



The Law Society

Anti-money laundering

Practice note

October 2009

supporting
solicitors

Contents

Definitions and glossary	5
Definitions.....	5
Glossary	7
Chapter 1 – introduction	9
1.1 Who should read this practice note?	9
1.2 What is the issue?	9
1.3 Definition of money laundering.....	9
1.4 Legal framework and other requirements.....	10
1.5 Status of this practice note.....	14
1.6 Terminology in this practice note.....	15
1.7 Other information and products.....	15
1.8 Acknowledgements.....	16
Chapter 2 – the risk-based approach	18
2.1 General comments.....	18
2.2 Application	18
2.3 Assessing your firm's risk profile	19
2.4 Assessing individual risk	20
Chapter 3 – systems, policies and procedures	21
3.1 General comments.....	21
3.2 Application	21
3.3 Nominated officers	21
3.4 Risk assessment.....	22
3.5 Internal controls and monitoring compliance	22
3.6 Customer due diligence	23
3.7 Disclosures	24
3.8 Record keeping.....	24
3.9 Communication and training	27
Chapter 4 – customer due diligence	30
4.1 General comments.....	30
4.2 Application	30
4.3 CDD in general	30
4.4 Ongoing monitoring.....	37
4.5 Records	38
4.6 CDD on clients.....	38
4.7 CDD on a beneficial owner	50

4.8 Simplified due diligence	59
4.9 Enhanced due diligence.....	60
4.10 Existing clients	65
4.11 FATF counter measures	65
4.12 Annex A – Examples of beneficial ownership for a trust.....	67
Chapter 5 – money laundering offences	72
5.1 General comments.....	72
5.2 Application	72
5.3 Mental elements	72
5.4 Principal money laundering offences	74
5.5 Defences to principal money laundering offences	76
5.6 Failure to disclose offences – money laundering.....	78
5.7 Exceptions to failure to disclose offences.....	79
5.8 Tipping off.....	81
Chapter 6 – legal professional privilege	84
6.1 General comments.....	84
6.2 Application	84
6.3 Duty of confidentiality.....	84
6.4 Legal professional privilege.....	85
6.5 Privileged circumstances	88
6.6 Differences between privileged circumstances and LPP	89
6.7 When do I disclose?.....	90
Chapter 7 – terrorist property offences	91
7.1 General comments.....	91
7.2 Application	91
7.3 Principal terrorist property offences.....	91
7.4 Defences to principal terrorist property offences	92
7.5 Failure to disclose offences.....	93
7.6 Defences to failure to disclose	93
7.7 Section 21D tipping off offences: regulated sector	94
7.8 Defences to tipping off	94
7.9 Making enquiries of a client.....	95
7.10 Other terrorist property offences in statutory instruments	95
Chapter 8 – making a disclosure	98
8.1 General comments.....	98
8.2 Application	98
8.3 Suspicious activity reports.....	98

8.4 Feedback on SARs	101
Chapter 9 – enforcement	102
9.1 General comments.....	102
9.2 Supervision under the regulations.....	102
9.3 Disciplinary action	104
9.4 Offences and penalties	104
9.5 Joint liability	107
9.5 Prosecution authorities	107
Chapter 10 – civil liability	108
10.1 General comments.....	108
10.2 Constructive trusteeship.....	108
10.3 Knowing receipt	108
10.4 Knowing assistance	109
10.5 Making a disclosure to SOCA	110
10.6 Notify your professional indemnity insurers	111
Chapter 11 – money laundering warning signs.....	113
11.1 General comments.....	113
11.2 General warning signs	113
11.3 Private client work.....	117
11.4 Property work.....	119
11.5 Company and commercial work	123
Chapter 12 – offences and reporting practical examples.....	127
12.1 General comments.....	127
12.2 Principal offences.....	127
12.3 Should I make a disclosure?	129

Definitions and glossary

Definitions

Beneficial owners	see - chapter 4.7
Business relationship	a business, professional or commercial relationship between a relevant person and a customer, which is expected by the relevant person at the time when contact is established to have an element of duration
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 SOCA under the Proceeds of Crime Act 2002 – also referred to as a suspicious activity report (SAR)
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 6.4
Nominated officer	a person nominated within the firm to make disclosures to SOCA under the Proceeds of Crime Act 2002 – 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 4.4
Overseas criminal conduct	<p>conduct which occurs overseas that would be a criminal offence if it occurred in the UK</p> <p>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</p> <p>that 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</p> <p>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</p> <p>see s102 of SOCPA</p>
Politically exposed persons	see - chapter 4.9.2
Privileged circumstances	see - chapter 6.5
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 firm 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	<p>a firm or sole practitioner who by way of business provides any of the following services to other persons -</p> <ul style="list-style-type: none"> a. forming companies or other legal persons b. acting or arranging for another person to act <ul style="list-style-type: none"> i. as a director or secretary of a company; ii. as a partner of a partnership; or iii. in a similar position in relation to other legal persons; c. 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; d. acting, or arranging for another person to act, as - <ul style="list-style-type: none"> i. a trustee of an express trust or similar legal arrangement; or ii. a nominee shareholder for another person other than a company listed on a regulated market when providing such services.
-----------------------------------	--

Glossary

AIM	Alternative Investment Market
AML / CTF	Anti-money laundering / counter-terrorist financing
CDD	Customer due diligence
EEA	European Economic Area
FATF	Financial Action Task-force
FSA	Financial Services 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

PEPs	Politically exposed persons
POCA	Proceeds of Crime Act 2002
Regulations	Money Laundering Regulations 2007
SARs	Suspicious activity reports
SRA	Solicitors Regulation Authority
SOCA	Serious Organised Crime Agency
Terrorism Act	Terrorism Act 2000
Third directive	Third European Money Laundering Directive

Chapter 1 – introduction

1.1 Who should read this practice note?

All solicitors and other staff in a law firm who are involved in anti-money laundering compliance.

1.2 What is the issue?

Solicitors are key professionals 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 their services are not used to further a criminal purpose. As professionals, solicitors 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, losing revenue and endangering life, and fuelling other criminal activity.

This practice note aims to assist solicitors in England and Wales 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. You can be targeted because a solicitor's firm commonly deals with client money.

1.3.2 Layering

Once proceeds of crime are in the financial system, layering obscures their origins by passing the money through complex transactions. These often involve different entities like companies and trusts and can take place in multiple jurisdictions. You 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 reappear as legitimate funds or assets. They will invest funds in legitimate businesses or other forms of investment, often using you to buy a property, set up a trust, acquire a company, or even settle litigation, among other activities. This is the most difficult stage of money laundering to detect.

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 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.

1.4.2 European Union directives

1991 – first money laundering directive

The European Commission issued this 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 (PDF, 122kb)

This 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, such as independent legal professionals, accountants, auditors, tax advisers and real estate agents. It was incorporated into UK law via the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2003.

2005 – third money laundering directive (PDF, 302kb)

This extended due diligence measures to beneficial owners, recognising that such measures can be applied on a risk-based approach, and required enhanced due diligence to be undertaken in certain circumstances. It is incorporated into UK law by the Money Laundering Regulations 2007 and the Terrorism Act 2000

and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 [\[link\]](#) (the TACT and POCA Regulations 2007).

1.4.3 Proceeds of Crime Act 2002 (POCA)

Scope

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

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

The TACT and POCA Regulations 2007 [\[link\]](#) repealed the s333 POCA tipping off offence. It has been replaced by section 333A which creates two new offences. S342(1) has also been amended to reflect these new offences.

Read more [\[link to 5.8\]](#)

Application

POCA applies to all persons, although certain failure to report offences and the tipping off offences 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 Proceeds of Crime Act 2002, changing the definition of the regulated sector to bring it into line with the Money Laundering Regulations 2007.

Under Schedule 9 of POCA, key activities which may be relevant to you are the provision by way of business, in one of the following ways:

- advice about the tax affairs of another person by a firm or sole practitioner
- legal or notarial services by a firm or sole practitioner 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 5, 6, and 8 of this practice note provide more details on your obligations under POCA.

1.4.4 Terrorism Act 2000

Scope

The Terrorism Act 2000, as amended, establishes several offences about engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. It establishes a list of proscribed organisations the Secretary of State believes are 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 7

Application

The Terrorism Act applies to all persons. There is also 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, changing the definition of the regulated sector to bring it into line with the Money Laundering Regulations 2007.

Chapters 7 and 8 provide more detail on your obligations under the Terrorism Act.

1.4.5 The Money Laundering Regulations 2007

Scope

The Money Laundering Regulations 2007 repeal and replace the Money Laundering Regulations 2003 and implement the third directive. They set administrative requirements for the anti-money laundering regime within the regulated sector and outline the scope of customer due diligence.

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

Copy of the regulations

Application

Regulation 3 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 includes a firm or a sole practitioner who by way of business provides legal or notarial services to other persons. It does not include solicitors employed by a public authority or working in-house.

The regulations only apply to certain solicitors' activities where there is a high risk of money laundering occurring. As such, they apply when solicitors participate 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 or similar structures

You will 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.

Activities covered by the regulations

In terms of the activities covered, note that:

- managing client money is narrower than handling it
- opening or managing a bank account is wider than simply opening a solicitor's client account. It would be likely to cover solicitors acting as a trustee, attorney or a receiver

Activities not covered by the regulations

The Treasury has confirmed that the following would not generally be viewed as participation in financial transactions:

- preparing a home information pack or any document or information for inclusion in a HIP - it is specifically excluded under Regulation 4(1)(f)

- payment on account of costs to a solicitor or payment of a solicitor'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, seek legal advice on the individual circumstances of your practice or simply take the broadest of the possible approaches 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. You must also consider the full range of related services, such as tax planning and tax compliance work.

You will also need to consider whether your firm undertakes activities falling within the definition of financial institution, particularly with respect to the list of operations covered by the banking consolidation directive, as contained in schedule 1 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 FSA, this may affect your supervision under these regulations. You should contact the SRA for advice on any supervisory arrangements that they may have in place with other supervisory authorities.

1.5 Status of this practice note

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

Practice notes are issued by the Law Society for the use and benefit of its members. They represent the Law Society's view of good practice that solicitors can follow. You are not required to follow them, but doing so will make it easier to account to oversight bodies for your actions.

Practice notes are not legal advice, nor do they necessarily provide a defence to complaints of misconduct or inadequate professional service.

However, the Solicitors Regulation Authority (SRA) has advised it will take into account whether a solicitor has complied with this practice note when undertaking its role as regulator of professional conduct, and as a supervisory authority for the purposes of the regulations. A solicitor may be asked by the SRA to justify a decision to deviate from it.

Some solicitors' firms are authorised and regulated by the FSA because they are involved in mainstream regulated activities, eg advising clients directly on investments such as stocks and shares. Those firms should also consider the Joint Money Laundering Steering Group's guidance.

We are seeking Treasury approval of this practice note, which, in accordance with regulation 45(2), will require the court to consider compliance with its contents 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 practice notes are accurate, up to date and useful, the Law Society will not accept any legal liability in relation to them.

1.6 Terminology in this practice note

Must – a specific requirement in the Solicitors' Code of Conduct or legislation. You must comply, unless there are specific exemptions or defences provided for in the code of conduct or relevant legislation.

Should – good practice for most situations in the Law Society's view. If you do not follow this, 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. Which option you choose is determined by the risk profile of the individual practice, client or retainer. You must be able to justify why this was an appropriate option to oversight bodies.

1.7 Other information and products

1.7.1 Law Society services

- Dedicated web page www.lawsociety.org.uk/moneylaundering.
- Practice Advice Service
<http://www.lawsociety.org.uk/productsandservices/services/practiceadvice.law>
- AML Directory
<http://www.lawsociety.org.uk/choosingandusing/findasolicitor/moneylaunderingdirectory.page>
- Regional training on AML compliance

- AML e-newsletters
- Regional MLRO networking groups
- Lexcel - our practice management standard, awarded only to practices meeting the highest management and client care standards
- Other Law Society publications – order from the book shop
 - *Solicitors and Money Laundering Handbook – 3rd edition*

1.7.2 Other

- the Solicitors Regulation Authority's Professional Ethics Helpline for advice on conduct issues
- Serious Organised Crime Agency <http://www.soca.gov.uk/>
- Joint Money Laundering Steering Group
<http://www.jmlsg.org.uk/bba/jsp/polopoly.jsp?d=749>
- HM Treasury http://www.hm-treasury.gov.uk/fin_money_index.htm

1.8 Acknowledgements

Many have had input into the preparation of this practice note. The members of the Money Laundering Task Force and others mentioned below deserve particular acknowledgement for both the time and energy they have committed to the development of the guidance.

Task force

Robin Booth	BCL Burton Copeland
Alison Matthews	Irwin Mitchell
Christopher Murray	Kingsley Napley
Peter Burrell	Herbert Smith
Stephen Gentle	Kingsley Napley
Nicola Boulton	Byrne and Partners
Louise Delahunty	Simmons and Simmons
Nick Cray	Lovells
Peter Rodd	Boys and Maugham
Chris McNeil	Freshfields Bruckhaus Deringer

Law Society staff

Che Odlum	Policy Adviser
Emma Oettinger	Policy Adviser
James Richards	E-communications Manager

Others

Richard Bark-Jones	Morecrofts
Daren Allen	DLA Piper
Sarah de Gay	Slaughter and May
Clive Cutbill	Withers
Johanna Waritay	Clifford Chance
Suzie Ogilvey	Linklaters
Elizabeth Richards	SRA

The Law Society would also like to specifically thank the following people for the generous provision of their time and expertise in assisting the Law Society with its campaign to ensure that the requirements regarding identification of beneficial owners were sufficiently clear and workable:

Richard Bark-Jones	Morecrofts
Toby Graham	Farrer & Co
Rabinder Singh QC	Matrix Chambers
Alex Balin	Matrix Chambers
Michael Furness QC	Wilberforce Chambers
Nicholas Le Poidevin	Lincolns Inn
Nicholas Green QC	Brick Court Chambers
Martyn Frost	STEP
Keith Johnston	STEP
Jacob Rigg	STEP

Chapter 2 – the risk-based approach

2.1 General comments

The possibility of being used to assist with money laundering and terrorist financing poses many risks for your firm, including:

- criminal and disciplinary sanctions for firms and individual solicitors
- civil action against the firm as a whole and individual partners
- 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 firm. If you know your client well and understand your instructions thoroughly, you will be better placed to assess risks and spot suspicious activities. Applying the risk-based approach will vary between firms. While you can, and should, start from the premise that most of your clients are not launderers or terrorist financiers, you must assess the risk level particular to your firm and implement reasonable and considered controls to minimise those risks.

No matter how thorough your risk assessment or how appropriate your controls, some criminals may still succeed in exploiting you for criminal purposes. But an effective, risk-based approach and documented, risk-based judgements on individual clients and retainers will enable your firm to justify your position on managing the risk to law enforcement, courts and professional supervisors (oversight bodies).

The risk-based approach 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

2.2 Application

The Money Laundering Regulations 2007 permit a risk-based approach to compliance with customer due diligence obligations.

This 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. [See chapters 5 and 7] The risk-based approach still applies to ongoing monitoring of clients and retainers which enables you to identify suspicions.

2.3 Assessing your firm's risk profile

This depends on your firm's size, type of clients, and the practice areas it engages in.

You should consider the following factors:

2.3.1 Client demographic

Your client demographic can affect the risk of money laundering or terrorist financing. Factors which may vary the risk level include whether you:

- have a high turnover of clients or a stable existing client base
- act for politically exposed persons (PEPs)
- act for clients without meeting them
- practice in locations with high levels of acquisitive crime or for clients who have convictions for acquisitive crimes, which increases the likelihood the client may possess criminal property
- act for clients affiliated to countries with high levels of corruption or where terrorist organisations operate
- act for entities that have a complex ownership structure
- are easily able to obtain details of beneficial owners of your client or not

2.3.2 Services and areas of law

Some services and areas of law could provide opportunities to facilitate money laundering or terrorist financing. For example:

- complicated financial or property transactions
- providing assistance in setting up trusts or company structures, which could be used to obscure ownership of property
- payments that are made to or received from third parties
- payments made by cash
- transactions with a cross-border element

Simply because a client or a retainer falls within a risk category does not mean that money laundering or terrorist financing is occurring. You need to ensure your internal controls are designed to address the identified risks and take appropriate steps to minimise and deal with these risks. Read examples of possible internal controls.

Chapter 11 provides more information on warning signs to be alert to when assessing risk.

2.4 Assessing individual risk

Determining the risks posed by a specific client or retainer will then assist in applying internal controls in a proportionate and effective manner.

You may consider whether:

- your client is within a high risk category
- you can be easily satisfied the CDD material for your client is reliable and allows you to identify the client and verify that identity
- you can be satisfied you understand their control and ownership structure
- the retainer involves an area of law at higher risk of laundering or terrorist financing
- your client wants you to handle funds without an underlying transaction, contrary to the Solicitors' Account Rules
- there are any aspects of the particular retainer which would increase or decrease the risks

This assessment helps you 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 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 firm generally and for each client, business relationship and retainer. In a solicitor's practice it is the overall information held by the firm gathered while acting for the client that will inform the risk assessment process, rather than sophisticated computer data analysis systems. The more 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 and procedures

3.1 General comments

Develop systems to meet your obligations and risk profile in a risk-based and proportionate manner. Policies and procedures supporting these systems mean that staff apply the systems consistently and firms can demonstrate to oversight bodies that processes facilitating compliance are in place.

3.2 Application

Regulation 20 of the Money Laundering Regulations 2007 requires the regulated sector to have certain systems in place. If you are in the regulated sector, failing to have those systems is an offence, punishable by a fine or up to two years' imprisonment. You must demonstrate your compliance to the SRA, as supervisor under the regulations.

If you are outside the regulated sector, you should still consider how these systems can assist you to comply with your obligations to report suspicious transactions in accordance with POCA and the Terrorism Act.

3.3 Nominated officers

3.3.1 Why have a nominated officer?

Regulation 20(2)(d)(i) requires that all firms 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 SOCA.

Regulation 20(3) 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.

Firms who do not provide services within the regulated sector should consider appointing a nominated officer, even though it is not required, because POCA and the Terrorism Act still apply. The Solicitors' Code of Conduct 2007 requires business management systems facilitating compliance with legal obligations.

3.3.2 Who should be a nominated officer?

Your nominated officer should be of sufficient seniority to make decisions on reporting which can impact your firm'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

firm's client files and business information to enable them to make the required decisions on the basis of all information held by the firm.

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

3.3.3 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 SOCA or law enforcement on the issue of whether to proceed with a transaction or what information may be disclosed to clients or third parties.

The size and nature of some firms may lead to the nominated officer delegating certain duties regarding the firm's AML/CTF obligations. In some large firms, one or more permanent deputies of suitable seniority may be appointed. All firms will need to consider arrangements for temporary cover when the nominated officer is absent.

3.4 Risk assessment

You can extend your existing risk management systems to address AML and CTF risks. The detail and sophistication of these systems will depend on your firm's size and the complexity of the business it undertakes. Ways of incorporating your risk assessment of clients, business relationships and transactions into the overall risk assessment will be governed by the size of your firm and how regularly compliance staff and senior management are involved in day-to-day activities.

Issues which may be covered in a risk assessment system include:

- the firm's current risk profile
- how AML/CTF risks will be assessed, and processes for re-assessment and updating of the firm's risk profile
- internal controls to be implemented to mitigate the risks
- which firm personnel have authority to make risk-based decisions on compliance on individual files
- how compliance will be monitored and effectiveness of internal controls will be reviewed

3.5 Internal controls and monitoring compliance

The level of internal controls and extent to which monitoring needs to take place will be affected by:

- your firm's size
- the nature, scale and complexity of its practice
- its overall risk profile

Issues which may be covered in an internal controls system include:

- the level of personnel permitted to exercise discretion on the risk-based application of the regulations, and under what circumstances
- 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

Monitoring compliance will assist you to assess whether the policies and procedures you have implemented are effective in forestalling money laundering and terrorist financing opportunities within your firm. Issues which may be covered in a compliance system include:

- 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
- reports to be provided from the nominated officer to senior management on compliance
- how to rectify lack of compliance, when identified
- how lessons learnt will be communicated back to staff and fed back into the risk profile of the firm

3.6 Customer due diligence

You are required to have a system outlining the CDD measures to be applied to specific clients. You should consider recording your firm's risk tolerances to be able to demonstrate to your supervisor that your CDD measures are appropriate.

Your CDD system may include:

- when CDD is to be undertaken
- information to be recorded on client identity

- 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
- when simplified due diligence may occur
- what steps need to be taken for enhanced due diligence
- what steps need to be taken to ascertain whether your client is a PEP
- when CDD needs to occur and under what circumstances delayed CDD is permitted
- how to conduct CDD on existing clients
- what ongoing monitoring is required

For suggested methods on how to conduct CDD see Chapter 4 of this practice note.

3.7 Disclosures

Firms, but not sole practitioners who have no other staff, need to 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 SOCA
- how to manage a client when a disclosure is made while waiting for consent
- the need to be alert to tipping off issues

For details on when a disclosure needs to be made see chapters 5, 6 and 7 of this practice note. For details on how to make a disclosure see chapter 8 of this practice note.

3.8 Record keeping

Various records must be kept to comply with the regulations and defend any allegations against the firm in relation to money laundering and failure to report offences. A firm's records system must outline what records are to be kept, the form in which they should be kept and how long they should be kept.

Regulation 19 requires that firms 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.

3.8.1 CDD material

You may keep either a copy of verification material, or references to it. Keep it for five years after the business relationship ends or the occasional transaction is completed. Consider holding CDD material separately from the client file for each retainer, as it may be needed by different practice groups in your firm.

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

- scan the verification 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 17 for the completion of CDD measures, you must keep the relevant documents for five years from the date on which you were relied upon.

3.8.2 Risk assessment notes

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 firms 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.

Firms may choose standard categories of comment to apply to notes.

3.8.3 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 the transaction is completed.

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

3.8.4 Suspensions and disclosures

It is recommended that you 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 SOCA, law enforcement, insurers, supervisory authorities etc regarding disclosures made
- decisions not to make a report to SOCA which may be important for the nominated officer to justify his position to law enforcement

You should ensure 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.

3.8.5 Data protection

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

Section 29 of the Data Protection Act 1998 states 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 firm.

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

HM Treasury guidance (PDF, 28kb)
Information Commissioner guidance (PDF, 73kb)

Note the definition of personal data.

3.9 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 firm.

Regulation 20 requires that you communicate your AML/CTF obligations to your staff, while regulation 21 requires that you give staff appropriate training on their legal obligations and information on how to recognise and deal with money laundering and terrorist financing risks.

Rule 5 of the Solicitors' Code of Conduct also requires you to train your staff to a level appropriate to their work and level of responsibility.

3.9.1 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 firm vulnerable to sanctions under the regulations for failing to properly train your staff.

3.9.2 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 firm

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
- firm 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.

3.9.3 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 firm'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

Some type of training for all relevant staff every two years is preferable.

3.9.4 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

4.1 General comments

Customer due diligence (CDD) is required by the Money Laundering Regulations 2007 because you can better identify suspicious transactions if you know your customer and understand the reasoning behind the instructions they give you.

4.2 Application

You must conduct CDD on those clients who retain you for services regulated under the regulations (see Chapter 1). Rule 2 of the Solicitors' Code of Conduct is also relevant to all solicitors.

4.3 CDD in general

4.3.1 When is CDD required?

Regulation 7 requires that you conduct CDD when:

- establishing a business relationship
- carrying out an occasional transaction
- you suspect money laundering or terrorist financing
- you doubt the veracity or adequacy of documents, data or information previously obtained for the purpose of CDD

The distinction between occasional transactions and long-lasting business relationships is relevant to the timing of CDD and the storage of records.

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, firms 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.

Existing business relationships before 15 December 2007

You must apply CDD measures at appropriate times to existing clients on a risk-sensitive basis. You are not required to apply CDD measures to all existing clients immediately after 15 December 2007. Where you have verified a client's identity to a previously applicable standard then, unless circumstances indicate the contrary, the risk is likely to be low. If you have existing high risk clients that you have previously

identified you may consider applying the new CDD standard sooner than for low risk clients. Read more.

4.3.2 What is CDD?

Regulation 5 says that CDD comprises:

- identifying the client and verifying their identity on the basis of documents, data or information obtained from a reliable and independent source
- identifying, where there is a beneficial owner who is not the client, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that you are satisfied that you know who the beneficial owner is. This includes understanding the ownership and control structure of a legal person, trust or similar arrangement.
- obtaining information on the purpose and intended nature of the business relationship

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 7(3) provides that you must:

- determine the required extent of customer due diligence measures on a risk-sensitive basis depending on the type of client, business relationship, product or transaction
- be able to demonstrate to your supervisory authority that you took appropriate measures in view of the risks of money laundering and terrorist financing

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.

You need only obtain information on the purpose and intended nature of your client's use of your services when you are in a business relationship with them. However, it's good practice and required by Rule 2 of the Solicitors' Code of Conduct to obtain such information to ensure you fully understand instructions and closely monitor the development of each retainer, even if it is for an occasional transaction or transactions below the threshold.

4.3.3 Methods of verification

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

- obtaining or viewing original documents
- conducting electronic verification
- obtaining information from other regulated persons

Independent source

You need an independent and reliable verification of your client's identity. 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. Often 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.

Documents

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

Electronic verification

This will only confirm 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 we believe electronic verification can be a sufficient measure for compliance with money laundering requirements, there may be circumstances where it will not be appropriate. For example, the Council for Mortgage Lenders notes that electronic verification products may not be suitable for fraud prevention purposes, such as verifying that a person's signature is genuine.

4.3.4 Reliance and outsourcing

Reliance has a very specific meaning within the regulations and relates to the process under Regulation 17 where you rely on another regulated person to conduct CDD for you. You remain liable for any failure in the client being appropriately identified. Reliance does not include:

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

You need

- the consent of the person on whom you rely for your reliance
- agreement that they will provide you with the CDD material upon request
- the identity of their supervisor for money laundering purposes. Consider checking the register of members for that supervisor, although a personal assurance of their identity may be sufficient where you have reasonable grounds to believe them.

We believe you should ask what CDD enquiries have been undertaken to ensure that they actually comply with the regulations, because you remain liable for non-compliance. This is particularly important when relying on a person outside the UK, and you should be satisfied that the CDD has been conducted to a standard compatible with the third directive (PDF, 302kb), taking into account the ability to use different sources of verification and jurisdictional specific factors. It may not always be appropriate to rely on another person to undertake your CDD checks and you should consider reliance as a risk in itself.

Reliance in the UK

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

- a credit or financial institution which is an authorised person
- a person in the following professions who is supervised by a supervisory authority listed in Part 1 of Schedule 3 of the regulations:
 - auditor
 - insolvency practitioner
 - external accountant
 - tax adviser
 - independent legal professional

Reliance in an EEA state

You can only rely on the following persons in an EEA state:

- a credit or financial institution
- auditor, or EEA equivalent
- insolvency practitioner, or EEA equivalent
- external accountant
- tax adviser
- independent legal professional

if they are both:

- subject to mandatory professional registration recognised by law, and
- supervised for complying with money laundering obligations under Chapter 5, Section 2 of the third directive (PDF, 302kb).

A person will only be supervised in accordance with the third directive if the third directive has been implemented in the EEA state. You can check on the International Bar Association's website on the progress of implementation across Europe.

Reliance in other countries

You can rely on the following persons outside of the EEA:

- a credit or financial institution, or equivalent
- an auditor, or equivalent
- an insolvency practitioner, or equivalent
- an external accountant
- a tax adviser or
- an independent legal professional.

The must also satisfy all of the following conditions:

- subject to mandatory professional registration recognised by law
- subject to requirements equivalent to those laid down in the third directive

- supervised for complying with money laundering obligations to a standard equivalent to that under Chapter 5, Section 2 of the third directive (PDF, 302kb)

HM Treasury has released a list of countries that the UK government accepts have anti-money laundering requirements equivalent to the money laundering directive.

- Consult the HM Treasury list. www.hm-treasury.gov.uk/4772.htm
- Consult the JMLSG's guidance on equivalence.
<http://www.jmlsg.org.uk/bba/jsp/polopoly.jsp?d=770&a=14398>
- Consult a list of national money laundering legislation around the world, and whether it applies to lawyers.

Passporting clients between jurisdictions

Many firms 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 firms 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 third directive. 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 firms may wish to rely on their international office to simply provide a letter of confirmation that CDD requirements have been undertaken with respect to the client. This will amount to reliance only if the firm can be relied upon under the terms of Regulation 17 and the CDD is completed in accordance with that regulation.

Finally, firms 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.

It is important to remember that one of your international offices may be acting for a client who is not a PEP in that country, but will be when they are utilising the services of your office. As such, 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.

4.3.5 Timing

When must CDD be undertaken?

Regulation 9 requires you to verify your client's identity and that of any beneficial owner, before you establish a business relationship or carry out an occasional transaction.

Regulation 11 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 an occasional transaction

You must also:

- terminate any existing business relationship
- consider making a disclosure to SOCA

Evidence of identity is not required if a one-off transaction involves less than €15,000 or if two or more linked transactions involve less than €15,000 in total. This exception does not apply if there is any suspicion of money laundering or terrorist financing.

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 SOCA.

Normal conduct of business

Regulation 9(3) provides that verification may be completed during the establishment of a business relationship, (not an occasional transaction), where:

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

You must complete verification as soon as practicable after the initial contact.

Consider your risk profile when assessing which work can be undertaken on a retainer prior to verification being completed.

Do not permit funds or 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 11 will apply.

Ascertaining legal position

Regulation 11(2) provides that the prohibition in 11(1) does not apply where:

'A lawyer or other professional adviser is in the course of ascertaining the legal position for their client or performing their task of defending or representing their client in, or concerning legal proceedings, including advice on instituting or avoiding proceedings.'

The requirement to cease acting and consider making a report to SOCA 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.

4.4 Ongoing monitoring

Regulation 8 requires that you conduct ongoing monitoring of a business relationship on a risk-sensitive and appropriate basis. 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.
- keeping the documents, data 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.

You are not required to:

- conduct the whole CDD process again every few years
- conduct random audits of files
- suspend or terminate a business relationship until you have updated data, information or documents, as long as you are still satisfied you know who your client is, and keep under review any request for further verification material or processes to get that material
- use sophisticated computer analysis packages to review each new retainer for anomalies

Ongoing monitoring will normally be conducted by fee earners handling the retainer, and involves staying alert to suspicious circumstances which may suggest money laundering, terrorist financing, or the provision of false CDD material.

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 SOCA with your nominated officer.

To ensure that CDD material is kept up-to-date, you should consider reviewing it:

- when taking new instructions from a client, particularly if there has been a gap of over three years between instructions
- when you receive information of a change in identity details

Relevant issues may include:

- the risk profile of the client and the specific retainer
- whether you hold material on transactional files which would confirm changes in identity
- whether electronic verification may help you find out if your clients' identity details have changed, or to verify any changes

4.5 Records

You are required to keep records of your CDD material.

4.6 CDD on clients

Your firm will need to make its own assessments 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.

4.6.1 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.

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 firm 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 considered 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, 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
- 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 from the DWP 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
- solicitor'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 firm 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.

Where you do not meet the client, the Regulations state that you must undertake enhanced due diligence measures.

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.

Where 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, 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, eg one produced and maintained by their professional body, and you can either translate the information, or understand it already.

4.6.2 Partnerships, limited partnerships and UK LLPs

A partnership 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 firm'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 firm's trading address.

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

4.6.3 Companies

A company is a legal entity in its own right, but conducts its business through representatives. So you must identify and verify the existence of the company. You should consider whether the person instructing you on behalf of the company has the authority to do so

A company's identity comprises its constitution, its business and its legal ownership structure. The key identification particulars are the company's name and its business address, although the registration number and names of directors may also be relevant identification particulars.

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 2007 regulations.

You will also need to consider the identity of beneficial owners where simplified diligence does not apply.

Public companies listed in the UK

Where a company is either:

- listed and its securities are admitted to trading on a regulated market, or
- a majority-owned and consolidated subsidiary of such a company

simplified due diligence applies.

For a listed company, this evidence may simply be 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

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 (ie 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: www.companieshouse.gov.uk)
- 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.

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.

The standard identifiers for private companies are:

- full name
- business / registered address
- names of two directors, or equivalent
- nature of business

Other 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, including the director's address
- filed audited accounts
- information from a reputable electronic verification service provider

Public overseas companies

Simplified due diligence applies when:

- a company or its subsidiary is listed on a regulated market subject to specified disclosure obligations

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 directive [2003/6/EC]

If a regulated market is located within the EEA, 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.

HM Treasury have released a list of countries that the UK government accepts have anti-money laundering requirements equivalent to the money laundering directive.

- Consult the HM Treasury list. www.hm-treasury.gov.uk/4772.htm
- Consult the JMLSG's guidance on equivalence.
<http://www.jmlsg.org.uk/bba/jsp/polopoly.jsp?d=770&a=14398>
- Consult a list of regulated markets within the EU

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.

4.6.4 Other arrangements or bodies

Trusts

A trust is not a separate legal entity. Your client may be the settlor, the trustee(s) or occasionally the beneficiaries.

UK common law trusts are used extensively in everyday situations and often pose limited risk. They can become more risky if:

- the client requests a trust be used when there seems to be little reason to do so
- the trust is established in a jurisdiction which has limited AML/CTF regulation

In a higher risk situation you should consider either conducting further CDD or enhanced monitoring. This could include:

- conducting CDD on all the trustees, or on the settlor even after the creation of the trust
- asking about the purpose of the trust and the source of the funds used to create it
- obtaining the trust deed or searching an appropriate register maintained in the country of establishment

Your client, whether they are the trustee(s), settlor or beneficiaries, must be identified in accordance with their relevant category, (ie natural person, company etc). Where you are acting for more than one trustee it is preferable that you verify the identity of at least two of the trustees. Where the trustee is another regulated person, you may rely on their listing with their supervisory body.

You must consider beneficial ownership issues where you are acting for the trustee(s).

Foundations

A foundation is the civil law equivalent to a common law trust and operates in many EEA countries. You should understand why your client is using a solicitor outside of the jurisdiction of establishment, and the statutory requirements for the establishment of the foundation. Then obtain similar information as you would for a trust.

Where the foundation's founder is anonymous, you may consider whether any intermediary or agent is regulated for AML/CTF and whether they can provide assurances that verify the identity of relevant persons involved with the foundation.

Foundations can also be a loose term for charitable institutions in the UK and the USA – where that is the case they must be verified in accordance with the procedures for verifying charities set out below.

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 at www.charity-commission.gov.uk
- the Office of the Scottish Charity Regulator at www.oscr.org.uk

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. Currently in Northern Ireland there is no regulator for charities.

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 the 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.

During the administration of the estate, Regulation 6(8) provides that the beneficial owner is:

- the executor, original or by representation, or
- the administrator for the time being of a deceased person

This definition is wide enough to cover you when you deal with foreign deceased estates that are in the course 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 and Skills maintains lists of approved educational facilities 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 constitutions
- 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 13 (7)(c) provides that simplified due diligence is permitted where:

'A pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by an employer or 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 (other than an assignment permitted by section 44 of the Welfare Reform and Pensions Act 1999 (disapplication of restrictions on alienation) or section 91(5)(a) of the Pensions Act 1995 (inalienability of occupational pension)).'

So you only 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.

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 Joint Money Laundering Steering Group's guidance.

4.6.5 Government agencies and councils

The money laundering and terrorist financing risks associated with public authorities varies 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

Simplified due diligence applies to UK public authorities and to some non-UK public authorities. See 4.8.2. Where simplified due diligence does not apply, you may get information verifying the existence of the public sector from:

- official government websites
- a listing in a national or local telephone directory

4.7 CDD on a beneficial owner

4.7.1 General comments

When conducting CDD on a client, you will need to identify any beneficial owners within the meaning of regulation 6 of the Regulations. 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.

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

4.7.2 Assessing the risk

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

- why your client is acting on behalf of someone else
- 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

Only in rare cases will you need to verify a beneficial owner to the same level that you would a client.

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(b)
- 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.

4.7.3 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 or activity is being conducted.

In these cases, it is presumed the client is himself the beneficial owner, unless the features of the transaction indicate 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.

- 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.

4.7.4 Companies

Regulation 6(1) defines the beneficial owner of a body corporate as meaning:

Any individual who:

- as respects any body other than a company whose securities are listed on a regulated market, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25 per cent of the shares or voting rights in the body, or
- as respects any body corporate, otherwise exercises control over the management of the body

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

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 if, 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 only 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 laundering risk 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.

4.7.5 Partnerships

Regulation 6(2) 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 this Regulation:

- 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

4.7.6 Trusts

Regulation 6(3) sets out three types of beneficial owners of a trust:

- Part A: individual with specified interest – those with at least a 25 per cent specified interest in trust capital
- Part B: class of persons to benefit – those in whose main interest the trust operates
- Part C: individuals who control a trust

You must identify persons within all relevant categories.

Non-individual beneficiaries

While generally the beneficiaries of a trust will be individuals, they may at times be a company, an entity or an arrangement, such as a charity.

Regulation 6(5) says you will have to apply Regulation 6(1) to a beneficiary company to determine their beneficial owners. This means that:

You should consider for all companies whether anyone exercises control over the beneficiary company outside of the normal management structures. Identify them as a beneficial owner of the client trust. You may ask the client if they are aware of any such person, as this information would not be on a publicly available register and it will generally not be proportionate for you to have direct dealings with the beneficiary company.

- Where the beneficiary company is a private or unlisted company, you should consider whether they have shareholders with more than a 25 per cent interest in the beneficiary company. This can be done by a simple search on Companies House or equivalent online registry.

- If you locate such a shareholder, you should note their identity as a beneficial owner of the client trust. You will have already verified the identity through the company register check. Where there is a tiered structure, eg where, through its shareholding in a such shareholder, another company has more than a 25 per cent interest in the beneficiary company enquire of the client why there is a tiered structure in use and make a risk-based decision, considering the risk of the client generally and the whole retainer, as to whether:
 - further identity enquiries are required
 - you simply identify the second company as the beneficial owner of the client trust and then conduct closer monitoring of any transactions
 - you have a suspicion warranting a disclosure to SOCA, and consider withdrawing from the retainer

The further you look for beneficial owners within beneficial owners the smaller the interest and the harder it is to exercise control. Therefore the risk of laundering or terrorist financing is lower. Consider this when setting proportionate CDD.

If you do not find an individual within either of the above categories, then simply list the beneficiary company as the beneficial owner of the client trust.

Regulation 6(5)(a) does not apply to beneficiaries that are non-corporate entities or another trust. You should still identify them as a beneficial owner of the client trust and consider whether you need to know more about them.

Individual with specified interest (Part A)

A person has a specified interest if they have a vested interest of the requisite level in possession or remainder or reversion, defeasible or indefeasible.

Vested interest

This is an interest not subject to any conditions precedent. It is held by the beneficiary completely and inalienably, even if it is still under the control of the trustees at that time.

Contingent interest

This interest is subject to the satisfaction of one or more conditions precedent, such as attaining a specified age or surviving a specified person. Failure to satisfy all conditions precedent results in the failure of the interest.

Interest in possession

This interest is the right to enjoy the use or possession of the fund and under the regulations relates solely to an interest in the capital of the fund.

Interest in remainder

This is the beneficiary's right to the capital of the fund which is postponed to one or more prior interests in possession in the income of the fund.

Interest in reversion

This is the right of the settlor to receive any part of the fund at the end of the trust. It occurs in cases including when the trust fails because all of the beneficiaries die or a life interest terminates and there are no remainder beneficiaries.

Defeasible interest

An interest is defeasible if it can be terminated in whole or in part, without the consent of the beneficiary, by the happening of an event, such as the failure of a condition subsequent or the exercise by the trustees of a power to terminate or vary the interest.

Indefeasible interest

An interest is indefeasible if it cannot be terminated in whole or in part without the consent of the beneficiary by the happening of any event.

Defeasible and indefeasible interests are included, so that you consider the beneficiaries who are going to get the property as at the time you are instructed, and conduct CDD on them.

Class of persons to benefit (Part B)

Part B of the definition in Regulation 6(3) covers any trust that includes persons who do not fit within Part A. Within Part B, you must identify the class of persons in whose main interest the trust operates. All discretionary trusts will fall within Part B.

Note: If a trust has one or more persons who are individuals with a 25 per cent specified interest, as well as other beneficiaries, identify the individuals who fit within the first part of the definition, then consider the rest of the beneficiaries as a class under Part B.

Identification of a class is by description, such as:

- the grandchildren of X
- charity Y
- pension holders and their dependents

When considering 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.

Where in doubt about which class has the main interest, you should identify all classes.

Note: Interests in parts of the trust property can change significantly between retainers, particularly with discretionary trusts. So it is good practice to obtain an update on any changes from the trustees with each set of new retainers your firm receives in relation to a discretionary trust.

Control of the trust (Part C)

Control is defined as a power, either:

- exercisable alone
- jointly with another person
- with the consent of another person

under the trust instrument or by law to either:

- dispose of, advance, lend, invest, pay or apply trust property
- vary the trusts
- add or remove a person as a beneficiary or to a class of beneficiaries
- appoint or remove trustees
- direct, withhold consent to or veto the exercise of a power such as is mentioned in the options above

The definition of control can include beneficiaries acting collectively where they have the power to take or to direct action.

Regulation 6(5)(b) specifically excludes from the definition of control:

- the power exercisable collectively at common law to vary or extinguish a trust by all of the beneficiaries – see *Saunders v Vautier* [1841] EWHC Ch J82 .
- the power of members of a pension fund to influence the investment of the fund's assets
- the power to consent to advancement implied to a person with a life interest under section 32(1)(c) of the Trustee Act 1925
- the powers of beneficiaries to require the appointment or retirement of trustees under Trusts of Land and Appointment of Trustees Act 1996

.

Identifying trust beneficial owners in practice

You are only required to make reasonable and proportionate enquiries to establish whether beneficial owners exist and, where relevant, verify their identity. If unsure whether a beneficiary or other person is a beneficial owner, you may consider taking

legal advice from a trust practitioner, or identify them and consider whether verification is required.

Enquires and verification may be undertaken by:

- getting assurances from trustees on the existence and identity of beneficial owners
- getting assurances from other regulated persons more closely involved with the client, particularly in other jurisdictions, on existence and identity of beneficial owners
- reviewing the trust deed
- obtaining information from a reputable electronic verification service on details of identified beneficiaries.

View practical examples of how various interests and powers of control may appear

4.7.7 Other arrangements and legal entities

Regulation 6(6) 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:

- where the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from at least 25 per cent of 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 at least 25 per cent of 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 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

4.8 Simplified due diligence

Regulation 13 permits simplified due diligence to be undertaken in certain circumstances.

4.8.1 What is simplified due diligence?

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

4.8.2 Who qualifies for simplified due diligence?

The following clients and products qualify:

- a credit or financial institution which is subject to the requirements of the money laundering directive (PDF, 309kb)
- a credit or financial institution in a non-EEA state which is supervised for compliance with requirements equivalent to the money laundering directive (PDF, 309kb)
- companies listed on a regulated EEA state market or a non-EEA market which are subject to disclosure obligations specified in regulation 2
- beneficial owners of pooled accounts held by a notary or independent legal professional, ie financial services firms are not required to apply CDD to the third party beneficial owners of omnibus accounts held by solicitors, provided the information on the identity of the beneficial owners is available upon request

- UK public authorities
- a non-UK public authority which:
 - is entrusted with public functions pursuant to the treaty on the European Union or the Treaties on the European Communities, or Community secondary legislation
 - has a publicly available, transparent and certain identity
 - has activities and accounting practices which are transparent
 - is accountable to a community institution, the authorities of an EEA state or is otherwise subject to appropriate check and balance procedures
- certain insurance policies, pensions or electronic money products
- products where:
 - they are based on a written contract
 - related transactions are carried out through a credit institution which is regulated under the money laundering directive or subject to equivalent requirements
 - they are not anonymous
 - they are within relevant maximum thresholds
 - realisation for the benefit of a third party is limited
 - investment in assets or claims is only realisable in the long term, cannot be used as collateral and there cannot be accelerated payments, surrender clauses or early termination

For further details on the requirements for qualification for simplified due diligence, see Regulation 13 and Schedule 2 of the regulations.

HM Treasury have released a list of countries that the UK government accepts have anti-money laundering requirements equivalent to the money laundering directive.

- Consult the treasury list. www.hm-treasury.gov.uk/4772.htm
- Consult the JMLSG's guidance on equivalence.
<http://www.jmlsg.org.uk/bba/jsp/polopoly.jsp?d=770&a=14398>
- Consult a list of national money laundering legislation around the world, and whether they apply to lawyers

4.9 Enhanced due diligence

Regulation 14 provides that you will need to apply enhanced due diligence on a risk-sensitive basis where:

- the client is not dealt with face-to-face
- the client is a politically exposed person (PEP)
- there is any other situation which can present a higher risk of money laundering or terrorist financing

The regulations do not set out what will be enhanced due diligence for the last option.

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
- obtain more detail on the ownership and control structure of the client
- request further information on the purpose of the retainer or the source of the funds, and/or
- conduct enhanced ongoing monitoring

4.9.1 Non face-to-face clients

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. The mere fact that you do not have face-to-face meetings with the agents of an entity or arrangement does not automatically require that enhanced due diligence is undertaken. You should consider 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.

Where a client is a natural person and they are not physically present for identification purposes, you must undertake enhanced due diligence.

Regulation 14 (2) outlines possible steps which can be taken above standard verification procedures to compensate for the higher risk of non face-to-face transactions. The regulations suggest the following options, although this list is not exhaustive:

- using additional documents, data or information to establish identity. This may involve using electronic verification to confirm documents provided, or using two or three documents from different sources to confirm the information set out in each.
- using supplementary measures to verify or certify the documents supplied or obtain confirmatory certification by a credit or financial institution which is subject to the money laundering directive. You may consider electronic verification to confirm the documents provided. Alternatively consider getting certified copies of documents:

When dealing with foreign passports or identity cards, check the requirements for that country with the relevant embassy or consulate.

With all other documents, consider whether the certifying person is regulated with respect to the regulations or is otherwise a professional person subject to some sort of regulation or fit and proper person test, who can easily be independently contacted to verify their certification of the documents. Such persons include bank managers, accountants, or local GPs. You may also consider accepting documents certified by the Post Office-provided Identity Checking Service.

ensuring the first payment in the retainer is through an account opened in the client's name with a credit institution. EU regulation 1781/2006 says credit institutions must provide the payers name, address and account number with all electronic fund transfers. It entered force on 1 January 2007 and is directly applicable to all member states. Use this to further verify your client's identity.

Further details: Part II – Wire transfers of the JMLSG guidance

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 FSA, if the institution refuses to give you written confirmation of the details. Take other steps to verify your client's identity.

4.9.2 Politically exposed persons

You must take the following steps to deal with the heightened risk posed by having a client who is a PEP:

- have senior management approval for establishing a business relationship with 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 is a PEP, you should consider on a risk-based approach what extra measures, if any, you need to take when dealing with that client.

Further, merely doing work for a non-UK public authority does not mean that you are in a business relationship with a PEP. You should however ensure that you have considered the risks associated with the particular public authority and taken steps to address those risks.

Who is a PEP?

A person who has been entrusted within the last year with one of the following prominent public functions by a community institution, an international body, or a state other than the UK:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament
- members of supreme courts, of constitutional courts, or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances

- members of courts of auditors or of the boards of central banks
- ambassadors, charges d'affairs and high-ranking officers in the armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises

Middle ranking and junior officials are not PEPs.

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

- family members of a PEP – spouse, partner, children and 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

The regulations only apply to persons appointed by governments and authorities outside the UK, but it may be appropriate, on a risk-based approach to apply some or all of the enhanced due diligence requirements to a person appointed in the UK, who would have been a PEP had they been appointed outside the UK.

How to identify PEPs

You are not required to conduct extensive investigations to establish whether a person is a PEP. Just have regard to information that is in your possession or publicly known.

To assess your PEP risk profile, you should consider your existing client base, taking into account the general demographic of your client base, and how many clients you currently know would be 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 actually come to your attention suggesting your client is 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.

Senior management approval

The regulations do not define senior management, so your firm must decide who that is, on a risk-sensitive basis. 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
- 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 firm's risk profile and compliance.

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.

Enhanced monitoring

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

4.9.3 High risk of money laundering

Enhanced due diligence is also required where there is a higher risk of money laundering.

The Financial Action Taskforce and HM Treasury advised on 20 October 2007 that transactions involving the following jurisdictions are at higher risk of money laundering:

- Iran

- Uzbekistan

You must undertake enhanced due diligence and enhanced ongoing monitoring when acting in relation to transactions involving these jurisdictions.

4.10 Existing clients

Regulation 7(2) states you must apply CDD measures to an existing customer at other appropriate times and on a risk-sensitive basis, repealing the previous exemption for customers with whom you had a business relationship prior to 1 March 2004.

You do not have to ensure all existing clients have been identified and verified by 15 December 2007, nor update all current identification in accordance with the new requirements by that date.

Factors that may trigger a need for CDD include:

- a gap in retainers of three years or more
- a client instructing on a higher risk retainer
- where you develop a suspicion of money laundering or terrorist financing by the client
- an existing high risk client

For all clients, you should ensure ongoing monitoring of the business relationship to identify any suspicious activity.

When conducting CDD on existing clients or a subsidiary of an existing client, you may consider information already on your files which would verify their identity or publicly available information to confirm the information you hold, rather than approaching the client to provide that information initially. It may be appropriate for a fee earner or partner who has known the client for long time to place a certificate on the file providing an assurance as to identity.

4.11 FATF counter measures

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

- senior politically exposed persons from jurisdictions which are subject to sanctions

The 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 at: <http://www.hm-treasury.gov.uk/financialsanctions>.

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

4.11.1 FATF Counter measures

Where FATF issues counter measures against a country, the country is added to the non-cooperative countries and territories list [http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236992_1_1_1_1_1,00.html]. There are currently no countries listed as non-cooperative.

Regulation 18 states that when the client is from a country subject to FATF counter measures, HM Treasury may instruct you to avoid:

- entering into a business relationship
- carrying out an occasional transaction
- proceeding further with a business relationship or occasional transaction.

4.11.2 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.

4.11.3 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 7 of the practice note covers the relevant offences.

4.12 Annex A – Examples of beneficial ownership for a trust

4.12.1 Example 1

Details

A's will provides that after payment of legacies and testamentary expenses his residuary estate passes to his children in equal shares. Three children survive A, one of whom (B) is under 18.

Application

On A's death each of the children have a vested interest in one third of the residuary estate, notwithstanding that B will not receive his share until he is 18 as he cannot give a valid receipt to the executors, and none of them will be entitled to receive anything until the conclusion of the administration of the estate.

As such all three children should be identified under Part A, after the estate ceases to be in administration.

4.12.2 Example 2

Details

C executed an inter vivos trust in 2000 'for the benefit of my grandchildren who shall be born before 31/12/2020'. At the time he had two grandchildren. C died in 2006, and in 2007 your firm is instructed to act for the trustees. There are now four grandchildren.

Application

Each of the grandchildren has a vested interest in possession in one quarter of the trust fund, notwithstanding that further grandchildren may be born before 31/12/2020 and their shares may be reduced. Therefore each grandchild has a specified interest in at least 25 per cent of the capital of the trust property and should be identified under Part A.

¹ editing note – link to these orders – see TLS AML webpage and add the 2009 order http://www.opsi.gov.uk/si/si2009/ukSI_20091747_en_1

Development

In 2015 new trustees are appointed, at which point there are five grandchildren, each of whom has a specified interest in 20 per cent of the fund.

Application

Your firm will have to apply CDD to the new trustees (either as part of the client CDD or a person who has control) and to the class of beneficiaries under Part B, which will be the grandchildren of C.

4.12.3 Example 3

Details

C's will provides that after payment of legacies and testamentary expenses his residuary estate passes to 'such of my children as shall survive me and attain the age of 21 years'. Three children survive C, one of whom (D) is under 21.

Application

While the estate is in administration, it is the personal representative who will be the beneficial owner. The two elder children will have been paid out following completion of the administration of the estate, as they have absolute vested interests. D's interest in the one third of the estate is not a specified interest, being subject to a contingency and therefore not vested. As D also does not have control, this leaves you to apply CDD under Part B to the class of one, constituted by D.

4.12.4 Example 4

Details

E executes an inter vivos trust on 31/01/2007, creating a life interest in income for his wife, with remainder to such of their children as shall be living at his wife's death. At the time he has two children.

Application

The wife has a vested interest in possession, but it is in income, not in the capital of the trust. Therefore she is not a beneficial owner under Part A. As s32(1)(c) of the Trustee Act 1925 is excluded from being defined as control over the trust, she is not a beneficial owner under Part C either.

The children have an interest in the remainder, but it is contingent on them surviving their mother and does not vest until their mother's death. Therefore they should be identified as a class under Part B.

The settlor would be identified under Part A as he also has a vested interest in reversion as he has not provided for the situation which will arise if all of the children

pre-decease their mother. Should this happen there will be a total failure of the trust, which will revert to E, or if he has predeceased his wife, to his estate.

The trustees would also be identified under Part C as a result of their control over the trust

4.12.5 Example 5

Details

F's will provides for a life interest for his wife, with remainder to his children in equal shares. One of the children dies prior to the wife.

Application

The wife is not a beneficial owner. (see example 4)

The child who has pre-deceased his mother has a vested interest in the remainder as there is no condition precedent that he must survive his mother. Therefore the interest survives him and is capable of being bequeathed by his will or passing under his intestacy.

It will depend on the number of children as to the level of interest each has. If it is under 25 per cent then it would simply be under Part B. If each has at least 25 per cent then they will need to be individually identified under Part A and enquiries will need to be made of the trustee as to who is now entitled to the deceased child's interest.

4.12.6 Example 6

Details

I's will provides for a life interest in favour of his wife, with remainder to his four children in equal shares. The trustee is given express power to vary the shares, in whole or in part.

Application

This means that the interests of the children are vested but are defeasible. Until the trustee exercises their power to vary the interest, all of the children will be identified under Part A. Once the trustee exercises their power, any children with an interest remaining at 25 per cent or more will continue to be identified under Part A, while the others will be identified under Part B. The trustees will be identified under Part C. The wife is not a beneficial owner (see example 4)

4.12.7 Example 7

Details

J by his will created a life interest in favour of his wife, with the remainder to his three children in equal shares. The trustees are given a power, during the life of the widow, to appoint an interest in all or part of the capital of the fund, without her consent, in favour of such charities as they may select.

Application

Until the power of appointment is exercised all three children have a vested interest in the remainder and should be identified under Part A.

If for example the power of appointment is exercised and 50 per cent of the fund is to be paid to one specified charity – prior to the distribution it is recommended that the charity be identified under Part A and the children under Part B. After the distribution is made, the children will then return to having a one-third share each and be identified under Part A. As such it is important to obtain updated information when taking on a new retainer for such a trust.

4.12.8 Example 8

Details

N creates an inter vivos trust for his three named grandchildren subject to attaining 21, with substitution for their issue, reserving to himself the power to appoint or remove trustees.

Application

The three grandchildren have contingent interests and so will be identified under Part B. N has control and should be identified under Part C due to the power to appoint or remove trustees.

4.12.9 Example 9

Details

O creates an inter vivos trust for his three named grandchildren subject to attaining 21, with substitution for their issue, appointing a protector (P) with power to veto any advancement of capital by the trustees under s32 of the Trustee Act 1925 and to appoint or remove trustees.

Application

The grandchildren have contingent interests and are identified under Part B. Both P and the trustees have control over the trust and should be identified under Part C.

4.12.10 Example 10

Details

Q's will creates discretionary trusts of which his wife and issue are the beneficiaries. He gives his trustees the power, with the consent of his children, to add beneficiaries from amongst the spouses and civil partners of his issue.

Application

Both the trustees and the children have control of the trust and are subject to identification under Part C, while the wife and all of the issue are discretionary beneficiaries and are to be identified as a class under Part B.

Chapter 5 – money laundering offences

5.1 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.

5.2 Application

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

5.3 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.

5.3.1 Knowledge

Knowledge means actual knowledge. There is some suggestion that wilfully 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.

5.3.2 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 *Da Silva* [1996] EWCA Crim 1654, which was prosecuted under the 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 11 of this practice note 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 judgement. To help form that judgement, consider talking through the issues with colleagues or with the Law Society. You could take legal advice, possibly from another solicitor on the Law Society's AML directory. 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.

5.3.3 Reasonable grounds to suspect

The issues here for the solicitor 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?

5.4 Principal money laundering offences

5.4.1 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 – see the second edition of Money Laundering Legislation: Guidance for Solicitors 2002 (PDF, 242kb)

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.

5.4.2 Section 327 – concealing

A person commits an offence if he 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.

5.4.3 Section 328 - arrangements

A person commits an offence if he 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 s328 does not cover or affect the ordinary conduct of litigation by legal professionals, including any step taken in litigation from the issue of proceedings and the securing of injunctive relief or a freezing order up to its final disposal by judgment.

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 s328 or s329 of the Act.

Sham litigation

Sham litigation created for the purposes of money laundering remains within the ambit of s328. 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 s328

If you are doing transactional work and become suspicious, you have to consider:

- whether an arrangement exists and, if so, whether you have entered into or become concerned in it or may do so in the future
- if no arrangement exists, whether one may come into existence in the future which you may become concerned in

5.4.4 Section 329 - acquisition, use or possession

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

5.5 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 (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 s329 you will also have a defence if you received adequate consideration for the criminal property (the adequate consideration defence).

5.5.1 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, such as Rule 4 of the Solicitors' Code of Conduct, relating to client confidentiality.

Where your firm 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 SOCA. If your firm does not have a nominated officer, you should make your disclosure directly to SOCA.

Appropriate consent

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 SOCA via your nominated officer and seek consent 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 SOCA and the process by which consent is gained, see chapter 8 of this practice note.

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 Law Society's view that you will have a reasonable excuse for not making an authorised disclosure and will not commit a money laundering offence.

Read more about legal professional privilege.

There may be other circumstances which would provide a reasonable excuse, however these are likely to be narrow. You should clearly document the reason for not making a disclosure on this ground.

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 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.

5.5.2 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 solicitors 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 to deal with the money before you transfer it.

Reaching a matrimonial settlement or an agreement on a retiring partner's interest in a business does not constitute adequate consideration for receipt of criminal property, as in both cases the parties would only be entitled to a share of the legitimately acquired assets of the marriage or the business. This is particularly important where your client would be receiving the property as part of a settlement which would be exempted from s328 due to the case of *Bowman v Fels*.

The defence is more likely to cover situations where:

- a third party seeks to enforce an arms 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 arms length transaction but unknown to them is paid from a bank account which contains the proceeds of crime

5.6 Failure to disclose offences – money laundering

5.6.1 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, solicitors 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 s330 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

5.6.2 Section 330 – failure to disclose: regulated sector

A person commits an offence if

- he 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 fails to disclose that knowledge or suspicion, or reasonable grounds for suspicion, as soon as practicable to a nominated officer or SOCA

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

5.6.3 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 s330, 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 SOCA.

5.6.4 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 SOCA.

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

5.7 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.

5.7.1 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, as with reasonable excuse under the principal money laundering offences, where common law legal professional privilege has not been expressly excluded, following the reasoning in *Bowman v Fels*, it is the Law Society's view that the decision not to make a disclosure because the information is subject to legal professional privilege would be a reasonable excuse.

You should carefully document any reasons for not making a disclosure under this section.

5.7.2 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
- 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 solicitor with the intention of furthering a criminal purpose.

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

http://www.cps.gov.uk/legal/p_to_r/proceeds_of_crime_money_laundering/#_Defences_to_section_330

For a further discussion of privileged circumstances see Chapter 6.

5.7.3 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 Money Laundering Regulations 2007 if they fail to train staff.

5.8 Tipping off

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

There are also tipping off offences for terrorist property in the Terrorism Act 2000, as amended by the TACT and POCA Regulations 2007 [\[link\]](#). Read more [\[link 7.7\]](#)

5.8.1 Offences

5.8.1.1 Tipping off – in the regulated sector

There are two tipping off offences in S333A of POCA. They apply only to business in the regulated sector.

- **S333A(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, SOCA 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 SOCA
 - 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
- **S333A(3) – disclosing an investigation.** It is an offence to disclose 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 where you are unaware that a SAR was submitted.

5.8.1.2 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 [\[link\]](#). 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.

5.8.2 Defences

5.8.2.1 Tipping off

The following disclosures are permitted:

- S333B - disclosures within an undertaking or group, including disclosures to a professional legal adviser or relevant professional adviser
- S333C - disclosures between institutions, including disclosures from a professional legal adviser to another professional legal adviser;
- S333D - disclosures to your supervisory authority
- S333D(2) - disclosures made by professional legal advisers to their clients for the purpose of dissuading them from engaging in criminal conduct.

A person does not commit the main tipping off offence if he does not know or suspect that a disclosure is likely to prejudice an investigation.

5.8.2.1.1 s333B – Disclosures within an undertaking or group etc

It is not an offence if an employee, officer or partner of a firm discloses that a SAR has been made if it is to an employee, officer or partner of the same undertaking.

A solicitor will not commit a tipping off offence if a disclosure is made to another lawyer either:

- within a different undertaking, if both parties carry on business in an EEA state
- in a country or territory that imposes money laundering requirements equivalent to the EU and both parties share common ownership, management or control

5.8.2.1.2 s333C – disclosures between institutions etc

A solicitor will not commit a tipping off offence if **all** the following criteria are met:

- The disclosure is made to another lawyer 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.
- Both parties have equivalent professional duties of confidentiality and protection of personal data.

5.8.2.1.3 S333D(2) – limited exception for professional legal advisers

A solicitor will not commit a tipping off offence if the disclosure is to a client and it is made for the purpose of dissuading the client from engaging in conduct amounting to an offence. This exception and the tipping off offence in s333A apply to those carrying on activities in the regulated sector.

5.8.2.2 Prejudicing an investigation

5.8.2.2.1 S342(4) – professional legal adviser exemption

It is a defence to a S342(1) offence that a disclosure is made by a legal adviser to a client, or a client's representative, in connection with the giving of legal advice or to any person in connection with legal proceedings or contemplated legal proceedings.

Such a disclosure will not be exempt if it is made with the intention of furthering a criminal purpose (s342(5)).

5.8.3 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, if possible, any concerns and enable the firm 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 firm's standard client care letter.

Chapter 6 – legal professional privilege

6.1 General comments

Solicitors 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 SOCA.

Solicitors 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 solicitor's duties and these provisions of POCA. Similar tensions also arise with respect to the Terrorism Act and you should refer to the Law Society's practice note on anti-terrorism in those circumstances.

This chapter should be read in conjunction with Chapter 5 of this practice note and if you are still in doubt as to your position, you should seek independent legal advice. The Law Society's AML directory may be of assistance in locating a solicitor who practises in this area of law.

6.2 Application

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

6.3 Duty of confidentiality

A solicitor 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 solicitor, from whatever source, by a client, or someone acting on the client's behalf. See Solicitors' Code of Conduct – Rule 4.

In exceptional circumstances this general obligation of confidence may be overridden. See Solicitors' Code of Conduct Rule 4 – note 10. 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).

6.4 Legal professional privilege

6.4.1 General overview

LPP is a privilege against disclosure, ensuring clients know that certain documents and information provided to lawyers 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 lawyers 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.

For the purposes of LPP, a lawyer only includes solicitors and their employees, barristers and in-house lawyers.

6.4.1 Advice privilege

Principle

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

- confidential
- for the purpose of seeking legal advice from a solicitor 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 lawyer using his legal skills and which are directly related to the performance of the lawyer'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 will attract LPP 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] are not privileged, as the content of the communication is not confidential.
- conversations, correspondence or meetings with opposing lawyers [*Parry v News Group Newspapers* (1990) 140 New Law Journal 1719] are not privileged, 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 are not communication so not subject to advice privilege [*R v Inner London Crown Court ex p. Baines & Baines* [1988] QB 579]

Advice within a transaction

All communications between a lawyer and his client relating to a transaction in which the lawyer 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 solicitor of his professional duty as legal adviser of his 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.

6.4.3 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 either:

- a lawyer and a client
- a lawyer and an agent, whether or not that agent is a lawyer
- a lawyer and a third party

These communications must be for the sole or dominant purpose of litigation, either:

- for seeking or giving advice in relation to it
- for obtaining evidence to be used in it
- for obtaining information leading to obtaining such evidence

6.4.4 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 lawyer 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.

6.4.5 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 Lloyd's 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 lawyer/client communication to be made with that purpose (eg 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 solicitor forms a genuine, but mistaken, belief that the privileged circumstances exemption (see 6.5 below) applies (for example, the client misleads the solicitor and uses the advice received for a criminal purpose) the solicitor 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.

6.5 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

- by any person for the purpose of/in connection with actual or contemplated legal proceedings
- the information or material cannot be communicated or given to you with a view to furthering a criminal purpose

The defence covers solicitors, their non-solicitor partners and their employees (see s330 (7B) of POCA) [\[link to POCA\]](#), barristers and in-house lawyers.

Consider the crime/fraud exception [\[link to 6.4.5\]](#) 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.

6.6 Differences between privileged circumstances and LPP

6.6.1 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)
- 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.

6.6.2 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 lawyer representing client A may hold or have had communicated to him information which is privileged as between client B and his own lawyer, 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).

However, privileged circumstances will not apply because the information was not communicated to client A's lawyer 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 lawyer 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.

6.6.3 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.

6.7 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 SOCA.

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. Section 337 of POCA permits 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 7 – terrorist property offences

7.1 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.

7.2 Application

All persons are required to comply with the Terrorism Act. The principal terrorist property offences in s15 – 18 apply to all persons and therefore to all solicitors. 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 [\[link\]](#) 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 the Proceeds of Crime Act 2002.

7.3 Principal terrorist property offences

7.3.1 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
- 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.

7.3.2 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.

7.3.3 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.

7.3.4 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 5

7.4 Defences to principal terrorist property offences

The TACT and POCA Regulations 2007 [link] of 26 December 2007 introduced three new defences to the main offences in s15 – 18. These defences are contained in s21ZA – 21ZC.

- **prior consent 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 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 5.7.1 [link] on reasonable excuse

Read chapter 8 for more information on how to make a disclosure and gaining consent. [link to chapter 8]

There are further defences relating to co-operation with the police in s21. You do not commit an offence under s15-18 in the following further circumstances:

- you are acting with the express consent of a constable, including civilian staff at SOCA
- you disclose your suspicion or belief to a constable or SOCA 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 SOCA 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 firm.

7.5 Failure to disclose offences

7.5.1 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 SOCA, 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.

7.5.2 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 firm'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 [\[link\]](#) to cover failure to disclose an attempted offence under section 15 -18.

7.6 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
- you received the information on which the belief or suspicion is based in privileged circumstances, without an intention of furthering a criminal purpose

TACT Regulations 2007 [\[link\]](#) 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 solicitor 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 5.7.2 [\[link\]](#)

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

7.7 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, SOCA 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 SOCA
 - 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.

7.8 Defences to tipping off

7.8.1 Section 21E – disclosures within an undertaking or group etc

It is not an offence if an employee, officer or partner of a firm discloses that a SAR has been made if it is to an employee, officer or partner of the same undertaking.

A solicitor will also not commit a tipping off offence if a disclosure is made to another lawyer 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.

7.8.2 Section 21F – other permitted disclosures

A solicitor will not commit a tipping off offence if all the following criteria are met:

- the disclosure is made to another lawyer 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
- both parties have equivalent professional duties of confidentiality and protection of personal data.

7.8.3 Section 21G – limited exception for professional legal advisers

A solicitor 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.

7.9 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.

7.10 Other terrorist property offences in statutory instruments

7.10.1 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
- 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
- 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 no 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
- corporate restructuring and strategy.

7.10.2 Obtaining a licence from the Treasury

You must not proceed with a transaction without a licence from the HM Treasury 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
- consider whether you have a suspicion of money laundering or terrorist financing which requires a report to SOCA

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

Telephone 020 7270 5664 or 020 7270 5454

Fax 020 7451 7677
Email assetfreezingunit@hm-treasury.gov.uk
Address 1 Horse Guards Road
London SW1A 2HQ

Chapter 8 – making a disclosure

8.1 General comments

The disclosure regime for money laundering and terrorist financing is run by the financial intelligence unit within the Serious Organised Crime Agency (SOCA). SOCA was created on 3 April 2006 by the Serious Organised Crime and Police Act 2005. 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 SOCA and their activities view their website at: www.soca.gov.uk

8.2 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 SOCA of suspected terrorist financing.

8.3 Suspicious activity reports

8.3.1 What is a SAR?

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

8.3.2 Who discloses?

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

8.3.3 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.

8.3.4 Types of disclosures

Reports can either take the form of a SAR or a limited intelligence value report (LIVR). SARs will generally be the normal method of reporting, particularly where consent is required; however, LIVRs may be appropriate where you know that a law enforcement agency already has an interest in a matter. SOCA has provided detailed information (PDF) on when LIVRs should be used. If in doubt, complete a SAR form.

8.3.5 How to disclose

Forms

SOCA has issued a preferred form to be completed when making a SAR. We encourage you to use the preferred form to enhance SOCA'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 SOCA allows you to:

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

Information and registration details

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 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

8.3.6 Information to include

SOCA has provided information on completing the preferred SARs form.

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

Your regulator number is your firm's ID number. Find this at www.solicitors-online.com or by calling the Solicitors Regulation Authority on 0870 606 2555.

8.3.7 Getting consent from SOCA to proceed

You will often be asking SOCA for consent to undertake acts which would be prohibited as a principal money laundering offence or a terrorist property offence. From 26 December 2007, the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 introduced a consent defence to sections 15-18 of the Terrorism Act 2000. The Regulations introduce s21ZA, which provides a defence if you made 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.

While SOCA has produced information on obtaining consent, here are a number of key points to remember:

- You only receive consent to the extent to which you asked for it. So it is vital you clearly outline all the remaining steps in the transaction that could be a prohibited act. For example:

We seek consent 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 is refused, the moratorium period is a further 31 calendar days from the date of refusal. If you need consent sooner, you should clearly state the reasons for the urgency in the initial report and perhaps contact SOCA to discuss the situation. SOCA can sometimes give consent 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.
- SOCA will contact you by telephone to advise that consent has been provided and will then send a follow up letter.

8.3.8 Talking to a SOCA representative

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

- help in submitting a SAR or with the SARs online system
- help on consent issues
- assessing the risk of tipping off so you know whether disclosing information about a particular SAR would prejudice an investigation

8.3.9 Confidentiality of SARs

SOCA 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 firm is not disclosed to other persons.

If you have specific concerns regarding your safety if you make a SAR, you should raise this with SOCA 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. In addition, you can e-mail the Law Society at antimoneylaundering@lawsociety.org.uk, so that we can continue to monitor this issue for discussion with SOCA.

8.4 Feedback on SARs

SOCA 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:

- on their website
- in their annual reports
- during SOCA legal sector seminars, details of which are advertised in the Law Society's AML e-newsletter

Chapter 9 – enforcement

9.1 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 regulators are working co-operatively with the regulated sector specifically and solicitors generally to assist compliance and increase understanding of how to effectively mitigate risks. However, be in no doubt of the seriousness of the sanctions for a failure to comply, nor the willingness of supervisory and enforcement bodies to take appropriate action against non-compliance.

9.2 Supervision under the regulations

Regulation 23 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 joint supervisory authorities must negotiate 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:

- monitor effectively the persons it is responsible for
- take necessary measures to ensure their compliance with the requirements of the regulations
- report to SOCA any suspicion that a person it is responsible for has engaged in money laundering or terrorist financing

9.2.1 Solicitors Regulation Authority

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 practice to the Solicitors Regulation Authority (SRA).

9.2.2 Other supervisors

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

- The Financial Services Authority – www.fsa.org.uk

- The Insolvency Practitioners Association – www.insolvency-practitioners.org.uk
- The Council of Licensed Conveyancers – www.thecclc.gov.uk
- The Chartered Institute of Taxation – www.tax.org.uk

Where the SRA reaches agreement with another supervisor about who is to be the supervisory authority for the solicitor, this agreement will be made known to the solicitor in accordance with Regulation 23(3).

In all other cases of supervisory overlap, and where you have questions about AML supervision, contact the SRA.

The SRA will be publishing information for trust and company service providers who are regulated by the SRA and are authorised persons. Details will appear on the SRA's website at www.sra.org.uk, and the Law Society's website at www.lawsociety.org.uk/antimoneylaundering.

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

Read JMLSG's guidance

9.2.3 Enforcement powers under the regulations

Part 5 of the regulations gives designated authorities a variety of powers for performing their functions under the regulations. They can also impose civil penalties for non-compliance.

The powers are:

- Regulation 37: power to require information from, and attendance of, relevant and connected persons without a warrant
- Regulation 38: power to enter and inspect without a warrant
- Regulation 39: power to obtain a warrant to do things under regulations 37 and 38
- Regulation 40: power to obtain a court order requiring compliance with regulation 37

HM Treasury has stated that designated authorities may use these powers in their role as supervisor, and only on those relevant persons they supervise.

9.3 Disciplinary action

Conduct which fails to comply with AML/CTF obligations may also be a breach of Rule 5 of the Solicitors' Code of Conduct 2007, and result in disciplinary action by the SRA.

For further information on the Solicitors' Code of Conduct go to www.sra.org.uk or contact the professional ethics helpline on 0870 606 2577 (inside the UK), 09:00 to 17:00, Monday to Friday.

9.4 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.

9.4.1 POCA

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

9.4.2 Terrorism Act

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	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
21	Tipping off –regulated sector	

9.4.3 Regulations

Regulation 45 lists a number of sections, the breach of which is an offence.

Section	Description	Penalty
7 (1)	Applying CDD to new customers	On summary conviction – a fine On indictment – up to two years imprisonment or a fine or both
7 (2)	Applying CDD to existing customers	
7 (3)	Determining extent of CDD on a risk-sensitive basis and being able to demonstrate this to the SRA	
8 (1)	Conducting ongoing monitoring	

8 (3)	Determining extent of ongoing monitoring on a risk-sensitive basis and being able to demonstrate this to the SRA	
9 (2)	Verification prior to the establishment of a business relationship or carrying out of an occasional transaction	
10 (1)	Relates to casinos	
11 (1)(a)	Not use a bank account without CDD	
11 (1)(b)	Not establish a business relationship or carry out an occasional transaction if no CDD	
11 (1)(c)	Terminate existing relationship or occasional transaction if no CDD	
14 (1)	Conduct enhanced due diligence	
15 (1)	Relates to financial and credit institutions	
15 (2)		
16 (1)		
16 (2)		
16 (3)		
16 (4)		
19 (1)	Keep your own records	
19 (4)	Keep records others have relied on	
19 (5)	Be prepared to provide records others have relied on	
19 (6)	Ensure those you rely on are willing to provide records	
20 (1)	Establish policies and procedures	
20 (4)	Relates to financial and credit institutions	
20 (5)		
21	Train relevant employees	
26	Does not relate to solicitors	

27 (4)		
33		
Directions under 18	Not to act where Treasury makes a direction	

9.5 Joint liability

Regulation 47 provides that offences under the regulations can be committed by a firm 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 firm and the individual can be liable.

9.5 Prosecution authorities

The Crown Prosecution Service 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 FSA is a prosecuting authority under POCA and the regulations as a result of section 402 of the Financial Services and Markets Act 2000.

The Office of Fair Trading, the Local Weights and Measures Authority and the Department of Enterprise, Trade and Investment in Northern Ireland are all prosecuting authorities for breaches of the regulations.

Chapter 10 – civil liability

10.1 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.

10.2 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.

10.3 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:

10.3.1 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

10.3.2 For your use and benefit

When you receive money, eg as an agent, or, as in the case of a solicitor's 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.

10.3.3 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 wilful 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 funds' provenance should be such that it was unconscionable for you to retain any benefit.

It's 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.

10.4 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:

10.4.1 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
- have sufficient ground for suspicion of this

10.4.2 You must be at fault

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, ie your intelligence, knowledge at the relevant time, and your experience.

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

10.5 Making a disclosure to SOCA

10.5.1 Risk of defensive disclosure to SOCA

Where you suspect or know your clients are involving you in circumstances that could amount to one of the principal money laundering offences, you must disclose your suspicions to SOCA, subject to the constraints of LPP, and obtain their permission before allowing the transaction to proceed.

Consent from SOCA only protects you from falling foul of the anti-money laundering regime. It will not defend you from civil liability. In fact, obtaining consent may create the very evidence on which a claimant can rely to found a civil liability.

It is therefore vital that you only disclose to SOCA those situations fulfilling the statutory tests in Part 7 of POCA; knowledge or suspicion of money laundering, or reasonable grounds to suspect money laundering.

10.5.2 While awaiting consent from SOCA

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 recent ruling on the obligations of banks is helpful in suggesting the courts' likely view of the obligations imposed on solicitors. 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.

10.5.3 Where SOCA consents

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

- Although you had sufficient suspicion to justify a disclosure to SOCA, 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. Solicitors are expected to be able to account for decisions to proceed with transactions.
- 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] 1 WLR 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.

10.6 Notify your professional indemnity insurers

You must notify your insurers at the earliest opportunity of any circumstances that might give rise to a claim. You should consider notifying your insurers whenever you make a disclosure to SOCA. In particular:

- you may be unable to follow clients' instructions, eg:
 - where consent has not been given by SOCA

- where you judge you may be exposing yourself to a civil claim, so may face a claim from the client for failure to meet the terms of your retainer
- SOCA has given consent, but where you fear civil liability. Consider whether to not proceed with the transaction.

Any disclosure made to insurers should clearly state any money laundering issues, that a disclosure has been made to SOCA and, if known, SOCA's response.

You may be concerned about tipping off offences under the Proceeds of Crime Act 2002 when talking to your insurer.

A key element of the offence is the likelihood of prejudicing an investigation. The risk of this is small when disclosing to a reputable insurer. Insurers are also regulated for the purposes of anti-money laundering and subject to the same obligations.

For further advice on tipping off, see chapter 5.8

For further information about avoiding tipping off in a particular case, contact SOCA's Financial Intelligence Helpdesk on 020 7238 8282.

Chapter 11 – money laundering warning signs

11.1 General comments

The Money Laundering Regulations 2007 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 solicitors generally and for those working in specific sectors, to help you decide whether you have reasons for concern or the basis for a disclosable suspicion.

11.2 General warning signs

Because money launderers are always developing new techniques, no list of examples can be fully comprehensive; however, here are some key factors which may heighten a client's risk profile or give you cause for concern.

11.2.1 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.

11.2.2 Unusual instructions

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

Instructions outside your firm's area of expertise

Taking on work which is outside your firm's normal range of expertise can be risky because money launderers might use such firms to avoid answering too many questions. An inexperienced solicitor might be influenced into taking steps which a more experienced solicitor would not contemplate. Be wary of instructions in niche areas of work in which your firm 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 firm? 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. Consider the Solicitors' 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
- complex or unusually large transactions
- unusual patterns of transactions which have no apparent economic purpose

11.2.3 Use of client accounts

Only use client accounts to hold client money for legitimate transactions for clients, or for another proper legal purpose. Putting dirty money through a solicitor's client account can clean it, 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.

Solicitors should not provide a banking service for their clients. However, it can be difficult to draw a distinction between holding client money for a legitimate transaction and acting more like a bank.

For example, when the proceeds of a sale are left with your firm to make payments, these payments may be to mainstream loan companies, but they may also be to more obscure recipients, including private individuals, whose identity is difficult or impossible to check.

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 SOCA.

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 accounts 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.

11.2.4 Suspect territory

While there are no longer any countries currently listed on the FATF non co-operative and compliant territories list, this does not mean that all have anti-money laundering standards equivalent to those in the UK .

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.

The Financial Action Taskforce and HM Treasury have released a list of countries which they consider present a higher risk of money laundering. These countries are:

- Iran
- Uzbekistan

You should undertake enhanced due diligence and ongoing monitoring with respect to these countries.

They have also released a list of countries which they consider have deficient anti-money laundering standards. These countries are:

- Turkmenistan
- Pakistan
- Sao Tome
- northern part of Cyprus

You should take these warnings into account when assessing the risk of any retainer.

[http://www.hm-treasury.gov.uk/press_107_08.htm]

The International Bar Association provides a summary of money laundering legislation around the world at: www.anti-moneylaundering.org.

Transparency International provides a corruption perception index which may help when you are considering dealing with clients from other countries.

You can also check whether your client is a proscribed person on the HM Treasury's consolidated list.

11.3 Private client work

11.3.1 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 are avoided. A key benefit of the *Bowman v Fels* judgment is that a solicitor 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. Information on the financial thresholds for benefits can be obtained from www.dwp.gov.uk or www.hmrc.gov.uk.

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 less 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'), you should carefully consider their position in conduct terms with respect to Rule 1.01 of the Solicitors' Code of Conduct.

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 lawyer 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.

11.3.2 Trusts

Trust work is a regulated activity.

Trusts can be used as a money laundering vehicle. The key 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 trustees using 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. 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 and those who have control of the funds, as required by the Money Laundering Regulations 2007, 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 trustees. 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.

11.3.3 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 it is aligned with. 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 7.10 of this practice note.

[http://www.hm-treasury.gov.uk/fin_sanctions_index.htm]

11.3.4 Powers of attorney/deputyship

Whether acting as, or on behalf of, an attorney or deputy, you should remain alert to money laundering risks.

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 SOCA.

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 SOCA 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. You can get legal advice on this through the Law Society's AML directory.

11.4 Property work

11.4.1 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.

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.

11.4.2 Methods of funding

Many properties are bought with a combination of deposit, mortgage and/or equity from a current property. Usually, as a solicitor, 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

Usually purchase funds comprise some private funding, with the majority 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

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.

Consider whether there are any obvious warning signs and what you know about:

- your client
- the third party
- their relationship
- 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.

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.

11.4.3 Valuing

An unusual sale price 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.

11.4.4 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 arms 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 consider the ethical implications of continuing with the retainer. 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.

See chapter 5 of the Mortgage Fraud practice note
<http://www.lawsociety.org.uk/productsandservices/practicenotes/mortgagefraud/522.article#mf5>

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 SOCA 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, possibly by contacting a solicitor in the AML directory.

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 are 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 anti-money laundering practice note, Chapter 5.8.

For further information about avoiding tipping off in a particular case, contact SOCA's Financial Intelligence Helpdesk on 020 7238 8282.

11.4.5 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.

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 under rule 1.10 of the Solicitors' Code of Conduct. If you discover the evasion after it has occurred, you are obliged to make a disclosure, subject to any legal professional privilege.

11.5 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 solicitors working with companies and in commercial transactions should remain alert throughout their retainers, with existing as well as new clients.

11.5.1 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, it may be helpful to clarify why this is the case. In countries where there are few anti-money laundering requirements, you should make particularly careful checks.

If you are in doubt, it may be better to refuse the retainer.

11.5.2 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.

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.

11.5.3 Private equity

Law firms 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
- 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 is likely to be the private equity sponsor or it may be an independent sponsor.

You will rarely, if ever, be advising the fund itself and, unless you are instructed directly by an investor, you will not be considered to be advising the investors in the fund.

You should therefore identify who your client is and apply the CDD measures according to their client type as set out in 4.6 [\[link\]](#).

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 FSA
- investors in private equity funds are generally large institutions, some of which will also be regulated for money laundering purposes. They will have long established relationships with the private equity firm, usually resulting in a well-known investor base
- 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
- the investment is generally illiquid and the return of capital is unpredictable
- the terms of the fund documentation generally strictly 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 third 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

JMLSG has prepared detailed advice on CDD measures for private equity businesses in Part II of its guidance, which you may wish to consider.

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
- 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 17
- 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
 - 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.

11.5.4 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

JMLSG have also issued guidance which touches on the area of collective investment schemes, which you may wish to have regard to.

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.

Page 127 of 137

12.2.1 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 be 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.

12.2.2 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 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 SOCA.

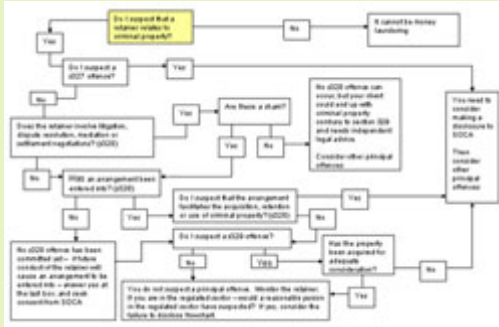
The following two flowcharts show the issues to consider when deciding whether to make a disclosure to SOCA.

I suspect continuation of a retainer will lead to me being a party to a principal offence. Do I have a defence?



Full screen view | Download (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?



12.3 Should I make a disclosure?

12.3.1Property 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 SOCA.
- 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 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 SOCA 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 SOCA.

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 and progressing the retainer

If you make a disclosure and consent is needed, consider whether you can continue working on the retainer before you receive that consent.

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.

12.3.2 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/consent 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.

Solicitors 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 solicitors which, in effect, result in the information being received again by the vendor's solicitor.

That second receipt from the purchaser, or their solicitor, 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 solicitor 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.

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, 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 solicitors 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 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
- 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 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, 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 before completion.
- The solicitors 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.

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 SOCA 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 from SOCA, 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 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 solicitor.