty has been breached.
2. Your knowledge of the funds' provenance should be such that it was unconscionable for you to retain any benefit.

It is unclear whether a reckless failure to make enquiries a reasonable person would have made would be sufficient to establish liability. In *Dubai Aluminium Co Ltd v Salaam* [2002] 3 WLR 1913 1933 Lord Millett described knowing receipt as dishonest assistance. However, that may well have been specific to the particular facts he was considering.

11.4 Knowing assistance

If you help in a breach of fiduciary or trust duties then you are personally liable for the damage and loss caused. See *Twinsectra v Yardley* [2002] WLR 802.

The requirements to establish liability of this kind are:

11.4.1 Assistance in a breach of trust or fiduciary duty

The breach need not have been fraudulent, (see *Royal Brunei Airlines v Tan* [1995] 2 AC 378), and you do not need to know the full details of the trust arrangements you help to breach, nor the obligations incumbent on a trustee/fiduciary. You assist if you either:

- know that the person you are assisting is not entitled to do the things that they are doing; or
- have sufficient ground for suspicion of this

11.4.2 Fault test

There must be dishonesty, not just knowledge. The test for dishonesty is objective. The Privy Council in *Eurotrust v Barlow Clowes* [2006]1 All ER stated that the test is whether your conduct is dishonest by the standards of reasonable and honest people, taking into account your specific characteristics and context, i.e. your intelligence, knowledge at the relevant time, and your experience.

Conscious impropriety is not required; it is enough to have shown willful blindness by deliberately failing to make the enquiries that a reasonable and honest person would make.

11.5 Making a disclosure to the NCA

11.5.1 While awaiting consent/DAML from the NCA

Your position can be difficult. While the client will be expecting you to implement their instructions, you may be unable to do so, or give explanations, as you may risk a tipping off offence.

The client may seek a court order for the return of the funds on the basis that you are breaching their retainer.

Case law provides no direct authority on the point, but a ruling on the obligations of banks is helpful in suggesting the courts' likely view of the obligations imposed on legal professionals. In *K v Nat West* the Court of Appeal ruled that a bank's contract with the customer was suspended whilst the moratorium period was in place, so the customer had no right to an injunction for return of monies. The court also said that as a matter of discretion, the court would not force the bank to commit a crime.

The Court of Appeal also approved the use of a letter to the court from the bank as evidence of its suspicion. Provision of evidence in these circumstances is permitted under s333(2)(b) of Proceeds of Crime Act as an exception to the tipping off provisions.

11.5.2 Where the NCA grants consent/DAML

In continuing with a transaction you will have to show that either:

- Although you had sufficient suspicion to justify a disclosure to the NCA, your concerns were not such as to render them accountable on a constructive trustee basis. Courts are likely to take into account the fact that you will generally operate in the regulated sector, and assume a degree of sophistication as a result of anti-money laundering training. Legal professionals are expected to be able to account for decisions to proceed with transactions; or
- Your suspicions were either removed or reduced by subsequent information or investigations.

The Courts have provided limited assistance in this area. *Bank of Scotland v A Limited* [2001]1WLR 751 stated that complying with a client's instructions was a commercial risk which a bank had to take. While the court gave some reassurance on the unlikelihood of any finding of dishonesty against an institution that had sought guidance from the court and did not pay funds away, this is of limited assistance because it is for the positive act of paying away funds that protection will be needed.

Such protection is not readily available. In *Amalgamated Metal Trading v City of London Police* [2003] 1 WLR 2711 the court held that while a court could make a declaration on whether particular funds were the proceeds of crime, a full hearing would be required with both the potential victim and the client participating. There

would have to be proof on the balance of probabilities that the funds were not the proceeds of crime. In practice this is highly unlikely to be practical.

11.6 Civil liability in relation to SARs

Under section 338(4A) of the Proceeds of Crime Act 2002: '[w]here 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'.

Chapter 12 – Money laundering warning signs

Note: The following sections of this chapter do not apply to barristers or advocates for the reasons set out in section 1.1.1:

- 12.2.3 (Use of client accounts)
- 12.3.1 (Administration of estates)
- 12.3.4 (Powers of attorney/deputyship)

12.1 General comments

The Regulations require you to conduct 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 chapter highlights a number of warning signs for legal professionals generally and for those dealing with particular types of work, to help you decide whether you have reasons for concern or the basis for a disclosable suspicion.

12.2 General warning signs during a retainer

Because money launderers are always developing new techniques, no list of examples can be fully comprehensive; however, here are some key factors which may arise after client and retainer acceptance and give you cause for concern.

12.2.1 Secretive clients

While face-to-face contact with clients is not always necessary, an excessively obstructive or secretive client may be a cause for concern.

12.2.2 Unusual instructions

Instructions that are unusual in themselves, or that are unusual for your practice or your client, may give rise to a cause for concern.

Instructions outside your area of expertise

Taking on work which is outside your practice's normal range of expertise can be risky because money launderers might use such practices to avoid answering too many questions. An inexperienced legal professional might be influenced into taking steps which a more experienced legal professional would not contemplate. Be wary of instructions in niche areas of work in which your practice has no background, but in which the client claims to be an expert.

If your client is based a long way from your offices, consider why you have been instructed. For example, have your services been recommended by another client or is the matter based near your practice? Making these types of enquiries makes good business sense as well as being a sensible anti-money laundering check.

Changing instructions

Instructions or cases that change unexpectedly might be suspicious, especially if there seems to be no logical reason for the changes.

The following situations could give rise to a cause for concern. Legal professionals should consider Accounts Rules if appropriate:

- a client deposits funds into your client account but then ends the transaction for no apparent reason;
- a client tells you that funds are coming from one source and at the last minute the source changes;
- 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.

Unusual retainers

Be wary of:

- disputes which are settled too easily as this may indicate sham litigation;
- loss-making transactions where the loss is avoidable;
- 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;
- settlements paid in cash, or paid directly between parties – for example, if cash is passed directly between sellers and buyers without adequate explanation, it is possible that mortgage fraud or tax evasion is taking place;
- transactions which appear to be complex or unusually large, having regard to the parties involved; and
- unusual patterns of transactions which have no apparent economic purpose.

12.2.3 Use of client accounts

Only use client accounts to hold client money for legitimate transactions for clients, or for another proper legal purpose. Putting the proceeds of crime through a client account can give the funds the appearance of legitimacy, whether the money is sent back to the client, on to a third party, or invested in some way. Introducing cash into a banking system can become part of the placement stage of money laundering. Therefore, the use of cash may be a warning sign.

Establish a policy on handling cash

Large payments made in actual cash may also be a sign of money laundering. It is good practice to establish a policy of not accepting cash payments above a certain limit either at your office or into your bank account.

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 transaction. Avoid

disclosing your client account details as far as possible and make it clear that electronic transfer of funds is expected.

If a cash deposit is received, you will need to consider whether you think there is a risk of money laundering taking place and whether it is a circumstance requiring a disclosure to the NCA.

Source of funds

Accounts staff should monitor whether funds received from clients are from credible sources. For example, it is reasonable for monies to be received from a company if your client is a director of that company and has the authority to use company money for the transaction.

However, if funding is from a source other than your client, you may need to make further enquiries, especially if the client has not told you what they intend to do with the funds before depositing them into your account. If you decide to accept funds from a third party, perhaps because time is short, ask how and why the third party is helping with the funding.

You do not have to make enquiries into every source of funding from other parties. However, you must always be alert to warning signs and in some cases you will need to get more information.

In some circumstances, cleared funds will be essential for transactions and clients may want to provide cash to meet a completion deadline. Assess the risk in these cases and ask questions if necessary.

Disclosing client account details

Think carefully before you disclose your client account details. They allow money to be deposited into your account without your knowledge. If you need to provide your account details, ask the client where the funds will be coming from. Will it be an account in their name, from the UK or abroad? Consider whether you are prepared to accept funds from any source that you are concerned about.

Keep the circulation of client account details to a minimum. Discourage clients from passing the details on to third parties and ask them to use the account details only for previously agreed purposes.

12.2.4 Suspect territory

Retainers involving countries which do not have comparative money laundering standards may increase the risk profile of the retainer.

Consider whether extra precautions should be taken when dealing with funds or clients from a particular jurisdiction. This is especially important if the client or funds come from a jurisdiction where the production of drugs, drug trafficking, terrorism or corruption is prevalent.

Note also that EDD measures must be applied where a transaction or business relationship is with a person established in a 'high risk third country' (subject to the limited exception set out in Regulation 33(2)). See section 4.12.3.

12.3 Private client work

12.3.1 Administration of estates

The administration of estates is a regulated activity. A deceased person's estate is very unlikely to be actively utilised by criminals as a means for laundering their funds; however, there is still a low risk of money laundering for those working in this area.

Source of funds

When you are acting either as an executor, or for executors, there is no blanket requirement that you should be satisfied about the history of all of the funds which make up the estate under administration; however you should be aware of the factors which can increase money laundering risks.

Consider the following when administering an estate:

- where estate assets have been earned in a foreign jurisdiction, be aware of the wide definition of criminal conduct in POCA and the provisions relating to overseas criminal conduct;
- where estate assets have been earned or are located in a suspect territory, you may need to make further checks about the source of those funds.

The wide nature of the offences of 'acquisition, use and possession' in section 329 of POCA may lead to a money laundering offence being committed at an early point in the administration. The section 328 offence may also be relevant.

Be alert from the outset and monitor throughout so that any disclosure can be considered as soon as knowledge or suspicion is formed and problems of delayed consent/DAML are avoided. A key benefit of the *Bowman v Fels* judgment is that a legal professional who makes a disclosure is now able to continue work on the matter, so long as they do not transfer funds or take any other irrevocable step.

How the estate may include criminal property

An extreme example would be where you know or suspect that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime.

If you know or suspect that the deceased person improperly claimed welfare benefits or had evaded the due payment of tax during their lifetime, criminal property will be included in the estate and so a money laundering disclosure may be required. While administering an estate, you may discover or suspect that beneficiaries are not intending to pay the correct amount of tax or are avoiding some other financial charge (for example, by failing to disclose gifts received from the deceased fewer than seven years before death). Although these matters may not actually constitute money laundering (because no criminal conduct has yet occurred so there is no 'criminal property'), solicitors should carefully consider their position in conduct terms with respect to Principle 1 of the SRA Handbook.

Grant of probate

A UK grant of probate may be required before UK assets can be released, while for overseas assets the relevant local laws will apply. Remain alert to warning signs, for example if the deceased or their business interests are based in a suspect territory.

If the deceased person is from another jurisdiction and a legal professional is dealing with the matter in the home country, it may be helpful to ask that person for information about the deceased to gain some assurances that there are no suspicious circumstances surrounding the estate. The issue of the tax payable on the estate may depend on the jurisdiction concerned.

12.3.2 Trusts

Trust work is a regulated activity.

Trusts can be used as a money laundering vehicle. One risk period for trusts is when the trust is set up, as if the funds going into the trust are clean, it is only by the settlor, beneficiaries or other persons who control the trust requiring the trustees to use them for criminal purposes that they may form the proceeds of crime.

When setting up a trust, be aware of general money laundering warning signs and consider whether the purpose of the trust could be to launder criminal property. Could funds be being paid offshore illegitimately to reduce properly taxable profits in an onshore jurisdiction? Information about the purpose of the trust, including why any unusual structure or jurisdiction has been used, can help allay concerns. Similarly, information about the provider of the funds, the trust's beneficial owners and potential beneficiaries and those who have control of the funds, as required by the Regulations, will assist.

Whether you act as a trustee yourself, or for trustees, the nature of the work may already require information which will help in assessing money laundering risks, such as the location of assets and the identity of the trust’s beneficial owners and potential beneficiaries. Again, any involvement of a suspect jurisdiction, especially those with strict bank secrecy and confidentiality rules, or without similar money laundering procedures, may increase the risk profile of the retainer.

If you think a money laundering offence has, or may have, been committed that relates to money or property which already forms part of the trust property, or is intended to do so, consider whether your instructions involve you in a section 328 arrangement offence. If they do, consider the options for making a disclosure.

Consider also whether a section 330 disclosure obligation has been triggered.

12.3.3 Charities

In common with trusts, while the majority of charities are used for legitimate reasons, they can be used as money laundering/terrorist financing vehicles.

If you are acting for a charity, consider its purpose and the organisations with which it is aligned. A charity which is registered with the Charity Commission is likely to be low risk. If you are receiving 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.

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. See also 9.6 of OFSI's Financial Sanctions Guidance.

https://www.gov.uk/government/publications/financial-sanctions-faqs

12.3.4 Powers of attorney/deputyship

Whether acting as, or on behalf of, an attorney or deputy, you should remain alert to money laundering risks.

Consider also your obligations to identify the authority of attorney or deputy to act on behalf of the client and verify their identity pursuant to Regulation 28(10).

If you are acting as an attorney you may learn financial information about the donor relating, for example, to non-payment of tax or wrongful receipt of benefits. You will need to consider whether to make a disclosure to the NCA.

Where the public guardian has an interest - because of a deputyship or registered enduring power of attorney - consider whether the Office of the Public Guardian (OPG) needs to be informed. Informing the OPG is unlikely to be tipping off because it is unlikely to prejudice an investigation.

If you discover or suspect that a donee has already completed an improper financial transaction that may amount to a money laundering suspicion, a disclosure to the NCA may be required (depending on whether legal professional privilege applies). However, it may be difficult to decide whether you have a suspicion if the background to the information is a family dispute.

12.4 Property work

12.4.1 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. Whilst you will need to identitfy the property-owning vehicle's beneficial owners where it is your client, consider advising a client in a property transaction whose counterparty is evidently a nominee company or recently formed special purpose vehicle, to obtain some information about the vehicle's beneficial owner.

Be alert to sudden or unexplained changes in ownership. One form of laundering, known as flipping, involves a property purchase, often using someone else's identity. The property 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.

Another potential cause for concern is where a third party is providing the funding for a purchase, but the property is being registered in someone else's name. There may be legitimate reasons for this, such as a family arrangement, but you should be alert to the possibility of being misled about the true ownership of the property. You may wish to undertake further CDD measures on the person providing the funding.

12.4.2 Methods of funding

Many properties are bought with a combination of deposit, mortgage and/or equity from a current property. Usually, as a legal professional, you will have information about how your client intends to fund the transaction, and will expect to be updated if those details change, for example if a mortgage falls through and new funding is obtained.

This is a sensible risk assessment measure which should help you decide whether you need to know more about the transaction.

Private funding

Purchase funds can comprise all or some private funding, with the balance of the purchase price being provided via a mortgage. Transactions that do not involve a mortgage have a higher risk of being fraudulent.

Look out for:

- large payments from private funds, especially if your client has a low income
- payments from a number of individuals or sources

If you are concerned:

- ask your client to explain the source of the funds. Assess whether you think their explanation is valid - for example, the money may have been received from an inheritance or from the sale of another property;
- consider whether the beneficial owners were involved in the transaction in the funds flow.

Remember that payments made through the mainstream banking system are not guaranteed to be clean.

Funds from a third party

Third parties often assist with purchases, for example relatives often assist first time home buyers. You may be asked to receive funds directly from those third parties. You will need to decide whether, and to what extent, you need to undertake any CDD measures in relation to the third parties. You may need to explain the identity of third party payers to your pooled client account to your bank on request.

Consider whether there are any obvious warning signs and what you know about:

- your client;
- the third party;
- their relationship; and
- the proportion of the funding being provided by the third party.

Consider your obligations to the lender in these circumstances – you are normally required to advise lenders if the buyers are not funding the balance of the price from their own resources.

Where you act for a vendor, you will also typically receive funds from the buyer or their solicitors, which you may hold on the buyer's behalf, pending an exchange or completion process. Where funds come direct from an unrepresented buyer you will need to undertake full CDD on the buyer.

Direct payments between buyers and sellers

You may discover or suspect that cash has changed hands directly, between a seller and a buyer, for example at a rural auction.

If you are asked to bank the cash in your client account, this presents a problem because the source of the cash is not your client and so checks on the source of the funding can be more difficult. The auction house may be able to assist because of checks they must make under the Regulations. However, you may decide to decline the request.

If you suspect that there has been a direct payment between a seller and a buyer, consider whether there are any reasons for concern (for example, an attempt to involve you in tax evasion) or whether the documentation will include the true purchase price.

A client may tell you that money is changing hands directly when this is not the case. This could be to encourage a mortgage lender to lend more than they would otherwise, because they believe that private funds will contribute to the purchase. In this situation, consider your duties to the lender.

12.4.3 Valuing

An unusual sale price (an evident overvalue or undervalue) can be an indicator of money laundering. While you are not required to get independent valuations, if you become aware of a significant discrepancy between the sale price and what you would reasonably expect such a property to sell for, consider asking more questions.

Properties may also be sold below the market value to an associate, with a view to obscuring the title to the property while the original owner still maintains beneficial ownership.

12.4.4 Lender issues

You may discover or suspect that a client is attempting 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. Transactions which are not at arm’s length may warrant particularly close consideration.

However, until the improperly obtained mortgage advance is received there is not any criminal property for the purposes of disclosure obligations under POCA.

If you suspect that your client is making a misrepresentation to a mortgagee you must either dissuade them from doing so or cease acting. Even if you no longer act for the client you may still be under a duty to advise the mortgage company.

If you discover or suspect that a mortgage advance has already been improperly obtained, consider advising the mortgage lender.

If you are acting in a re-mortgage and discover or suspect that a previous mortgage has been improperly obtained, you may need to advise the lender, especially if the re-mortgage is with the same lender. You may also need to consider making a disclosure to the NCA as there is criminal property (the improperly obtained mortgage advance).

Legal professional privilege

If your client has made a deliberate misrepresentation on their mortgage application you should consider whether the crime/fraud exemption to legal professional privilege will apply, so that no waiver to confidentiality will be needed before a disclosure is made.

However, you will need to consider matters on a case-by-case basis and if necessary, seek legal advice.

Tipping off offences

You may be concerned that speaking to the lender client conflicts with tipping off offences.

A key element of these offences is the likelihood of prejudicing an investigation. The risk of this is small when disclosing to a reputable lender or your insurer. The financial services sector is also regulated for the purposes of anti-money laundering and subject to the same obligations. There is also a specific defence of making a disclosure for the purposes of preventing a money laundering offence.

In relation to asking further questions of your client and discussing the implications of the Proceeds of Crime Act 2002, there is a specific defence for tipping off for legal advisers who are seeking to dissuade their client from engaging in a money laundering offence.

For further advice on tipping off, see section 6.8.

For further information about avoiding tipping off in a particular case, contact the NCA's Financial Intelligence Helpdesk on 020 7238 8282.

12.4.5 Tax issues

Tax evasion of any type, whether committed by your client or the other party to a transaction, can result in you committing a section 328 arrangements offence.

Your firm may also be exposed to the offence of corporate failure to prevent the facilitation of tax evasion under the Criminal Finances Act 2017 if one of your employees or associated persons facilitates tax evasion.

Abuse of the Stamp Duty Tax procedure may also have money laundering implications, for example if the purchase price is recorded incorrectly.

If a client gives you instructions which offend the Stamp Duty Land Tax procedure, you must consider your position in relation to your professional obligations. If you discover the evasion after it has occurred, you are obliged to make a disclosure, subject to any legal professional privilege.

12.5 Company and commercial work

The nature of company structures can make them attractive to money launderers because it is possible to obscure true ownership and protect assets for relatively little expense. For this reason legal professionals working with companies and in commercial transactions should remain alert throughout their retainers, with existing as well as new clients.

12.5.1 Forming a new company

If you work on the formation of a new company, be alert to any signs that it might be misused for money laundering or terrorist financing.

If the company is being formed in a foreign jurisdiction, you should clarify why this is the case. In countries where there are few anti-money laundering requirements, you should make particularly careful checks.

Refuse the retainer if you have doubts or suspicions.

12.5.2 Holding of funds

If you wish to hold funds as stakeholder or escrow agent in commercial transactions, consider the checks you wish to make about the funds you intend to hold, before the funds are received and whether it would be appropriate to conduct CDD measures on all those on whose behalf you are holding funds, particularly if any of them are unrepresented.

Consider any proposal that you collect funds from a number of individuals, whether for investment purposes or otherwise. This could lead to wide circulation of your client account details and payments being received from unknown sources.

12.5.3 Private equity

Legal professionals could be involved in any of the following circumstances:

- the start-up phase of a private equity business where individuals or companies seek to establish a private equity firm (and in certain cases, become authorised to conduct investment business);
- the formation of a private equity fund;
- ongoing legal issues relating to a private equity fund; and
- execution of transactions on behalf of a member of a private equity firm's group of companies, (a private equity sponsor), that will normally involve a vehicle company acting on its behalf, (newco).

Who is the client?

Start-up phase

In this phase, as you will be approached by individuals or a company seeking to become established (and in certain cases authorised) your client would be the individuals or company and you would therefore conduct CDD accordingly.

Formation of private equity funds

Your client may be the private equity sponsor or it may be an independent sponsor.

Consider whether you are advising the fund itself and whether you need to identify its investor beneficial owners.

You should therefore identify who your client is and apply the CDD measures according to their client type as set out in Chapter 4.

Where the client is a newco, you will need to obtain documentation evidencing the establishment of the newco and consider the issue of beneficial ownership.

Generally private equity work will be considered at low risk of money laundering or terrorist financing for the following reasons:

- private equity firms in the UK are also covered by the Regulations as a financial institution and they are regulated by the FCA;
- investors in private equity funds may be large institutions, some of which will also be regulated for money laundering purposes ;
- where the private equity sponsor or fund manager is regulated in the UK, EEA or a comparable jurisdictions, it is likely to have followed CDD processes prior to investors being accepted but their risk-based procedures and reputational risk appetite may be different from yours;
- the investment is generally illiquid and the return of capital is unpredictable;
- the terms of the fund documentation control the transfer of interests and the return of funds to investors.

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 (a private equity fund of funds);
- where the private equity sponsor is seeking to raise funds for the first time.

You may wish to consider the JMLSG Guidance.

The following points should be considered when undertaking CDD measures in relation to private equity work:

- where your client qualifies for simplified due diligence you do not have to identify beneficial owners unless there is a suspicion of money laundering; but ensure you identify your client correctly as where you are acting for the benefit of the fund as opposed to for the benefit of the investment manager, you will need to identify and consider the fund's investor beneficial owners;
- where simplified due diligence does not apply you need to consider the business structure of the client and conduct CDD on the client in accordance with that structure;

- where there is an appropriately regulated professional closely involved with the client who has detailed knowledge of the beneficial owners of the client, you may consider relying on them in accordance with Regulation 39;
- 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-sensitive basis, issues to consider include:
    - the profile of the private equity sponsor, fund manager, (if different), or such other person;
    - their track record within the private equity sector; and
    - their willingness to explain identification procedures and provide confirmation that all beneficial owners have been identified.
- where you are using another person as an information source for beneficial owners, where there are no beneficial owners within the meaning of Regulation 6, the source may simply confirm their actual knowledge of this, or if beneficial owners do exist, the source should provide you with the identifying details of the beneficial owner or an assurance that the beneficial owners have been identified and that the details will be provided on request.
- where there is a tiered structure, such as a feeder fund or fund of funds structure, you must identify the beneficial owner but you may decide having made enquiries that no such beneficial owners exist even though you have got to the top of the structure.
- where it is envisaged that you will be acting for a newco which is to be utilised at a future point in a flotation or acquisition, it is only once they are established and signed up as a party to the transaction that you need to commence CDD measures on the newco. However, once you start acting for a newco, you will need to consider identification for it, and its beneficial owner. You may therefore wish to commence the process of identifying any beneficial owner in advance.

12.5.4 Collective investment schemes

Undertaking work in relation to retainers involving collective investment schemes may pose similar problems when undertaking CDD as for private equity work.

The risk factors with respect to a collective investment scheme will be decreased where:

- the scheme is only open to tax exempt institutional investors;
- investment managers are regulated individuals or entities;
- 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 equivalent to the third directive;

- neither the scheme nor the investment managers are regulated and do not conduct CDD on the investors.

You may also wish to take into account the JMLSG Guidance.

In addition to the points to consider outlined for private equity work, where a collective investment scheme has issued a prospectus it is advisable to review a copy of the prospectus to understand the intended structure of the investment scheme.

Chapter 13 – offences and reporting practical examples

13.1 General comments

Chapters 6 and 7 of this guidance worked through the theory of the law relating to when a money laundering offence has occurred, the requirements for making a disclosure and when you are unable to make a disclosure because of LPP or are exempted from making a disclosure due to privileged circumstances.

This chapter contains:

- flowcharts to give an overview of how all the obligations link together; and
- examples to help put the theory into context.

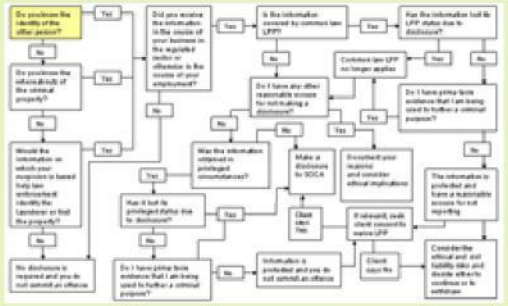
This chapter does not replace application of the legislation to your situation; nor should it be viewed without reference to the detailed discussion of the law in the rest of the guidance.

Further examples may be added to future editions of this guidance.

13.2 Principal offences

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.

Do I have a suspicion that a principal money laundering offence is occurring?



Download the decision chart (PDF, 25kb)

13.2.1 Do I have an arrangement?

Under section 328, an arrangement must be created at a particular point in time. If you have formed a suspicion, first consider whether an arrangement already exists. For example, a client may instruct you to act for them in the purchase of a property, including the drafting of the contract and transfer documents. When you are instructed there will already an arrangement between the vendor and the purchaser, but not yet an arrangement for the purposes of section 328.

If an arrangement within section 328 already exists, any steps you take to further that arrangement will probably mean you are concerned in it. In this case, you would immediately need to consider making a disclosure.

13.2.2 No pre-existing arrangement

If there is no pre-existing arrangement, the transactional work you carry out may bring an arrangement under section 328 into existence. You may become concerned in the arrangement by, for example, executing or implementing it, which may lead you to commit an offence under section 328, and possibly under section 327 or 329.

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

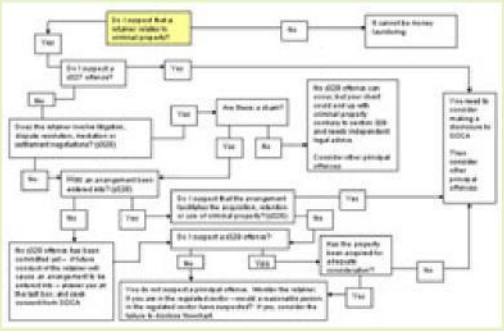
If you are acting within the regulated sector, consider whether you risk committing a failure to disclose offence, if you do not make a disclosure to the NCA.

The following two flowcharts show the issues to consider when deciding whether to make a disclosure to the NCA.

I suspect continuation of a retainer will lead to me being a party to a principal offence. Do I have a defence?

Download the decision chart (PDF, 24kb)

I suspect someone else of a principal offence, or should reasonably suspect them, and am concerned I may commit a failure to disclose offence. Do I have a defence?



Download the decision chart (PDF, 27kb)

13.3 Should I make a disclosure?

13.3.1 Property transactions

Considering further the earlier example of a suspect contract for the purchase of a property, the following issues will be relevant when considering the disclosure requirements under POCA.

- If the information on which your suspicion is based is covered by LPP and the crime/fraud exception does not apply, you cannot make a disclosure under POCA.
- If the information was received in privileged circumstances and the crime/fraud exception does not apply, you are exempt from the relevant provisions of POCA, which include making a disclosure to the NCA.
- If neither of these situations applies, the communication will still be confidential. However, the material is disclosable under POCA and an authorised disclosure should be made

You have the option of withdrawing from the transaction rather than making an authorised disclosure, but you may still need to make a disclosure to avoid committing a failure to disclose offence.

What if I cannot disclose?

If you decide that either you cannot make a disclosure due to LPP or you are exempt from making a disclosure due to privileged circumstances, you have two options:

- you can approach the client for a waiver of privilege to make a disclosure and obtain consent/DAML to carry out the prohibited act, or
- you should consider your ethical obligations and whether you need to withdraw from the transaction

Waiver of privilege

When approaching your client for a waiver of privilege, you may feel less concerned about tipping off issues if your client is not the suspect party but is engaged in a transaction which involves criminal property. However, if you suspect that your client is implicated in the underlying criminal conduct, consider the tipping off offence and whether it is appropriate to discuss these matters openly with your client.

If you raise the matter with your client and they agree to waive privilege, you can make a disclosure to the NCA on your own or jointly with your client and seek consent if required.

If you are acting for more than one client on a matter, all clients must agree to waive privilege before you can make a disclosure to the NCA.

Refusal to waive privilege

Your client, whether sole or one of a number for whom you act, may refuse to waive privilege, either because he does not agree with your suspicions or because he does not wish a disclosure to be made. Unless your client provides further information which removes your suspicions, you must decide whether you are being used in a criminal offence, in which case neither LPP nor privileged circumstances apply.

If your client refuses to waive privilege but accepts that in proceeding with the transaction he may be committing an offence, you might conclude that you are being used in a criminal offence in which case neither exemption applies. In such circumstances it is not appropriate to tell the client that you are making the disclosure, as the risks of tipping off are increased.

If you are unable to make a disclosure, consider the ethical and civil risks of continuing in the retainer and consider withdrawing.

Consent/DAML and progressing the retainer

If you make a disclosure and consent/DAML is needed, consider whether you can continue working on the retainer before you receive that consent/DAML.

This will depend on whether an arrangement already exists or whether the further work will bring the arrangement into existence. Provided there is no pre-existing arrangement you should be free to continue your preparatory activities. However, the arrangement/prohibited act should not be finalised without appropriate consent/DAML.

13.3.2 Company transactions

Criminal property in a company

The extent of the regulatory and legal obligations affecting companies and businesses means that there is an increased possibility that breaches will have been committed by your client that constitute criminal conduct and give rise to criminal property under POCA.

For example, the Companies Act 1985 contains many offences which will give rise to criminal property as defined by POCA. There does not need to be a criminal conviction, nor even a prosecution underway. If criminal conduct has, (or is suspected to have) taken place, and a benefit has been achieved, the result is actual or notional criminal property.

For a number of offences, the only benefit to your client (for the purposes of POCA) is saved costs. For example, it is criminal conduct to fail to notify the Information Commissioner that a

company will be processing 'personal data'. The saved notification fee should be treated as criminal property for the purposes of POCA.

It may be difficult to establish whether property or funds which are the subject of the transactions are the 'saved costs' in whole or in part and are therefore tainted. If you are dealing with the whole of a company's business or assets, no distinction is necessary. In other cases, it would be wrong to assume that because some assets are tainted, they all are, or that you are dealing with the tainted ones.

In most cases, unless there is some basis for suspecting that the assets in question result from saved costs, no disclosure or consent/DAML may be required in respect of the principal offence. However, a disclosure may still be required in respect of the failure to disclose offences.

Mergers and acquisitions

In typical corporate merger/acquisition/sale/take-over transactions, there are a number of issues to consider.

Legal professionals acting in company transactions will be acting in the regulated sector and so will have dual disclosure obligations, under the failure to disclose offence and in respect of the principal offences.

Different tests have to be applied to determine whether a disclosure can be made. When you are considering whether you are obliged to make a disclosure to avoid committing a failure to disclose offence, either LPP or privileged circumstances may apply.

When you are considering whether you must make a disclosure as a defence to the principal offences, only LPP is relevant.

For example, when you are acting for a vendor, you may receive information from the client about the target company which is protected under LPP and exempt from disclosure due to privileged circumstances. However, you may receive information from other representatives of the client (such as other professional advisers) which may only be exempt due to privileged circumstances. If information received is initially privileged, you need to consider whether the privilege is lost in the course of the transaction.

The information may be put into a data room and the purchaser, as part of the due diligence inquiries, may raise questions of the vendor's legal representatives which, in effect, result in the information being received again by the vendor's legal representatives.

That second receipt from the purchaser, or their legal representative, would not be protected by privileged circumstances. It will lose its exemption from disclosure unless the information was also subject to LPP which had not been waived when it was placed in the data room (eg a letter of advice from a legal professional to the vendor).

Consider whether privilege is removed by the crime/fraud exception. You may suspect, or have reasonable grounds to suspect someone of money laundering (which may simply mean they possess the benefits of a criminal offence contrary to section 329). Where the information on which the suspicion is based could be protected by LPP or exempted due to privileged circumstances, consider whether the crime/fraud exception applies

This may depend on:

- the nature of the transaction;
- the amount of the criminal property;

- the strength of the evidence.

These factors are considered in more detail below with respect to specific types of company sales.

Asset sales

In the case of an asset sale, all or some of the assets of the business may be transferred. If any asset transferred to a new owner is criminal property, a money laundering offence may be committed:

- The vendor may commit a section 327 offence by transferring the criminal property;
- Both the vendor and purchaser may be entering into an arrangement contrary to section 328;
- The purchaser may be committing a section 329 offence by possessing the criminal property

Adequate consideration defence

When looking at the purchaser's position, you will need to consider whether there would be an adequate consideration defence to a section 329 possession offence. This is where the purchase price is reasonable and constitutes adequate consideration for any criminal property obtained. In such a case, should the purchaser effectively be deprived of the benefit of that defence by section 328.

It is a question of interpretation whether sections 328 and 329 should be read together such that, if the defence under section 329 applies, an offence will also not be committed by the vendor under section 328. You should consider this point and take legal advice as appropriate.

Disclosure obligations after completion

As well as making disclosures relating to the transaction, vendors and purchasers will need to consider disclosure obligations in respect of the position after completion.

The purchaser will, after the transaction, have possession of the assets and may be at risk of committing a section 329 offence (subject to the adequate consideration defence outlined above).

The vendor will have the sale consideration in their possession. If the amount of the criminal property is material, the sale consideration may indirectly represent the underlying criminal property and the vendor may commit an offence under section 329.

Whether the criminal property is material or not will depend on its impact on the sale price. For example, the sale price of a group of assets may be £20m. If the tainted assets represent 10 per cent of the total, and the price for the clean assets alone would be £18m, it is clear that the price being paid is affected by, and represents in part, the criminal property.

If a client commits one of the principal money laundering offences, whether you are acting for the vendor or purchaser, you will be involved in a prohibited act. You will need to make a disclosure along with your clients and obtain appropriate consent/DAML.

When considering whether to advise your client about their disclosure obligations, remember the tipping off offences.

Am I prevented from reporting due to LPP?

Where you are acting for either the purchaser or vendor and conclude that you may have to make a disclosure and seek consent/DAML, first consider whether LPP applies. As explained above, this depends on how you received the information on which your suspicion is based.

Generally, when acting for the purchaser, if the information comes from the data room, LPP will not apply. When acting for the vendor, LPP may apply if the information has come from the client for the purpose of obtaining legal advice.

The crime/fraud exception

Where LPP applies, you will also need to consider whether the crime/fraud exception applies. The test is whether there is prima facie evidence that you are being used for criminal purposes.

Whether the crime/fraud exception applies will also depend on the purpose of the transaction and the amount of criminal property involved. For example, if a company wished to sell assets worth £100m, which included £25 of criminal assets, it would be deemed that the intention was not to use legal professionals for criminal purposes but to undertake a legitimate transaction. However, if the amount of criminal property was £75m, the prima facie evidence would be that the company did intend to sell criminal property and the exception would apply to override LPP.

Real cases will not all be so clear-cut. Consider the parties' intentions. If you advise your client of money laundering risks in proceeding with a transaction and the client decides, despite the risks, to continue without making a disclosure, you may have grounds to conclude that there was prima facie evidence of an intention to use your services for criminal purposes and therefore that privilege may be overridden.

Remember that for the purposes of the crime/fraud exception, it is not just the client's intention that is relevant.

Where LPP applies and is not overridden by the crime/fraud exception, it is nonetheless possible for your client to waive the privilege in order for a disclosure to be made.

Share sales

A sale of a company by way of shares gives rise to different considerations to asset sales. Unless shares have been bought using the proceeds of crime they are unlikely to represent criminal property, so their transfer will not usually constitute a section 327 offence, (for the vendor), or a section 329 offence, (for the purchaser).

However, the sale of shares could constitute a section 328 offence, depending on the circumstances, particularly if the criminal property represents a large percentage of the value of the target company. Consent/DAML may be needed if:

- the benefit to the target company from the criminal conduct is such that its share price has increased;
- as part of the transaction directors will be appointed to the board of the target company and they will use or possess criminal property; or
- the purpose of the transaction is to launder criminal property. That is, it is not a genuine commercial transaction.

Is the share value affected by criminal property?

If a company has been used to commit criminal offences, some or all of its assets may represent criminal property. The value of the shares may have increased as a result of that criminal activity. When the shares are then sold, by converting a paper profit into cash, the vendor and the purchaser have both been involved in a prohibited arrangement

For example, if 10 per cent of the profits of a company are earned from criminal activity, it is likely that the share price would be lower if only the legitimate profits were taken into account.

However, if the value of the criminal property is not sufficient to affect the purchase/sale price, the transaction is unlikely to be considered a prohibited arrangement since the vendor does not benefit from the company's criminal conduct. For example, a company is being purchased for £100m and within it is £25 of saved costs. If the costs had been paid by the company, it is unlikely that the price would be £99,999,975. The business is still likely to be valued at £100m.

Where criminal property is immaterial

Even if the value of criminal property is very small and immaterial to the purchase price, purchasers still need to consider their position after the acquisition. While shareholders do not possess a company's assets, the target company and directors may subsequently transfer, use or possess the assets for the purposes of the principal money laundering offences in sections 327 and 329.

If as part of the transaction, the purchaser proposes appointing new directors to the board of the target company, those directors may need to make a disclosure and seek consent/DAML so that they may transfer use or possess and use the criminal property.

In this case, you, and the vendors and the existing and new directors, may still need to make a disclosure, (subject to LPP issues), and seek consent/DAML, because they will be involved in an arrangement which involves the acquisition, use or control of criminal property by the new directors contrary to section 328.

In summary, the position may be as follows where the amount of the criminal property is immaterial:

- The target company will possess the proceeds of criminal conduct and may need to make a disclosure. If you discover this in privileged circumstances or it is protected by LPP, you cannot make a disclosure unless the fraud/crime exception applies.
- Those individuals or entities which, as a result of the transaction, will be in a position after completion to possess and use criminal property will need to make a disclosure and seek consent/DAML before completion.
- The legal professionals acting on the transaction and the vendor may also need to make a disclosure if they are involved in an arrangement which facilitates the acquisition or use of criminal property.
- Whenever a disclosure must be made, you must first consider whether privilege applies and, if applicable, whether the fraud/crime exception applies.

Shareholders

Generally, in a purchase or sale transaction, you will act for the company, not for its shareholders. However, it is possible for shareholders to become involved in an

arrangement prohibited by section 328. This is most likely to happen when the transaction requires a Class I or Class II circular to shareholders under the listing rules.

Firstly, consider whether the shareholders are, or may become, aware – perhaps through the risk warnings in the circular – of the risk of criminal conduct. Unless they are so aware, they are unlikely to have the necessary suspicion to be at risk of committing a money laundering offence.

Secondly, where shareholders are aware of the criminal conduct, consider whether the amount of criminal property is material to the transaction. That is, it would have an impact on the price or terms. If it is material, by voting in favour of it the shareholders will become concerned in a prohibited arrangement and will be required to make a disclosure and seek consent/DAML.

Also consider, in the context of an initial public offering, what risk warnings to include in any prospectus. You may need to give shareholders notice of their disclosure obligations via such a risk warning.

It is good practice to discuss the issue with the NCA to ensure that there are no tipping off concerns if details of the risks are set out in the public circular.

When each shareholder requires consent/DAML from the NCA, their express authority to make the disclosure will be required. It may be simplest to ask the shareholders to authorise the board of the vendor to make a disclosure and seek consent/DAML on their behalf at the same time as asking them to give conditional approval for the transaction.

Overseas conduct

Where your suspicion of criminal conduct relates in whole or in part to overseas conduct, be aware of the wide definition of criminal conduct.

For example, you might discover or suspect that a company or its foreign subsidiary has improperly manipulated its accounting procedures so that tax is paid in a country with lower tax limits. Or you might form a concern about corrupt payments to overseas commercial agents which might be illegal in the UK.

Even where the conduct is lawful overseas, in serious cases it will still be disclosable if the money laundering is taking place in the UK and the underlying conduct would be criminal if it had occurred in the UK.

In some cases the only money laundering activity in the UK may be your involvement in the transaction as a UK legal professional.