



Guidance for the Prevention of Money Laundering and Combating Terrorist Financing

16 Glebe Road, Chelmsford, CM1 1QG

t: 01245 349599
f: 01245 341300
w: www.clc-uk.org

Council for Licensed Conveyancers
**Guidance for the Prevention of Money Laundering
and
Combating Terrorist Financing**

Table of Contents

		Page no
Chapter 1	A Short Guide to Anti-Money Laundering and Combating Terrorist Financing	4
Chapter 2	Scene Setting	12
Chapter 3	Systems and Controls	16
Chapter 4	Nominated Officer	21
Chapter 5	Education & Training	25
Chapter 6	Customer Due Diligence	29
Chapter 7	Internal Reporting Procedures	52
Chapter 8	Assessment of Internal Reports	55
Chapter 9	External Reporting to SOCA	58
Chapter 10	Record-Keeping	64
Chapter 11	Money Laundering and Terrorist Financing Overview	70
Annex	Glossary of Terms and Definitions	83
	Acknowledgments	88

Chapter 1 - A short guide to Anti-Money Laundering and Combating Terrorist Financing

1.1 Introduction

Since 1 March 2004, Licensed Conveyancers have been regulated under the anti-money laundering (AML) and countering terrorist financing (CTF) legislation. New regulations take effect from 15 December 2007 which, to some extent, modify the approach to be adopted both by practitioners and their regulators. But a very considerable part of the existing requirements continues as before. So Practices which have sound AML/CTF procedures will be well-placed to comply with these new regulations. CLC is issuing this Guidance (which fully updates that issued in 2004) to help Practices meet the requirements of the primary and secondary legislation and to promote good practice. At the same time, CLC is issuing its AML Toolkit, which provides practical suggestions on ways to put many of the requirements into effect.

This first Chapter gives a brief outline of the main provisions, with pointers to where more detail is to be found. At the end of the chapter, you'll find examples of situations in which Licensed Conveyancers might come into contact with money laundering or terrorist financing.

Key points to bear in mind include:

- the responsibility and regulatory obligation for compliance falls firmly on all Principals (which includes non-Licensed Conveyancer Directors of Recognised Bodies), who must implement and maintain appropriate policies and procedures
- these must be tailored to the risks and vulnerabilities faced by their particular Practice (taking a *risk-based* approach – for more on this, see Box on page 8)
- central to effective AML/CTF measures is knowing just who a Practice is dealing with - the new regulations place even greater emphasis on this, underpinning it with criminal sanctions.

What is money laundering?

Criminals seek to launder dirty money in an attempt to make it look clean by giving it an air of legitimacy. Money laundering is therefore the process of moving any proceeds of crime through a cycle of transactions or events to achieve these purposes, allowing criminals to retain control and continued use of such proceeds by avoiding suspicion, detection, confiscation or forfeiture.

Legitimate businesses (like Practices of Licensed Conveyancers) are used to create an air of legality. The Client Accounts of property professionals are particularly vulnerable and property transactions generally have proved to be an especially high risk area. It is therefore vital that Principals take all appropriate and necessary steps to make sure that their Practices are not used to further criminal purposes.

What about terrorist financing?

Terrorism is financed not only from the proceeds of illegal activities but also from donations and contributions originating from lawful sources. The ways used to transfer funds or to conceal the connecting sources which finance terrorism are similar to those used in money laundering. Terrorist property is widely defined to include money or other property which is likely to be used for the purposes of terrorism, the proceeds derived from actual acts of terrorism or the proceeds of any acts carried out to further terrorist purposes.

One of the principal differences between criminal money laundering and terrorist financing is that the latter often involves smaller sums of money coming from sources that may be legitimate at the outset. As such, it has sometimes been called "reverse money laundering", a process though which "clean" money is converted into "dirty" money because of its intended destination. That alone makes it far harder to detect.

1.2 Key Areas: What you are required to do

The eight key areas which must be tackled by all Practices are summarised below. Further detailed information on each area is provided in Chapters 3 to 10, which include what the CLC expects of licensed conveyancers as well as practical guidance on how this can be achieved. In larger Practices, the task of carrying out the various procedures can be delegated as appropriate; in single-handed Practices, the responsibility largely falls onto one person, who should nevertheless make sure that they have clear policies and procedures in place and documented. Whichever the case, the Principals will remain ultimately liable.

1.2.1 Systems and Controls

Every Practice must establish and implement appropriate and adequate policies and procedures to prevent it being used to launder the proceeds of crime or to finance terrorists or terrorist organisations. Based on a Practice's own assessment of risk, these must be tailored to the specific needs and circumstances of each individual Practice and its business activities. They must be clearly documented and capable of independent verification and must cover:

- identification of clients (now referred to as *Customer Due Diligence* or CDD measures), including ongoing monitoring,
- reporting,
- record-keeping,
- internal control,
- risk assessment and management,
- monitoring and management of compliance with these policies and procedures and internal communication of them, including appropriate training for those working within the Practice.

More information: Chapter 3, page 16

1.2.2 Nominated Officer

A Practice must appoint a Nominated Officer from within the organisation, unless the Practice is a sole principal with no employees engaged in the conveyancing or accounts process of the business (single handed Practice). The Nominated Officer receives and assesses all internal reports and makes external reports as appropriate. It would be sensible to have suitable arrangements (e.g. a Deputy) to cover normal or unexpected absences. The persons appointed should have sufficient seniority and authority to access all client files and other client and Practice records. Any vacancy should be filled without delay. The Nominated Officer needs to be given sufficient resources, support and time to fulfil his regulatory obligations.

Practices may consider appointing a Money Laundering Reporting Officer (MLRO) to take on delegated responsibility for all or some aspects of compliance. However, this will not absolve the Principals of the Practice from liability if the MLRO fails to fulfil that delegated responsibility adequately. The MLRO may also be the Nominated Officer.

More information: Chapter 4, page 21

1.2.3 Education and Training

Every Practice must ensure that all relevant members and employees are made aware of:

- the relevant law relating to money laundering and terrorist financing (including the offences, reporting obligations and penalties),
- its internal AML and CTF policies and procedures, and
- the identity and responsibilities of the Nominated Officer.

They should all be given regular training in how to recognise and deal with any transactions and other activities which may be related to money laundering or terrorist financing. Not all need

necessarily be trained to the same level. Their training should match their status, responsibility and the extent to which they may take part in potentially risky activities. Training should cover:

- guidance on how to recognise suspicious activity,
- the importance of CDD measures, including ongoing monitoring,
- the importance of following internal procedures, and
- the dangers of “tipping-off”.

It will be not be sufficient just to provide them with copies of the law, the internal policies and procedures or the Guidance provided by the CLC. Ongoing training must be provided on a regular basis and records must be kept of all training undertaken. Single-handed practitioners must make sure that they keep themselves up-to-date on all these aspects.

More information: Chapter 5, page 25

1.2.4 Customer Due Diligence Measures & Ongoing Monitoring

Customer Due Diligence (CDD) means, at the most basic level, knowing who you are dealing with. It has several elements including:

- identifying the client and verifying that client’s identity on the basis of information obtained from reliable and independent sources, and
- identifying any beneficial owner who is not one and the same as the client. In the case of a company, trust or similar entity, measures to understand the ownership and control structure are needed, and
- obtaining information on the purpose and intended nature of the business relationship.

These measures must be taken when:

- establishing a business relationship, or
- carrying out an occasional transaction, or
- there is a suspicion of money laundering or terrorist financing, or
- there are any doubts as to the veracity or adequacy of documents, data or information previously obtained for CDD purposes (e.g. for an existing/former client).

Identification and verification must take place before a business relationship is established or an occasional transaction carried out. Obtaining information about the purpose and intended nature of the business relationship should be addressed at the same time.

One-off checks are not sufficient – Practices must also conduct ongoing monitoring of the business relationship. This means checking on transactions as they proceed (including, where necessary, the sources of funds) to make sure that they remain consistent with what is known about the client, his business and risk profile.

The new Regulations introduce enhanced CDD (EDD) and enhanced ongoing monitoring in circumstances where there is potentially more risk – e.g. if the client is not dealt with face-to-face, or if the client is in a prominent public role and therefore may be exposed to corruption.

How much checking and monitoring a practice does is not set in stone – it depends on the judgement made by the Practice of how much risk is posed by that particular client (or type of client) or by the type of transaction involved.

More information: Chapter 6, page 29

1.2.5 Internal Reporting Procedures

Being alert for suspicious behaviour is one thing; making sure that such information gets through to the right authorities is the crucial next step. Every Practice must have written internal reporting procedures, which require all members and employees to report any suspicions and which explain how to do this and to whom. A report must be made to the Nominated Officer if someone

knows or suspects or has reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing. This report must be made as soon as reasonably practicable and without informing anyone else that it is being done.

All internal reports need to go directly to the Nominated Officer. Any failure to report in the above circumstances constitutes a criminal offence. Any reports made by telephone should be confirmed in writing. Systems and controls need to exist to make sure that these procedures are followed and that no internal reports are filtered out or suppressed.

Where a report has been made, no further action should be taken on the transaction without the approval of the Nominated Officer. Having made an internal report, the employee has fulfilled his reporting obligations and it is then up to the Nominated Officer to assess the report. It is important that a client or third party is not alerted to the fact that a report has been made as this may prejudice any investigation by a law enforcement agency. If the client is directly or indirectly alerted, this could constitute "tipping-off", a separate offence which carries criminal sanctions.

In a single-handed Practice with no employees or where the person who has gained the knowledge or formed the suspicion is the Nominated Officer, the details should be recorded as if for an internal report, though he will then also proceed to make an assessment – see next section below.

More information: Chapter 7, page 52

1.2.6 Assessment

When he receives a report, a Nominated Officer should make an evaluation promptly and make a written record of his findings. He should take reasonable steps to consider all the relevant CDD information available in the Practice about the person or business covered by the report. This may include reviewing other transaction patterns and volumes of business, previous patterns of instructions, the length of the business relationship and any other relevant information. He will be expected to act honestly and reasonably and to make his decision in good faith. The Practice must make sure that no barriers are put in the way of his full and frank assessment.

If the Nominated Officer concludes that actual knowledge or suspicion or reasonable grounds for knowledge or suspicion exists, he will need to make a Suspicious Activity Report (SAR) to the Serious Organised Crime Agency (SOCA) in the prescribed form. Only the Nominated Officer has authority to determine whether or not a suspicion has foundation and must be reported to SOCA. If he fails to make an external disclosure in circumstances which warrant one being made, a Nominated Officer will commit a criminal offence carrying separate sanctions which can be more severe than the standard penalties applying to a breach of the Regulations.

The Table on page 9 gives some examples of situations which might give rise to concern.

More information: Chapter 8, page 55

1.2.7 External Reporting to SOCA

The Nominated Officer must send his report (the SAR), in the prescribed form, to the UK Financial Intelligence Unit at SOCA. If the report is sent after a transaction has taken place, it will simply be acknowledged by SOCA. However, if the transaction is ongoing, 'consent' from SOCA will be needed before it can proceed further.

Any disclosure requiring consent should be clearly marked "CONSENT". SOCA can then fast-track the processing of the report and, if appropriate, contact the appropriate law enforcement agency for a decision. If consent is given, the Nominated Officer will be told. Under the money laundering provisions, if no decision is made within seven working days starting on the first working day after a disclosure is made, the transaction may continue as if consent had been given. If consent is refused within that 7-day period, the law enforcement agency must obtain a

Restraint Order within 31 calendar days commencing on the day refusal of consent is notified to prevent the transaction proceeding after the end of that 31-day that period. If no notification is received within these time limits a transaction can go ahead.

Note that this procedure applies only to money laundering and does not currently apply where terrorist financing or suspicion of terrorist financing is involved. A similar 7 working day consent provision is anticipated for terrorist financing, but not a 31-day moratorium period.

The importance of not continuing with a transaction until consent has been obtained from SOCA and the dangers of "tipping off" while waiting for such consent, cannot be underestimated. The interaction between a client and a regulated business during that time can be very difficult to manage. Through its Nominated Officer, a Practice is encouraged to contact SOCA and/or any law enforcement agency and to maintain close liaison during the waiting period (or after the issue of any notice refusing consent) to help both parties in handling the situation.

More information (including contact addresses): Chapter 9, page 58

1.2.8 Record- Keeping

Every Practice must maintain records for at least five years covering evidence of:

- client and beneficial owner identification,
- the supporting evidence and records of the CDD measures taken,
- any ongoing monitoring carried out on all business relationships and occasional transactions, and
- details of all transactions carried out.

It would also be prudent to keep records of the reports made under the internal and external reporting requirements (as these may be needed in any subsequent investigation into money laundering or terrorist financing).

The five-year period starts from the date on which a business relationship ended or an occasional transaction was completed. The relevant records can be kept on the client file and/or in a central record which should be reasonably accessible. The records will need to be sufficient to provide an audit trail for that particular client and that particular transaction in any subsequent investigation.

More information: Chapter 10, page 64

What is a risk-based approach?

Setting up controls and procedures to guarantee that all money laundering and terrorist financing is prevented is impossible. Even getting close to that would impose costs on businesses and clients alike which would be out of proportion to the benefits achieved. The Regulations now expect compliance in these areas to be tackled in a way that takes into account the likely risk associated with particular activities. Property transactions are viewed as a high-risk area to start with, but some types of property transaction and some type of customer pose particular risks. (See the end of this short guide for some examples of situations which should set alarm bells ringing.) Adopting a risk-based approach means having systems and controls to identify and assess the risks faced by a particular business and then monitoring, mitigating and managing those risks. Practices will be expected to be able to demonstrate to their regulator that they have applied a risk-based approach to managing money laundering and terrorist financing risks – and that means documenting the strategy adopted, however large or small your practice is.

More information: Chapter 2, page 13

SOME WARNING SIGNS

- Secretive clients (i.e. client refusal to provide requested information without reasonable explanation)
- Unusual transactions involving instructions that are unusual in themselves or that are unusual for a Practice or a client
- Instructions or transactions that change unexpectedly, particularly where there is no apparent logical reason for the changes
- Illogical third party transactions (i.e. unnecessary routing or receipt of funds from third parties or through third party accounts)
- Involvement of an unconnected third party or involvement of a third party beneficial or legal owner without a logical reason or explanation
- Payment or Settlement (and particularly of large sums) in cash
- Unusual settlement requests (e.g. where funds are received prior to exchange or completion from an unexpected source or where settlement funds are to be paid to an unexpected destination)
- Overpayments (e.g. client provides more money than required or requested)
- Unsolicited deposit of funds by a client into the Practice's client account
- Requests to send money received into a client account back to its source, to a client or to a third party
- No underlying transaction (e.g. instructions to receive and pay out money where there is no linked substantive property transaction involved)
- Requests for the release of client account details other than in the normal course of business
- Extensive use of corporate structures or trusts in circumstances where the client's needs are inconsistent with the use of such structures
- A third party is providing funding for a purchase but the property is being registered in the name of another, unless there is a legitimate reason, such as a family or other related arrangement
- Large payments provided from private funds, especially where the client has a low income
- Payments from a number of different individuals or sources
- Unusual property investment transactions with no discernible investment purpose or rationale
- Loss making transactions where the loss seems to be avoidable
- Dealings with property or money which could involve it being transferred to avoid the attention of a Trustee in Bankruptcy, HM Revenue & Customs or a Law Enforcement Agency

Some examples of how conveyancers may come across money-laundering

Example 1: Small-time 'crook' buys a house

A small-time local criminal wants to "get onto the property ladder" for the same reasons as his hard-working honest neighbour. He does not have a legitimate job or, if he does, he is poorly paid. The conveyancing instruction seems routine but the "hallmarks" of this type of criminal investment are likely to be one or more of the following:

- no requirement for mortgage funds;
- a deposit, possibly provided in cash, which is larger than is usual or unexpectedly large when compared with the client's income as declared (eg on the mortgage application);
- the property is more expensive than might otherwise be expected for this type of Buyer.

Although it does not fit the classic view of money laundering (i.e. money on the move), this example introduces the concept of "criminal property", which is now the focus under the UK legislation. The money used for the deposit represents the proceeds of crime at the outset. When the property is sold on a few years later, it will be criminal property. In this way, the conveyancers acting on both the purchase and subsequent sale of the property will be involved in money laundering.

Example 2: 'Lifestyle' criminal seeks to extend his property portfolio

The successful "lifestyle criminal" is a "man of property" who already owns one or more properties. The conveyancer may have been instructed when those properties were bought. These purchase transactions appeared routine, particularly if the successful "lifestyle criminal" is a respected member of the community. However, there may be tell-tale signs, including the following, which may suggest that all is not what it seems to be:-

- a cavalier attitude towards fees and costs;
- no requirement for mortgage funds but no other obvious source of wealth (e.g. large income from employment or business, family inheritance, etc);
- an instruction requiring the property to be purchased in the name of a third-party (e.g. a wife, a partner, a son or daughter or someone else who is related or unrelated like a so-called business partner) without offering a reasonable explanation;
- an instruction requiring ownership to be taken in the name of a private, possibly off-shore, company or trust, with the private company acquirer often being owned by other private companies or the trust being controlled or owned by others in what appears to be a deliberate attempt to disguise the true ownership.

Example 3: Proceeds of crime being invested in property

A successful criminal or criminal organisation may invest its proceeds in commercial property and/or residential property to let. Such an investment comes at the end of any laundering cycle when the criminal or organisation is confident that the funds seem to be clean. This type of

criminal investment can occur across all price ranges from bed-sits to hotels, farms or even shopping complexes. These may be tell-tale signs:

- an unnecessarily complicated corporate structure;
- the ownership structure, including companies incorporated in remote jurisdictions with strong secrecy laws;
- unusually small local funding requirement with the investment monies sourced from overseas;
- investment funds provided in full or in part by Banker's Drafts and/or cash rather than by direct bank transfers;
- duplicated payments needing a refund from the Practice's client account.

Example 4: Money laundered through the client account

There is the more traditional money laundering ploy, where a client account is abused to move and launder criminal proceeds without the knowledge of the Practice. For example:

- purchasing properties with the intention of a quick sale;
- paying deposits or funding the full purchase price in advance to the conveyancer but with no intention of completing the transaction. The aim is to get a refund from the client account of a respected Practice or giving instructions for the money to be sent to a third-party;
- duplicating payment of the deposit and/or the purchase price in order to get repayment of the deliberate overpayment from the client account although still completing the purchase of the property. The property may be held for a while or sold on quickly.

Example 5: Mortgage or Stamp Duty Land Tax fraud can be money-laundering too

- Having agreed a price above a Stamp Duty Land Tax (SDLT) threshold, a Buyer asks the Seller to agree that part of the total price should be allocated to fixtures and fittings to bring the price for the property below the SDLT threshold. The Seller tells you that the fixtures and fittings are old and are not worth the value the Buyer gives them. If the proposal is agreed, the conveyancers for both the Buyer and the Seller could find themselves handling the proceeds of a SDLT fraud and be involved in the laundering of the proceeds of crime, as well as being complicit in a fraud on HM Revenue & Customs.
- A conveyancer may hold funds as a deposit on an investment property. When the mortgage offer or funds are received, it is discovered that the amount of the loan will cover the full purchase price. The conveyancer may suspect that his client has deliberately overstated the true purchase price to the Lender. Such deliberate misrepresentation is fraud. The deposit and even the full amount received from the Lender are criminal proceeds.

A Practice will need to take account of any guidance issued on Mortgage Fraud (see in particular CLC Guidance Note 14 – Mortgage Fraud).

CHAPTER 2: SCENE SETTING

Introduction

- 2.1 Chapter 1 gave a quick snapshot of what a Practice must do in order to comply with the anti-money laundering and countering terrorist financing law. In particular, it outlined the eight key areas which must be covered in all Practices:
- **Systems and controls** must be in place to guard against being used to launder money or finance terrorism
 - **A Nominated Officer** must be appointed to receive and assess all internal reports and to make external reports where necessary
 - **Education and training** must be provided for staff (including Principals) on the relevant law and on how to recognise and deal with any activity related to money laundering or terrorist funding
 - **Client Due Diligence** and **Ongoing Monitoring** must be in place so that the Practice knows at the outset and on an ongoing basis who it is doing business with and the nature and purpose of the business relationship, and will recognise if any inconsistencies occur
 - **Internal Reporting** procedures must ensure that any suspicions are reported to the Nominated Officer
 - **Assessment** of such reports by the Nominated Officer must take place so that he can make a judgement about whether or not to make an external report to the relevant authority (ie SOCA)
 - **External reporting to SOCA** follows if the Nominated Officer decides that it is appropriate to do so
 - **Record keeping** is crucial both as an audit trail/evidence for law enforcement agencies as well as meeting CLC's regulatory requirements.
- 2.2 Chapters 3 to 10 give more details on each of these areas. At the start of each chapter, the key requirements of the Regulations are summarised. This is followed by what CLC expects of each Practice in order to meet the obligations placed on them. And, finally, some practical guidance is given to help Practices to comply with the regulations. Where relevant, there are references to CLC's Anti-Money Laundering Toolkit, which gives suggestions how the various policies and procedures can be put into effect.
- 2.3 Chapter 11 provides a brief outline of the nature of money laundering and terrorist financing, the development of the relevant law, offences and penalties. In the Appendix, there is a Glossary of the terms used throughout this Guidance.
- 2.4 The rest of this Chapter clarifies two important aspects of the current regulatory regime, notably:
- A risk-based approach to anti-money laundering and combating terrorist financing, and

- The expectations placed on regulated practices by the Regulations and their regulators.

A Risk-Based Approach to AML and CTF

2.5 The Regulations require firms to take a “risk-sensitive” approach (a term used in the Third Money Laundering Directive) to AML and CTF . The Government has confirmed that:

- a “risk-sensitive approach” is the same as a “risk-based approach”, the term used throughout this Guidance;
- the “risk-based approach” to AML & CTF is essential to the effective and proportional functioning of the UK’s strategy to deter, detect and disrupt money laundering and terrorist financing;
- the risk-based approach to AML & CTF aims to ensure that measures to reduce money laundering and terrorist financing are commensurate to the risks identified.

2.6 The CLC’s approach is as follows:

- a) Practices must be able to demonstrate a thorough and up-to-date understanding of the risks posed to it by clients, the likelihood of the risk becoming a reality (ie of identifying money laundering and terrorist financing) and the impact on the Practice of it occurring. The assessment will change depending on how circumstances develop and threats evolve. Each change must be recorded.
- b) Practices will be encouraged to achieve outcomes aimed at reducing money laundering and terrorist financing, rather than concentrating on detailed compliance with prescriptive rules.
- c) Practices will not always be able to eliminate money laundering – the CLC will consider what reasonable steps a particular Practice can reasonably be expected to take to prevent money laundering and terrorist financing.
- d) Practices will be expected to have documented policies, procedures and systems in place that are being effectively applied and subject to appropriate quality assurance testing. The CLC will apply a range of proportionate measures to ensure that Practices comply with these expectations.

2.7 It follows that, as a result of adoption of a risk-based approach, a Practice’s AML/CTF systems and controls can be different even within one sector or among comparable firms. The risk-based approach to AML means that there may be more than one “right” answer to the same problem,

2.8 There are some situations when a risk-based approach cannot be taken – ie for the statutory requirements under POCA and TACT not to engage in certain activities and to make SARs when knowledge or any actual or reasonable suspicion is formed.

2.9 Factors for Practices to take into account in applying a risk-based approach are:

- a) Probability: the intrinsic risk associated with the activity undertaken by the Practice, which can vary depending on other indicators:
 - i. Product and service risk (likelihood that products or services on offer can be used for laundering money)
 - ii. Client risk (likelihood that clients' funds may have criminal origins)
 - iii. Geographical risk (does the Practice trade, or with clients, in locations that might pose greater risks?)

- b) Impact: The potential harm that could be caused to the Practice should it be implicated in money laundering and terrorist financing:
 - i. Firm size (turnover, number of clients, number of premises, etc.)
 - ii. Links with other businesses (susceptibility of the Practice being involved inadvertently in 'layering' activity).

2.10 In summary, the Regulations state that regulated businesses will need to be able to demonstrate to their Supervisory Authorities (in this case the CLC) how they have determined their money laundering and terrorist financing risks, that the steps they have taken to manage those risks are reasonable and appropriate in the light of that determination, that the strategy has been approved by those who control the business (i.e. the Principals) and that there is a regular review of the assessment process and strategy.

Regulatory expectations and role of CLC

2.11 In the chapters which follow, the Guidance spells out what CLC expects of Practices in order to meet AML/CTF requirements. These expectations will generally form the basis on which the CLC will fulfil its supervisory function and provide the standards against which it will assess compliance in line with Government expectations.

2.12 All existing Practices should already have systems and controls in place under the 2003 Regulations and the earlier CLC Guidance. However, all Principals must now consider what additional methods, systems and controls they need to introduce to reflect the enhanced regulatory requirements under the new Regulations. This is particularly the case in areas where the obligations have been extended (e.g. CDD measures, ongoing monitoring).

2.13 In so doing, a Practice must always bear in mind:-

- that those seeking to launder the proceeds of crime or finance terrorism may target it and the services it offers;
- of the ways in which those services may be abused to further criminal intentions and achieve money laundering and terrorist financing objectives; and
- that a Practice may be in breach of the requirement to report even if it does not know or suspect money laundering or terrorist financing (the subjective test) if it should reasonably have had that knowledge or suspicion (the objective test).

2.14 Principals must take reasonable steps to ensure that neither they nor their staff commit any offences and that they all fulfil their positive reporting and other obligations. They must be familiar with the law and the requirements of the Regulations and adopt a risk-based

approach in taking all necessary steps to ensure that there is compliance with the Regulations.

Status of Guidance in any Court action

- 2.15** Having drawn up this Guidance as the Supervisory Authority for the profession of Licensed Conveyancers, the CLC may submit it to HM Treasury for approval, either in its current or in an amended form. A court is likely to take guidance into account (even if it has not had HM Treasury approval) in considering whether or not an offence has been committed under the AML/CTF legislation.

Role of Supervisory Authorities

- 2.16** The CLC is designated as the Supervisory Authority for the profession of Licensed Conveyancers. Similar arrangements will exist throughout the regulated sector.
- 2.17** The CLC is required to monitor Licensed Conveyancers effectively and to take necessary measures (which may include disciplinary sanctions) to ensure that they comply with the Regulations. If a Supervisory Authority forms any suspicion that a person for whom it is responsible has engaged in money laundering or terrorist financing, it is under a duty to make a disclosure report to SOCA.
- 2.18** Guidance Note 10 provides that the CLC will take into account (a) the adequacy of the arrangements made by any Practice and (b) whether it has followed the provisions of the Guidance Note and this Guidance when considering whether there has been a breach of the Council's Rules.

Dual Supervision

- 2.19** A Licensed Conveyancer employed by a firm of solicitors will be primarily expected to comply with the AML Practice Note issued by the Law Society at www.lawsociety.org.uk. The CLC will liaise with the Solicitors Regulation Authority (or other supervisory authority) before determining how a disciplinary complaint against a Licensed Conveyancer should be investigated.

Enforcement Powers under the Regulations

- 2.20** There are a variety of powers given to designated authorities under Part 5 of the Regulations for use in connection with the regulatory functions, including the imposition of civil penalties for non-compliance. HM Treasury has stated that these powers are limited for use by those authorities in their role as supervisors for the relevant persons that they supervise (ie the CLC in respect of Licensed Conveyancers). The relevant powers are found in Regulations 36 – 41.
- 2.21** If an officer of a designated authority (other than the CLC) seeks to exercise the compliance powers under these Regulations, a Practice may wish to require the production of a warrant or Court Order under Regulations 39 – 40 to protect itself against proceedings for breach of its duty of confidentiality. The Court has power under Regulation 40 to order the costs of the applicant to be paid by the defaulter.

Offences and Penalties

- 2.22** A Licensed Conveyancer may be prosecuted for failure to comply with the AML and CTF requirements. Details of the offences and the relevant penalties are contained in Chapter 11 (page 70), and where relevant in chapters 3 to 10.

CHAPTER 3 - SYSTEMS AND CONTROLS

The Requirements of the Regulations

A Practice must have in place Policies and Procedures (Regulation 20(1)) to cover:

(a) specific requirements for:-

- a Nominated Officer to be appointed – Regulation 20(2)(d)(i)
- Education and training on AML/CTF to be provided – Regulation 21
- CDD Measures and Ongoing Monitoring to be in place – Regulations 5-9 and 13-14;
- both Internal and External Reporting – Regulation 20(2)(d)(ii) and (iii) and Part 7 of POCA and Part 3 of TACT
- Record keeping - Regulation 19

(b) general requirements for:-

- Internal control;
- Risk assessment and management;
- Compliance monitoring and management; and
- Internal communication of such policies and procedures.

Policies must exist and be communicated. Staff must be made aware of the law relating to money laundering and terrorist financing and be given regular training in how to recognise and deal with activities which may be related to money laundering or terrorist financing.

CLC Expectations

3.1 A Practice must have clearly documented systems and controls in place which enable it to:-

- take a risk-based approach in managing the threat of money laundering and terrorist financing;
- place specific AML and CTF accountabilities and responsibilities on the Principals, Directors, senior management, the Nominated Officer (and any MLRO) appointed and other relevant staff of the Practice;
- produce clear written Client Acceptance Policies for taking on business and instructions from new and existing clients, with particular reference to higher risk situations (e.g. dealing with non face-to-face clients and PEPs);

- identify and scrutinise complex or unusually large transactions, unusual patterns of transactions which have no apparent economic or lawful purpose and any transactions which might favour anonymity ;
- apply CDD measures to any client or beneficial owner, and ongoing monitoring of any business relationship and transactions undertaken;
- apply EDD measures and enhanced ongoing monitoring of transactions and relationships which present a higher risk of money laundering or terrorist financing (Regulation 14);
- ensure that procedures are implemented and reviews are carried out regularly to monitor the implementation and operation of all AML and CTF systems and controls;
- produce evidence of such systems and controls and the operation of such systems and controls to the CLC on request; and
- co-operate with the CLC to improve its systems and controls.

3.2 In addition a Practice must:-

- devise and implement appropriate systems and controls based on its own assessment of its risks and vulnerabilities (Chapter 3);
- appoint a Nominated Officer (Chapter 4, page 21);
- provide education and training to all management and staff (Chapter 5, page 25);
- apply CDD measures in determining and obtaining confirmation of the true identity of all clients and any beneficial owner (as defined by Regulation 6);
- understand the nature of the business that any client expects to conduct through the Practice and the rationale for the business relationship and retainer being formed between the Practice and the client concerned;
- ensure that all CDD information is accurate, relevant and up-to-date;
- conduct ongoing monitoring of any business relationship and where appropriate or as required by the Regulations, carry out EDD of a business relationship or occasional transaction and enhanced ongoing monitoring (Chapter 6, page 29);
- provide clear written internal reporting procedures for its staff (Chapter 7, page 52);
- facilitate the processing of internal reports by the Nominated Officer without hindrance or undue influence and without giving rise to any fear or favour (Chapter 8, page 55);
- enable reports to be made to SOCA (Chapter 9, page 58); and
- keep all required CDD and other transaction records for the periods prescribed by the Regulations (Chapter 10, page 64).

Practical Considerations

General

- 3.3** Each Practice must manage its money laundering and terrorist financing risks in the wider context. This is most likely to be achieved by a set of effective and proportionate systems and controls incorporated into its business strategy based on a principled rather than a tick-box approach.

Documentary Evidence

- 3.4** All systems, controls, procedures and policies must be clearly documented and capable of being produced on request.
- 3.5** It is recommended that a Practice's AML/CTF policy is relevant to the business of the Practice and written in terms that will be easily understood and followed by all staff. There is no "one size fits all" policy. The systems and controls adopted will depend on the number of employees, the nature and range of services, and the type, nature and source of its clients. The CLC AML Toolkit, primarily aimed at a small Practice, is a useful starting point.

Exceptions

- 3.6** There are limited exceptions to the regulatory requirements.
- 3.7** Sole Practitioners with no employees are not required to appoint a Nominated Officer or have procedures for the internal reporting and the training of staff, but other policies and procedures must still be documented and implemented.

New Key Area Requirements

- 3.8** A Practice will need to develop and expand its policies and procedures to include CDD measures, ongoing monitoring, EDD measures and enhanced ongoing monitoring (Chapter 6, page 29). Other pre-existing requirements have been enhanced.

Policies for accepting instructions

- 3.9** The following examples of higher-risk criteria can be taken into account in developing policies and procedures for accepting clients:
- (a) clients who are not met on a face to face basis for the purpose of CDD measures;
 - (b) corporate structures, e.g. trusts where knowledge of the identity of the true underlying beneficial owners or controllers cannot be guaranteed;
 - (c) private limited companies;
 - (d) relationships where there is any form of delegated authority in place, e.g. powers of attorney.

- (e) those individuals defined as PEPs, members of their families and known close associates, or those previously known to be involved with terrorist organisations.
- 3.10** In all cases, a “Beneficial Owner” (Regulation 6) will need to be identified and verified (Chapter 6, page 41).
- 3.11** The geographical location of clients and their business activities will also affect the AML/CTF risk analysis.
- 3.12** Significantly greater risks are posed by clients who are located in countries:
- (a) without adequate anti-money laundering strategies;
 - (b) which have been seen to support or be associated with terrorist activities;
 - (c) where there is a politically unstable regime with high levels of public or private sector bribery and corruption;
 - (d) that are known to be drug-producing or drug-transit countries; or
 - (e) that have been classified as NCCTs.
- 3.13** Such clients will need to be subjected to EDD measures (eg additional CDD measures) and enhanced ongoing monitoring to manage the enhanced risks of money laundering and terrorist financing (Chapter 6, page 35).
- 3.14** The following range of questions might be asked before accepting instructions:-
- Are the client’s intentions logical in relation to the conveyancing services offered by the Practice?
 - Is there a logical reason for the client to use the particular Practice for his business?
 - Is the client acting on his own behalf or for another party and, if so, does the Practice know the third party and the nature of the relationship between the other party and the “client”?
 - Does the Practice fully understand the nature of the business that the client intends to transact?
 - Does the Practice fully understand the source of funds to be used to fund the services requested?
 - Is there any geographical or other risk that will affect the decision to accept instructions?
 - Are there any other additional risks inherent within this business (eg non face-to face contact, a PEP or a complex or unusual circumstances risk)?
 - What additional CDD or EDD or enhanced ongoing monitoring might be required to satisfy the Regulations and the Supervisory Authority
- 3.15** A Practice may have internal controls that require a higher risk client or a higher risk transaction to be approved by a manager.

Home Information Packs

- 3.16** The Regulations do not apply to a person who prepares a Home Information Pack before the marketing of a property or any document or information for inclusion in such a Pack (Regulation 4(1)(f)). CDD measures will not need to be applied at the pre-marketing stage, but will need to be covered once a buyer has been found if the seller instructs the Practice to act on the sale.

•

Responsibility and Accountability

- 3.17** Sole Practitioners, Partners, Directors and senior management need to accept full responsibility for all areas of compliance and ensure that:

- sufficiently robust measures are implemented to protect them against the risk of money laundering and terrorist financing and the prospect of criminal or disciplinary sanctions, and
- staff are made aware of their responsibilities for their actions.

- 3.18** They need to:

- engage consistently and regularly with the Practice's AML/CTF policies and procedures to ensure that the systems and controls are working well;
- provide leadership to establish a positive culture for the AML/CTF process;
- maintain close contact with any MLRO to make strategic decisions about ongoing AML/CTF activity; and
- equip themselves (and be willing) to make key decisions about how the Practice should deliver a risk-based approach.

Penalties

- 3.19** A Licensed Conveyancer who fails to comply with AML/CTF obligations may be prosecuted. The standard penalty tariff for contravening the Regulations (Regulation 45) is:

- on summary conviction, a fine not exceeding the statutory maximum; and
- on conviction on indictment, imprisonment for a term not exceeding 2 years or a fine.

- 3.20** Anyone working in the regulated sector (including a Licensed Conveyancer and member of staff in a Practice) who fails to make an internal report to a Nominated Officer or any Nominated Officer who fails to make an external report to SOCA in relevant circumstances will be liable:-

- on summary conviction, to imprisonment for a term not exceeding 6 months or a fine not exceeding the statutory maximum or both (money laundering and terrorist financing) ; and
- on conviction on indictment, to imprisonment for a term not exceeding 5 years for money laundering (and not exceeding 14 years for terrorist financing) or a fine or both.

CHAPTER 4 NOMINATED OFFICER

The Requirements of the Regulations and of CLC Guidance

Regulation 20(2)(d)(i) requires every relevant person to include a specific policy and procedure among the appropriate and risk-sensitive policies established and maintained under Regulation 20(1) which require an individual in the relevant person's organisation to be nominated as a Nominated Officer for the purpose of Part 7 of POCA and Part 3 of TACT to receive internal disclosures.

Under Regulation 20(3) a Nominated Officer does not need to be appointed where the relevant person is an individual who neither employs nor acts in association with any other person (i.e. a sole principal with no employees).

A relevant person who breaches this requirement will be guilty of an offence to which the standard penalty tariff applies.

In addition, Paragraphs 6(b) and (c) of CLC's Guidance Note 10 – Anti Money Laundering require a Practice to:-

- appoint a Senior Manager (who may or may not be the Nominated Officer) with responsibility for ensuring the Practice's compliance with AML and the Guidance Note and
- ensure that the Senior Manager so appointed has an appropriate level of authority and independence within the Practice and access to resources and information sufficient to enable him to carry out that responsibility.

CLC Expectations

- 4.1 A Practice must appoint a Nominated Officer unless the Practice is a sole principal with no employees (Regulation 20(3)). A Deputy should normally be appointed. If the position of Nominated Officer falls vacant, a Practice must immediately appoint another suitable person as its Nominated Officer.
- 4.2 The Nominated Officer (and any Deputy) must work within the Practice.
- 4.3 A Practice must notify the CLC on request of the name and status of their Nominated Officer (and of any Deputy Nominated Officer). In addition, a Practice must advise the CLC on request of the name and status of the Senior Manager appointed under Paragraph 6(b) of Guidance Note 10 (see above) and/or any other person appointed as MLRO to oversee its AML and CTF compliance. If the Nominated Officer or the Senior Manager or MLRO is changed, the CLC must be informed within 14 days of the new appointment.

Practical Considerations

The role and duties of the Nominated Officer

- 4.4 A Nominated Officer is the person within a business nominated to receive internal disclosures of actual or suspected money laundering arising from its business activities. He acts as a filter to assess all internal reports and to decide whether a SAR (Suspicious

Activity Report) should be made to SOCA. His role is therefore crucial under the Regulations and in the fight against money laundering and combating terrorist financing.

- 4.5** The Nominated Officer will also be responsible for liaising with SOCA or law enforcement agencies on the question of whether or not to proceed with any particular instructions or retainer, on what steps may be taken once a disclosure has been made and what information (if any) may be disclosed to clients or third parties in such circumstances.
- 4.6** The Nominated Officer need not pass on intelligence which provides no actual or reasonable grounds for suspicion of money laundering or terrorist financing. However, if he fails to make an external report in circumstances which warrant one being made, a Nominated Officer will be guilty of an offence under either s.331 POCA or s.21A TACT. On conviction on indictment the maximum term of imprisonment is 5 years (money laundering) or 14 years (terrorist financing) or a fine or both. On summary conviction, the maximum term is 6 months' imprisonment and/or a fine, subject to the statutory maximum.
- 4.7** It is suggested that a Deputy is appointed to cover absences (e.g. annual leave, sickness, etc.). The appointment of a Deputy may also help in sharing responsibility and will also be particularly relevant when planning for succession. The experience gained in the deputy role (e.g. in learning the suspicion evaluation process) should be invaluable to both the individual involved and to the Practice.

Nomination Criteria

- 4.8** The Nominated Officer (and any Deputy) must work within the Practice or within the same group of Practices and should be either a Principal or someone else employed at a senior level as part of the senior management team.
- 4.9** To be able to carry out his responsibilities effectively, the Nominated Officer must:-
- (a) be resident in the UK;
 - (b) hold a sufficient level of seniority, authority and independence in the Practice to enable him to have access to all client files and records and other sources of relevant information held by the Practice so that he is able to make the necessary decisions on the basis of all the information held by the Practice;
 - (c) be given the full support of management;
 - (d) have sufficient resources, including sufficient time and training and, if considered appropriate, a Deputy Nominated Officer to assist him and an appropriate level of support staff;
 - (e) be fully aware of the AML and CTF obligations and the policies and procedures applying to the Practice for which he is appointed.
- 4.10** In view of the significance of his role, he must be allowed to fulfil his regulatory responsibilities with full autonomy and should hold the trust and confidence of all Principals and staff. His decisions must not be subject to the consent or approval of anyone else.
- 4.11** Sufficient seniority is an important consideration since the Nominated Officer will need to make decisions on reporting which can impact on the business relationships of the Practice with its clients and the exposure to criminal, civil, disciplinary and reputational sanctions.

- 4.12** A Licensed Conveyancer even if he practises as a sole practitioner must appoint either himself or a senior member of staff as Nominated Officer if he employs any staff, since he will not come within the exception under Regulation 20(3).

The wider role of a Money Laundering Reporting Officer (MLRO)

- 4.13** A member of the senior management team must be appointed (Paragraph 6(b) of Guidance Note 10) to have specific responsibility for AML/CTF compliance, although statutory responsibility remains with the owners and controllers. For convenience the term MLRO is used to describe this role.

- 4.14** The responsibilities of an MLRO normally include some or all of the following:-

- (a) developing and maintaining the AML/CTF policies and procedures for the Practice on a risk-based approach;
- (b) undertaking, in consultation with senior management, the required money laundering and terrorist financing risk assessment of the business conducted by the Practice, on at least an annual basis;
- (c) ensuring that all staff within the Practice (whether employed or engaged on a self-employed basis) are aware, through regular adequate training, of their personal obligations and the internal policies, procedures and controls relating to money laundering or terrorist financing
- (d) undertaking and controlling the internal review of all knowledge and suspicions in the light of all available CDD and EDD and ongoing monitoring information and determining whether or not such suspicions have substance and require disclosure to SOCA;
- (e) ensuring that client and other related relationships are managed after a disclosure has been made to avoid tipping off;
- (f) acting as the liaison point with the CLC and SOCA and in any other third party enquiries in relation to money laundering and terrorist financing prevention, investigation or compliance;
- (g) ensuring that all parts of the Practice are complying with its policies and procedures and monitoring the operation and development of the policies and procedures to that end;
- (h) undertaking or arranging regular money laundering compliance reviews;
- (i) advising the Principals of compliance issues that need to be brought to their attention;
- (j) obtaining and using information concerning (i) NCCTs, (ii) those countries against which HM Treasury may have issued prohibition notices and (iii) the names of sanctions targets included in the consolidated Sanctions List maintained by HM Treasury Asset Freezing Unit (www.hmtreasury.gov.uk/financialsanctions);
- (k) responding promptly to any requests for information made by the CLC, SOCA or law enforcement agencies; and

- (l) ensuring the proper recording of information and its retention to facilitate the formation and establishment of audit trails.
- 4.15** If any or all of these responsibilities are not delegated, the Principal(s) of the Practice will need to assume direct responsibility for fulfilling these responsibilities, other than 4.14(d), (e) and (k) which are the responsibility of the Nominated Officer and 4.14(f) which will be a dual responsibility shared by the Principal(s) and the Nominated Officer.
- 4.16** Ultimately, of course, the Principals of the Practice remain responsible for compliance and have a duty to monitor and assess the level of internal compliance and the performance of any MLRO or Nominated Officer appointed (by, for example, the use of internal audit procedures or through an internal compliance department, if available).

CHAPTER 5 - EDUCATION AND TRAINING

Requirements of the Regulations

A relevant person must take appropriate measures (Regulation 21) so that all relevant employees of his are:-

- (a) made aware of the law relating to money laundering and terrorist financing; and
- (b) regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

A relevant person who breaches the training requirements will be guilty of an offence.

An employee within the regulated sector charged under POCA for failure to report has a statutory defence (s.330(7) POCA) where that employee

- does not know or suspect that another person is engaged in money laundering, and
- has not been provided with anti-money laundering training as specified under the Regulations by his employer.

If that defence is successful, the Principals may be prosecuted for breach of their training obligations. Currently, there is no equivalent defence under TACT.

CLC Expectations

5.1 Practices must take appropriate measures to ensure that all relevant employees are aware of:-

- the money laundering offences contained in Part 7 of POCA and the terrorism offences contained in the Part 3 of TACT and the requirements of the Regulations and any other amending legislation;
- the likely effect of any breach of that legislation or the Regulations;
- AML/CTF practices and procedures adopted by the Practice including the importance of the CDD and EDD requirements, how to make internal reports and the responsibilities of the Nominated Officer.

5.2 Employees must receive regular training.

5.3 Based on general industry guidance, the obligation at 5.2 will be taken to mean the provision of a continuing training programme which keeps everyone working within the Practice

- up-to-date with trends and changes in the patterns and types of schemes and devices used to launder money and finance terrorism to aid recognition, and
- enable them to handle transactions once any such elements are recognised

on a basis which is appropriate to their position within the Practice.

- 5.4 For review and continuing training purposes, an up-to-date central record of the training undertaken by every member of staff must be kept and should be reviewed and monitored on a regular basis. It must be supplied to the CLC on request.

Practical Considerations

Training Strategy

General

- 5.5 It is important for each Practice to devise a training strategy which will deliver a training programme for all staff and that the training is provided at appropriate levels for the individual members of staff concerned, including Principals. The risk-based approach suggests that those with fee-earner status or working in an Accounts Department will need fuller training on the law and on the recognition of suspicious transactions and activities.
- 5.6 Frontline staff including Telephonists, Receptionists and Secretaries may need specific training in how to handle enquiries so as not to alert the client or any third party to the fact that a disclosure report has been made and avoid the dangers of “tipping-off”.
- 5.7 Awareness-raising and training should cover not only the need to know the true identity of the client and any beneficial owner but also the need to know enough about the activities expected in relation to that client or beneficial owner so as to know what might constitute suspicious activity and the circumstances that would give rise to reasonable grounds for suspicion [See Chapter 6, page 29].

Induction

- 5.8 Induction training in money laundering prevention, combating terrorist financing, recognition and reporting of suspicions and the CDD and EDD requirements is important and should be given as a starting point to anyone. This should be at a relevant level at the start of their employment in any role which might expose them to the risk of AML and CTF.

Continuing Training

- 5.9 Any education and training programme should be progressive. It should take account of any developments in the money laundering and terrorist financing fields and any change in the policies and procedures of the Practice. The content and frequency should reflect the ongoing risk assessment of the services provided by the Practice. The training supplied should be stimulating, well-communicated and provided in context as a work-related process.

Training Delivery

- 5.10 A Practice should consider incorporating its AML/CTF training within the overall training strategy for employees and Principals.
- 5.11 All AML/CTF arrangements must relate to the level of risk and so those made in respect of awareness and other training should be no different and ought to reflect and relate to the levels of risk within the particular Practice. The level of risk will fluctuate, reflecting the types services, clients and employees of the Practice. The levels and degrees of training may need to be varied from time to time.

Core Obligations

5.12 The core obligations and considerations are that:-

- Principals are ultimately responsible for ensuring that adequate training arrangements are in place although, if an MLRO is appointed, they may devolve all or part of that responsibility to him;
- All staff must be made aware of the risks of money laundering and terrorist financing, the relevant legislation and their obligations under that legislation;
- Relevant staff must be made aware of how the services offered by the Practice may be abused as a vehicle for money laundering or terrorist financing and of the procedures adopted by the Practice for managing that risk;
- Relevant staff need to be trained in how to operate a risk-based approach to AML/CTF and how to recognise and deal with potential money laundering or terrorist financing transactions;
- Staff must be made aware of the identity and responsibilities of the Practice's Nominated Officer or MLRO, of the need to report knowledge or suspicion and of the impact of failing to do so;
- Staff need to be supplied with information about the legal position of the Practice and of its individual members of staff and when changes in those positions occur;
- Staff training must be given regularly. The frequency and content of the training should reflect the risk assessment of the services provided by the Practice and the role of the individual within the Practice;
- Details of all training undertaken must be recorded;
- Training needs and requirements must be kept under regular review to provide relevant ongoing training to maintain staff awareness of money laundering and terrorist financing issues including how these crimes are operating and developing and how such developments might have an impact on the Practice.

Types of Training

5.13 To meet their obligations under the Regulations, Practices might consider one or more or a combination of the following:-

- Insertion of relevant information into existing procedure manuals, although a separate summary document covering the AML and CTF procedures might be helpful;
- The preparation of a Money Laundering Handbook for management and staff to provide all relevant information about the legislation and the policies and procedures of the Practice setting out the procedures for taking on clients and new business, the CDD and EDD measures to be applied and the internal reporting procedures;

- An awareness-raising booklet, supported by in-house familiarisation sessions, for staff who may not need to be informed of the detail of the law and the Practice's policies and procedures (other than for the internal reporting obligations);
- Delivery of information electronically;
- E-learning;
- External training courses;
- Dedicated in-house training sessions;
- Provision of updates on developments, case studies and examples in money laundering and terrorist financing methods and techniques to relevant staff with information on how they might impact on the business of the Practice.

5.14 Practices should be committed to advancing and maintaining the AML/CTF competences within their business and to ensure that all are properly equipped to fulfil their respective roles and that adequate supervision of the attainment and maintenance of that competence is provided through training development.

Records

5.15 To minimise the risk of prosecution for failure adequately to train staff, it is important for the Practice to ensure that:

- training for all relevant employees is mandatory;
- a central record is kept of the date and specific nature of the training that has been given; and
- regular reviews are undertaken to assess competency levels, the effectiveness of training and the nature of additional training requirements.

Defences

5.17 A member of staff has a defence to a charge of failing to report if he has not received appropriate training from his employer (s.330(7) POCA). A successful defence may lead to prosecution of a Practice for failing to provide AML/CTF training (Regulation 21).

CHAPTER 6 - CUSTOMER DUE DILIGENCE

Requirements of the Regulations

Under Regulation 7(1), a relevant person must carry out Customer Due Diligence measures on a “risk-sensitive basis” (i.e. with a risk-based approach) before instructions are accepted whenever he:

- establishes a business relationship, or carries out an occasional transaction amounting to €15,000 or more;
- suspects money laundering or terrorist financing,
- doubts the information previously obtained for client identification,

and, under Regulation 7(2), as part of ongoing monitoring during the course of a transaction.

CDD means identifying and verifying the identity of a client and any beneficial owner and obtaining information on the purpose and intended nature of the business relationship (Regulation 5).

A beneficial owner (Regulations 2 and 6) owns or controls the client or is the person on whose behalf the transaction is being carried out. A beneficial owner includes any person with at least 25% ownership or control of an entity.

Under Regulation 14, Enhanced Customer Due Diligence (EDD) measures and enhanced ongoing monitoring must be applied with a risk-based approach where:

- the relevant person does not meet the client
- the client is a politically exposed person, and
- there is a higher risk of money laundering or terrorist financing.

It is an offence to breach any of these provisions.

CLC Expectations

6.1 The purpose of the Regulations is to ensure that:

- at the outset of a transaction (whether as part of a business relationship or as an occasional transaction), by the application of CDD or EDD processes:-
 - every client is identified and the Practice holds adequate evidence of that identity;
 - every beneficial owner is identified and that identity is checked;
 - steps are taken to understand the ownership and the control structure of a person, trust or arrangement;
 - information is obtained about the purpose and intended nature of the proposed business relationship with any client;
- ongoing monitoring of the relationship with the client is undertaken as any transaction or transactions proceed;

- additional checks and verification (EDD) are applied in any higher risk situations. This applies in particular to the specific circumstances outlined in Regulation 14 – i.e. for clients dealt with remotely and clients who are PEPs (or their family members or known close associates) – or otherwise in any situation which by its nature can present a higher risk of money laundering or terrorist financing. Enhanced ongoing monitoring of the business relationship with this group should be carried out as any transaction or transactions proceed.
- 6.2** Every Practice must make sure that it has documented policies and procedures with which it complies dealing with:
- CDD and EDD procedures, applied with a risk-based approach. These should include situations where satisfactory evidence of identity or satisfactory replies to CDD and/or EDD enquiries cannot be obtained,
 - keeping client information up-to-date for existing clients and business relationships,
 - identification and verification issues for those who cannot produce standard evidence so that no prospective client is unreasonably denied access to the services of the Practice (Paragraph 5(f) of Guidance Note 10 – Anti Money Laundering),
 - the making of internal reports.
- 6.3** A Practice must not act or continue to act until the requirements for all CDD and any EDD have been met. If these cannot be met, a Practice must:
- not establish a new business relationship; or
 - terminate any existing business relationship; or
 - not allow any occasional transaction to proceed further; and
 - consider whether a SAR should be made (Regulation 9(3)).

Practical Considerations

- 6.4** The purpose of this part of the Regulations is to make sure that a Practice does not act for a client if it does not know that client or that client's business. In order to achieve this, a Practice must apply Customer Due Diligence (CDD) measures (or Enhanced Customer Due Diligence (EDD) measures in riskier situations). There is a further requirement for the Practice to keep its initial investigations about its clients up to date through ongoing monitoring.
- 6.5** This sounds relatively straightforward and entirely consistent with sound business practice. But Practices will already be aware (from the earlier Know your Client requirements) that what constitutes proof of identity varies with the type of client. This Chapter may appear to have a daunting amount of detail in it, but it is provided to give practical help to Licensed Conveyancers in meeting their obligations.
- 6.6** The outcome of a Practice carrying out CDD and EDD should be that it is reasonably satisfied that its clients are who they say they are and that it can:-
- know with some certainty whether or not it is acting on behalf of another (called a beneficial owner);

- establish that there is no bar to providing the services requested;
- assess whether the purposes of the instruction is consistent with the lifestyle and economic means of the client and;
- establish that there are no obvious elements which suggest that any transaction is unusual or over-complex in the context of those instructions;
- assist law enforcement by providing information about clients or activities which may be being investigated at the time or later.

Guide to the rest of this Chapter

6.7 The guide below is aimed to help a Practice navigate its way around the rest of this chapter or to go directly to a particular section dealing a specific type of client it needs to check on.

Clarifying some underlying principles	page
Business relationship of occasional transaction	32
Beneficial ownership	32
A risk-based approach	33
What's involved in CDD/EDD?	
Verification of identity	34
EDD	35
Remote identification	35
Politically exposed Persons (PEPs)	36
Other CDD measures	37
Simplified Due Diligence	38
Reliance	38
Default of delay by clients	38
Ongoing monitoring	
Within a business relationship	39
For existing clients	39
What counts as identity and verification?	
For a private individual	40
For a beneficial owner	41
What evidence is required?	
Individuals (UK and non-UK residents)	42
Evidence for UK residents	42
Evidence for non-UK residents	44
Unincorporated businesses/partnerships	45
Corporate clients	45
Public registered companies (UK and non-UK)	46
Private companies	46
Trust vehicles	47
Deceased person's estates	47
Other legal entities and arrangements	48
Foundations	48
Charities and other bodies	48
Clubs and associations	49

What form should the evidence take?

Paper-based evidence	49
Electronic checks	50

Clarifying some underlying principles**Business Relationship or Occasional Transaction?**

- 6.8** The Regulations distinguish between a “business relationship” and an “occasional transaction”.
- 6.9** A Practice dealing with property transactional work is more likely to be forming a business relationship with a client because it is likely to have an element of duration, a number of elements (e.g. purchase, a new mortgage, mortgage redemption, declarations of trust, sale and possibly wider elements of advice), and the potential for extension.
- 6.10** A Practice is likely to be instructed on an “occasional transaction” where advice is given or action is taken on a one-off basis (e.g. advice given to a third party on a bank guarantee or advice given on a property-related matter on an isolated basis) where there is not expected to be a continuing relationship which can be subject to ongoing monitoring. In some circumstances, the giving of advice may constitute the establishment of a business relationship if further contact is possible.
- 6.11** For property transactional work, it will be a question of fact and degree, to be determined by the Practice in each case, as to when the business relationship actually ends.
- 6.12** Where it appears that the consideration for an occasional transaction (or series of linked transactions) is less than €15,000 (in which case CDD and EDD do not apply), it is advisable for a Practice to check the official exchange rate against the Official Journal of the European Communities.
- 6.13** A Practice may determine as a matter of policy that each transaction should be treated as a “business relationship” to avoid the possibility that a “business relationship” may be wrongly identified as an “occasional transaction”.

Beneficial Ownership

- 6.14** Where a Practice’s customer is not a private individual, the identity of the beneficial owner of that customer must be established. In the broadest terms, the beneficial owner is the individual who ultimately owns or controls the client on whose behalf a transaction is being conducted.
- 6.15** The beneficial ownership verification requirements mean that a Practice must establish (i) who owns (directly or indirectly) 25% or more of the structure and (ii) who exercises the effective management and control of the structure and therefore dictates the way it operates and its business activities.
- 6.16** Regulation 5(b) applies similar general principles to checking and verifying the identity of beneficial owners as for private individuals. However, in this situation, the specific requirement is to take adequate risk-based measures to verify that identity so that the Practice is satisfied that it knows who the beneficial owner is. This means understanding the ownership and control structure of the natural or legal person, trust, entity or other arrangement involved.

- 6.17** Less transparent and more complex structures are likely to pose a higher money laundering or terrorist financing risk, particularly if any overseas element is linked to a country or jurisdiction which has lower or no national compliance with the international FATF standards. A Practice may have reason for concern or suspicion where it is asked to act for a client which has a complex structure with an intricate beneficial ownership framework.
- 6.18** If it is unable easily to understand the ownership structure of a client, a Practice may consider referring to other guidance, such as the JMLSG Guidance or to the AML Practice Note issued by the Law Society which contains examples of beneficial ownership under a trust in Chapter 4. The Practice may wish to take independent legal advice as to whom or what may constitute a “beneficial owner” in any particular case, or it may decide not to act.
- 6.19** A Practice which already acts for or is likely to act for clients with complex beneficial ownership structures, may consider applying EDD measures similar to those for higher risk clients and transactions, and providing specific training for designated members of staff.

A risk-based approach to CDD

- 6.20** Practices are expected to take a risk-based approach in deciding the extent of CDD measures to be applied at the outset of a transaction and then on an on-going basis. The following are examples of higher-risk criteria for Practices to take into account in making those decisions:
- (a) clients who are not met face to face for the purpose of CDD measures;
 - (b) corporate structures, e.g. trusts where knowledge of the identity of the true underlying beneficial owners or controllers cannot be guaranteed;
 - (c) private limited companies;
 - (d) relationships where there is any form of delegated authority in place, e.g. powers of attorney.
 - (e) those individuals defined as PEPs, members of their families and known close associates, or those previously known to be involved with terrorist organisations.
- 6.21** The geographical location of clients and their business activities will also affect the AML/CTF risk analysis. Significantly greater risks are posed by clients who are located in countries:
- (a) without adequate anti-money laundering strategies;
 - (b) which have been seen to support or be associated with terrorist activities;
 - (c) where there is a politically unstable regime with high levels of corruption;
 - (d) that are known to be drug-producing or drug-transit countries; or
 - (e) that have been classified as NCCTs.

- 6.22** Such clients will need to be subjected to additional CDD measures or EDD measures to manage the enhanced risks of potential money laundering and terrorist financing (page 35).
- 6.23** The following range of questions might be asked before accepting instructions:-
- Are the client's intentions logical in relation to the conveyancing services offered by the Practice?
 - Is there a logical reason for the client to use the particular Practice for his business?
 - Is the client acting on his own behalf or for another party and, if so, does the Practice know the third party and the nature of the relationship between the other party and the client?
 - Does the Practice fully understand the nature of the business that the client intends to transact?
 - Does the Practice fully understand the source of funds to be used to fund the services requested?
 - Is there any geographical or other risk that will affect the decision to accept instructions?
 - Are there any other additional risks inherent within this business (e.g. a PEP or a complex or unusual circumstances risk)?
 - What additional CDD or EDD or ongoing monitoring might be required to satisfy the Regulations and the Supervisory Authority?
- 6.24** A Practice may have internal controls that require a higher risk client or a higher risk transaction to be approved by a manager.

What's involved in CDD and EDD?

Verification of Identity

- 6.25** The identity of all persons for whom a Practice will act (including those where a beneficial owner is involved) must be verified at the outset of instructions.
- 6.26** "Identification" is the process of identifying details about a person whilst "verification" is obtaining evidence supporting the identity claimed.
- 6.27** For more details of what counts as identity and verification, see page 40; for the evidence required, see page 41.
- 6.28** In certain higher-risk situations, greater checks on identity will be required – see Enhanced customer Due Diligence Measures page 35.

- 6.29** All evidence of identity must be kept up-to-date. This may be particularly relevant where a Practice acts for a client on a regular basis where after a period evidence of identity held by the Practice may no longer be applicable.

Enhanced Customer Due Diligence Measures

- 6.30** Enhanced checks (EDD) must be made in any situation which by its nature can present a higher risk of money laundering or terrorist financing. In addition, the Regulations identify two specific examples where EDD must be carried out:
- where the client has not been physically present for identification purposes; or
 - where the client is a PEP, including any family members and known close associates.
- 6.31** These categories are not exclusive. Based on information publicly available and its own knowledge and experience, a Practice will need to make its own risk-based assessment as to which types of client, situation, circumstance and transaction may present a higher risk.
- 6.32** It is for the Practice to decide the extent of the additional information required and of any enhanced ongoing monitoring for any particular client, type of client or transaction based on the perceived risk.
- 6.33** In principle, a Practice is likely to hold a fuller set of information for clients or classes of clients which have been assessed as higher risk.

Remote Identification

- 6.34** A client who is not a natural person (such as a company or trust) can never be physically present for identification purposes and will always be represented by an agent (such as a director or trustee). The mere fact that face-to-face meetings are not held with such agents does not automatically mean that EDD must be undertaken. A Practice will need to consider the risks associated with the instructions and the client, assess how well their standard CDD requirements address those risks and decide whether further measures are required.
- 6.35** EDD must be applied where a client who is a natural person is not physically present for identification purposes. A Practice must take specific and adequate measures to compensate for the higher risk, for example, by applying one or more of the measures prescribed in Regulation 14(2) (see 6.37).
- 6.36** The extent of the additional verification will depend on the nature and characteristics of the service provided and the money laundering risk assessed to be presented by the client. A Practice may wish to assess if it is reasonable for the client to remain remote or if the client is deliberately avoiding direct contact, taking account of the risk of impersonation fraud.
- 6.37** Regulation 14(2) provides examples of the measures which can be taken:-
- using additional documents, data or information to establish identity (which could involve using electronic verification to confirm documents provided or using 2 or 3 documents from different sources to confirm the information set out in each);

- using supplementary measures to verify or certify the documents supplied or obtaining confirmatory certification by a credit or financial institution which is subject to AML/CTF requirements (an alternative, not expressly provided in the Regulations may be to use electronic verification to supplement certified copies of documents);
- ensuring that the first payment made by the client is through an account opened in his name with a credit institution. (EU Regulation 2781/2006 requires credit institutions to provide the payer's name, address and account number with all electronic fund transfer, enabling these to be used as part of the further identification process.)

Politically Exposed Persons (PEPs)

- 6.38** Individuals entrusted with high public office (and their immediate families and known close associates) can pose a significant risk as their positions make them vulnerable to corruption. These individuals are known as Politically Exposed Persons or PEPs.
- 6.39** Where it knows, suspects or is advised that the business relationship that they are about to create is being formed with a PEP, a Practice can reduce substantially the risk to reputation of being implicated in high profile money laundering or terrorist financing investigations by conducting EDD, and subsequently enhanced ongoing monitoring of that relationship.
- 6.40** A Practice is likely to apply a risk-based approach to determine how long to carry out enhanced ongoing monitoring after an individual has stopped being a PEP. In many cases, a longer period may be appropriate to ensure that the higher risk associated with the position that he previously held has adequately abated. Although not specifically defined, enhanced ongoing monitoring is "ongoing monitoring" extended in frequency and intensity.
- 6.41** A PEP includes (paragraph 4(1)(a) Schedule 2):-
- Heads of State, Government, Ministers and Deputy or Assistant Ministers;
 - Members of Parliaments;
 - Members of Supreme Courts, Constitutional Courts or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances;
 - Members of Courts of Auditors or the Boards of Central Banks;
 - Ambassadors, chargés d'affaires and high ranking officers in the Armed Forces; and
 - Members of the Administrative, Management or Supervisory Boards of State-owned enterprises (other than in respect of relevant positions at community and international level).
- 6.42** These categories do not include middle ranking or more junior officials (paragraph 4(1)(b) Schedule 2).
- 6.43** "Immediate family members" can include a spouse, a partner (including a person who is considered by his national law as equivalent to a spouse), children and their spouses or partners and parents.

- 6.44** Persons who are "known close associates" include any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person who is a PEP. It also includes any individual who has a sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person who is a PEP.
- 6.45** A Practice must have regard to any information which is in its own possession or which is publicly known for the purpose of deciding whether a person is a known close associate (Regulation 14(6)).

Other CDD measures

- 6.46** Depending on the particular risk assessment, some or all of the following information may be relevant:-
- (a) the nature and detail of the client's business, occupation and employment;
 - (b) a record of any change of address;
 - (c) the expected source and origin of the funds to be used in the transaction;
 - (d) initial and ongoing sources of wealth or income;
 - (e) copies of recent and current financial statements;
 - (f) the relationships between the client and any underlying beneficial owner;
 - (g) the anticipated level and nature of any activity that is to be undertaken throughout the business relationship.
- 6.47** This information will help a Practice to establish the purpose and nature of the business proposed, and that it is consistent and rational.
- 6.48** From a practical point of view, enquiries of this type will need to be made at the outset of the business relationship.
- 6.49** In addition, it is advisable at the outset to establish the intended destination of any proceeds and, if payment is to be made other than to the client, to understand the purpose of such a payment (funds paid to a third party may raise suspicion of layering – see page 70).
- 6.50** Effective CDD and EDD procedures protect a Practice from being used for money laundering and terrorist financing. In addition, it provides protection for the Practice against fraud and other risks (particularly to reputation).
- 6.51** In most cases, CDD and EDD is likely to be relatively straightforward where a house is bought or sold, but a Practice may wish to consider how the wider context can be taken into account.
- 6.52** The risks of different types of transaction can be graded as part of the risk assessment. For example:
- A property bought as a home, funded by the sale of the previous home and by mortgage funds from a regulated credit institution, will generally create the lowest level of risk.

- Investment properties, including 'Buy to Let' transactions, may produce a somewhat higher risk.
- The highest risk transactions are likely to involve significant funding from an off-shore source where there is a lack of transparency as to the beneficial ownership of the purchase monies.

Simplified Due Diligence (SDD)

6.53 SDD means not having to:

- identify the client or verify the client's identity
- verify the identity of a beneficial owner
- obtain information on the purpose or intended nature of the business relationship.

6.54 It is unlikely that Practices will be instructed on matters for which SDD is applicable. Even if it does apply, ongoing monitoring of the business relationship must be maintained and a Practice must remain aware of its duty to report knowledge or suspicion of money laundering or terrorist financing which becomes apparent as a result of the ongoing monitoring process.

Reliance

6.55 A Practice remains liable for any CDD measures carried out by a third party which must be made at the outset of the business relationship or occasional transaction.

6.56 Where a Practice intends to rely on a CDD measure carried out by a third party, the third party must:

- give consent to that reliance; and
- agree that the CDD material will be provided on request.

6.57 Since it will remain liable for non-compliance, it is advisable for the Practice to satisfy itself that the CDD measures will comply with the Regulations by obtaining confirmation of what CDD has been carried out.

6.58 Electronic means of verification is outsourcing rather than third party reliance.

6.59 A "Third party" is narrowly defined (Regulation 18).

6.60 Before relying on them, it would be prudent to check the credentials of the third party by checking with their regulator or supervisor unless the person or firm concerned is well known to the Practice.

6.61 Even if it relies on a check carried out by a third party at the outset of a transaction, a Practice is still required to carry out ongoing monitoring.

Default or delay by clients

6.62 Even where a client appears not to pose any money laundering or terrorist financing risk, it is not advisable for a Practice to accept a retainer, carry out any substantive work or receive or pay over any funds until all CDD procedures have been completed to its reasonable satisfaction.

- 6.63** Regulation 9(3) allows verification of identity to be completed “as soon as practicable after contact is first established” in limited circumstances. A Practice is likely only to rely on this provision in exceptional circumstances where any delay is readily explained. In any other circumstances the fact of delay in producing relevant identification evidence and responding to CDD enquiries is likely in itself to give rise to suspicion.
- 6.64** A Practice must consider making a suspicion report to SOCA (Chapter 9, page 58) where a new or existing client fails to provide satisfactory identification evidence or replies to other CDD enquiries within a reasonable period and without adequate explanation.
- 6.65** Where money has been received before a decision not to accept instructions has been communicated, a Practice’s procedures are likely to require the consent of SOCA to be obtained before any funds are returned to the original source or directed elsewhere. Alternatively, in the absence of consent, no action must be taken until 7 working days after the date following the date the disclosure was made, provided that before any such action is taken no refusal of consent has been received from SOCA.

Ongoing Monitoring

Within a business relationship

- 6.66** Where a business relationship has been established, any further and later transactions undertaken for that client must be assessed in the context of the relationship to date and against the economic circumstances and expected pattern of activity of that client. The history of the business relationship should be viewed as a whole rather than as independent isolated events.
- 6.67** In the context of CDD and ongoing monitoring, any unexplained activity or source of funding will need to be examined to determine whether there is a reasonable suspicion of money laundering or terrorist financing.
- 6.68** It is reasonable (see Chapter 9, page 58) to make enquiries to understand more about a transaction to determine whether a concern amounts to a valid suspicion. This cannot constitute “tipping-off” if the enquiry is undertaken before an internal report or SAR is made and where there is no knowledge or indication that an investigation by any law enforcement agency is already under way or contemplated.
- 6.69** However, the situation changes where an internal report has already been made to a Nominated Officer or a SAR has been made by the Practice or it is known that a SAR has been made by anyone else or an investigation has been commenced or is contemplated. Great care must then be taken to ensure that any further enquiries do not lead to disclosure (even inadvertently) of the fact that a SAR has been made either to the client or to any other third party. Such enquiries are likely to be made only by the Nominated Officer or under his specific direction, following consultation with SOCA.
- 6.70** A Practice’s procedures may require the Nominated Officer to assume overall control of any ongoing monitoring activity once an internal report has been made.

Existing Clients

- 6.71** The Practice’s procedures may require updated, revised or additional evidence following a range of trigger events (such as a new transaction or a new type of transaction).

- 6.72** Where it already holds a considerable amount of information about a client of some years' standing, the Practice may decide to collate and assess existing information rather than calling for additional identification data or information.
- 6.73** The procedures of a Practice must ensure that any significant change in the nature of a client relationship triggers a proportionate response.

What counts as identity and verification?

- 6.74** Generally, identity means a set of attributes which together uniquely identify a natural or legal person (e.g. a natural person's identity comprises his name, all other names used by him and the residential address at which he can be located).
- 6.75** The first requirement of knowing an individual client for AML/CTF purposes is to be reasonably satisfied that any prospective client is who he claims to be and that someone of that name lives at the address given. For a non-natural legal person, it will be necessary to establish that the prospective client is what it claims to be, that it exists and is duly registered (where applicable), and that its principal address corresponds with any official records held.

For a private individual

- 6.76** For clients, verification must be completed on the basis of documents, data and information which come from reliable and independent sources. This can be achieved by a number of means including one or a combination of the following:-
- obtaining or viewing original documents; and/or
 - conducting electronic verification;
 - obtaining external information from official or reliable sources;
 - obtaining information from other regulated persons under the reliance provisions.
- 6.77** Provided the source is independent and reliable, the evidence may include official documents produced by the client himself although, in most cases, these are capable of being corroborated by other means (e.g. electronic verification).
- 6.78** Overall, a Practice should consider the cumulative weight of information held for any client and the risk levels associated both with that client and the business he wants to transact in deciding whether it is reasonably satisfied with the identity claimed and the evidence produced. Realistically, under the risk-based approach, only a Practice will be able to make the judgment as to what will provide the appropriate degree of confidence, either for standard CDD or EDD purposes.
- 6.79** The requirement to check a client's identity is mandatory. Reliance on personal knowledge of a client by anyone in a Practice is not sufficient. Personal introductions may provide comfort but cannot replace formal identification evidence. A Practice's procedures may encourage details of who initiated and authorised an introduction to be kept with the client's records. Staff must not be pressured to waive normal identification procedures.
- 6.80** Where a client is buying a property with funds supplied by a third party (e.g. parents supporting a purchase by a child), the third party is treated as a beneficial owner (6.81).

For a Beneficial Owner

- 6.81** For private individuals, there can be a presumption that the client himself is the beneficial owner, unless there are features of the transaction or circumstances which indicate otherwise. A Practice is not required to enquire about beneficial owners, unless the client appears to be acting on behalf of someone else.
- 6.82** The verification requirements (Regulation 5) differ slightly between a client and a beneficial owner. The obligation to verify the identity of a beneficial owner is for a Practice to take risk-based (but adequate) measures to be satisfied that it knows who the beneficial owner is (Regulation 5(b)).
- 6.83** In order to identify a beneficial owner, it is for each Practice to decide if it will make use of public records, ask its clients for relevant data or obtain the information by other means. For example, for an incorporated client, a search made at Companies House will establish whether a company of that name exists and is duly registered. If returns are up to date the current directors and shareholders will be disclosed. Separate enquiries may be needed to establish the identity of the directors and shareholders.
- 6.84** Checks with professional bodies will establish the identity of professional firms such as lawyers and accountants and of their partners. Details about the firm's internal ownership and control structure are likely to be supplied by the partners.
- 6.85** The nature and structure of a trust or other legal entity is likely to be more difficult to establish, unless it is registered as a charity by the Charity Commission. Often, the only source of information may be the instructing Trustee.

What evidence is required?

- 6.86** The objective is for a Practice to establish to its satisfaction that it is dealing with a real person or organisation and obtain identification evidence sufficient to verify that the prospective client is that person or organisation.
- 6.87** The identification process needs to be cumulative, particularly in cases where the EDD requirements apply.
- 6.88** Different considerations will apply to:-
- UK and non-UK resident nationals;
 - unincorporated businesses or partnerships;
 - corporate clients (either public registered companies or private companies);
 - trust vehicles;
 - deceased person's estates
 - other legal entities and arrangements.
- 6.89** These are dealt with below.

Individuals (UK and non-UK residents)

- 6.90** A Practice must satisfy itself that an individual is who he says he is and that a person of that name lives at the address given. Where any client poses a higher risk, additional evidence of identity will be required under EDD. Identification evidence should be obtained for each joint client. Where clients share the same address, one form of address verification may be sufficient.
- 6.91** In any investigation, a date of birth is essential to law enforcement agencies and can provide a safeguard against identity fraud (a forged or stolen passport or driving licence may bear a date of birth which is clearly inconsistent with the age of the person presenting the document). There is no specific requirement to verify the date of birth provided, although any obvious discrepancy is likely to give rise to a suspicion.
- 6.92** Information concerning place of birth, residency and/or nationality is useful in assessing whether a customer is resident in or has links with a high-risk country. Residency is essential for determining whether a customer is based or incorporated in a country against which the Treasury has issued a Prohibition Notice or issued a Sanctions Notice.
- 6.93** Both residency and nationality are necessary in a non-money laundering context for preventing breaches of UN or other international sanctions to which the UK may be a party. Where a passport or national identity card is taken as evidence of identity, the number, date and country of issue should be recorded.
- 6.94** Other factors about an individual may accumulate over time, particularly where a Practice continues to act for a person on a regular basis. These will contribute to his identity footprint (e.g. family circumstances, current and former addresses, employment and business career, financial history, physical appearance, contacts with other advisers in the wider context).
- 6.95** Where there is no face-to-face contact, Practice must undertake EDD and enhanced ongoing monitoring (Regulation 14(2)).
- 6.96** When acting for lenders, Licensed Conveyancers are required (Clause 3B3.3 CML Handbook) to follow the guidance issued by the CLC (Guidance Note 13 – Acting for Lenders). For AML/CTF, a Practice must satisfy the identity verification requirements at the outset of instructions.

Evidence for UK Residents

Personal Identity

- 6.97** The following are examples of documents which might be relied on to verify an individual's personal identity:-
- Current signed passport;
 - Current EEA member state identity card;
 - Residence Permit issued by the Home Office to EU or EEA Nationals on sight of their own country's passport;
 - Current Identity card issued by the Electoral Office for Northern Ireland;

- Current UK or EEA photo-card driving licence or an official Disabled Driver's pass;
- Current full UK old-style driving licence (excluding an old-style provisional driving licence);
- Benefit Book or original notification letter from the DWP (Department of Work and Pensions) confirming the right to benefits;
- Photographic registration cards for self-employed individuals and partnerships in the construction industry (e.g. Forms C155, C156 or SC60);
- Formal HM Revenue & Customs tax notifications (e.g. Self Assessment Statement or Tax Demand);
- Shotgun Licence or Firearms Certificate;
- Birth Certificate

Address

6.98 The following are examples of the types of evidence that might be produced to verify a residential address:-

- Record of home visit;
- Confirmation from a search of an Electoral Register that a person of that name lives at the stated address;
- Recent utility bill or utility statement, or a certificate from a utility supplier confirming an arrangement to pay for such services on pre-payment terms (but care should be taken not to accept mobile telephone bills which can be sent to different addresses);
- Local Authority Council Tax bill valid for the current year;
- Bank, Building Society or Credit Union Statement or passbook containing a current address;
- The most recent original mortgage statement from a recognised Lender;
- A letter from a Licensed Conveyancer or a Solicitor confirming a recent house purchase or Land Registry confirmation of address (although in such cases the previous address should also be verified);
- Local Authority or Housing Association Rent Card or Tenancy Agreement;
- House or Motor Insurance certificate;

and if not already used as evidence of personal identity:-

- Benefits book or original notification letter from the DWP confirming the rights to benefit;

- Current UK driving licence (an old full licence or new photo-card licence but not an old-style provisional driving licence);
 - EEA Member State Identity Card;
 - HM Revenue & Customs Self Assessment Statement or Tax Demand addressed to the prospective client at his stated address.
- 6.99** Copies of the documents (or the relevant sections of the documents) produced and seen or a full reference of all the relevant details must be taken and retained to meet the record-keeping requirements (Chapter 10, page 64).

Evidence for Non-UK Residents

- 6.100** For prospective clients who are UK nationals who are not normally resident in the UK or who are foreign nationals, similar provisions will apply for personal identity. Passports or national identity cards are evidence of the name of the client.
- 6.101** Any concerns about the validity of foreign documents (e.g. a passport, national identity card or driving licence) can be checked by contacting the appropriate national Embassy, Consulate or High Commission of the country of issue, or by a lawyer or attorney from the country of issue or, in the case of international students, possibly by staff in the Registry of a UK Higher Education Institution. Where a senior member of a Practice has experience of such documents, he could be used as a point of reference for assessing validity under the Practice's Client Acceptance Policy.
- 6.102** Copies of the pages containing the relevant information should be taken (e.g. reference numbers, date, and country of issue), or recorded by the Practice in the prospective client's records as part of the identification evidence. Where other pages contain relevant information (eg visas), details of these should be noted with the client records. The relevant sections of any documents relied on will need to be translated where they are in a foreign language.
- 6.103** A Practice should obtain separate evidence of the prospective client's permanent residential address from the best available evidence, preferably from an official overseas source; e. a national identity card or driving licence (where these have not been used as evidence of name), or a reputable directory.
- 6.104** In places where P.O. Box numbers are normally used (eg Hong Kong and the Gulf States), a box number alone is unlikely to be sufficient evidence of address. It will be for the Practice to be satisfied that the prospective client's residential address can be physically located.
- 6.105** Evidence of identity and address can be obtained directly from the prospective client or under the reliance provisions relating to non-UK residents (Regulations 17(c) & (d)). This will normally be taken from a person in the equivalent regulated sector in the country where the individual is resident who can confirm that the person is known to them and lives or works at the overseas address given. Care should be taken when relying on evidence provided by a third party to ensure that the client's true identity and current permanent address have been confirmed.
- 6.106** Where a UK national who is not ordinarily resident in the UK or a foreign national has recently arrived and taken up residence in the UK, an employer, further education

institution, university, etc. may be asked to verify his current UK residential address in addition to seeking verification of his normal overseas address.

- 6.107** The evidence obtained should be such that the Practice is reasonably satisfied that the person is who he says he is and that he lives or has recently lived at the overseas address given and at any UK address provided.
- 6.108** A Practice must apply EDD where the client is not met face-to-face.

Unincorporated Businesses/ Partnerships

- 6.109** As a partnership or an unincorporated business is not a separate legal person or entity, identity information must generally be obtained and verified for all individuals involved in it, namely the partners, principal owners and controllers. In some cases, this will include identifying one or more individuals with significant control over the business. For a limited liability partnership, the guidance for corporate clients applies.
- 6.110** The size and nature of a partnership or business may mean it is not practical to identify all individuals involved. Applying a risk-based approach, a Practice may decide that the assessed risk is met by verifying the identity of one or more of the partners or owners, including at least the partners or owners who are giving the instructions, and supporting this approach by making independent checks.
- 6.111** For a smaller partnership or unincorporated business, the risk may be higher because of a lack of internal or external controls.
- 6.112** The evidence of identity for a partnership or unincorporated business is likely to include:
- Evidence of the registered and principal trading address (if different). This may be available from a professional or trade directory, or through a professional body or trade association;
 - The nature of the business or partnership, to ensure that it has a legitimate purpose. Where there is a formal partnership arrangement, an instruction from the partnership authorising the transaction and conferring authority on those who will give instructions for the transactions may be required.
 - A partnership of regulated professionals (e.g. accountants, lawyers, etc), may be asked to produce Practising Certificates or Licences
 - If a member of a firm is acting in a personal capacity (e.g. as trustees, attorneys, etc.), identity should be verified as for any other individual acting in that capacity.

Corporate Clients

- 6.113** A company, whether public or private, is a legal person in its own right and conducts its business through its officers. A Practice must identify and verify the existence of the company itself and of any representative, satisfying itself that they have proper authority.
- 6.114** A Company's identity is made up of its constitution and its business and legal ownership structure. The key identification features are:-
- its registered number;

- its registered corporate name and any trading names used;
- its registered address and any separate principal trading addresses;
- its directors;
- its owners and shareholders; and
- the nature of the company's business.

Public Registered Companies (UK or Non-UK)

- 6.115** For corporate clients listed on a recognised stock exchange, SDD under Regulation 13(3) should apply and there will be no need to verify the identity of individual shareholders or directors. If such companies are well-known household names, they may be considered to present a low level of risk of money laundering or terrorist financing.
- 6.116** For a listed company, it may be sufficient to obtain a copy of the dated page of the website of the relevant exchange showing the listing, a photocopy of the listing in a reputable daily newspapers or information from an electronic verification data provider or an on-line registry. The recognised market in the UK is the London Stock Exchange.
- 6.117** AIM does not count as a "recognised exchange" but evidence of a listing gives equivalent comfort. Additional verification may be sought by company search, by inspection of the Certificate of Incorporation or by seeking supporting information from an electronic data provider.
- 6.118** As additional protection, a Board Resolution or other authority for any representative to act on behalf of the company in its dealings with the Practice can be obtained to confirm that the individual has the authority to act.
- 6.119** No further steps will normally be required to verify its identity, where the client company:
- is listed and its shares are traded on a recognised or an approved stock exchange; or
 - where there is independent evidence to show that the applicant is a wholly-owned subsidiary or a subsidiary under the control of such a company; or
 - is registered with and licensed by a non-ministerial government department, eg OFGEN, OFWAT, OFTEL.

Private Companies

- Private companies (i.e. those which are not listed on a recognised stock exchange) are generally subject to a lower level of public disclosure and may present an increased risk of money-laundering or terrorist financing. Verification expectations are likely to be higher. Any copy documents produced should be certified to be true copies of the originals by a lawyer or the company's external auditors
- 6.121** Sufficient evidence of identity and address must be obtained for the principal underlying beneficial owner(s) of the company (i.e. those with 25% interest or more) and those

exercising control over the company's assets (e.g. principal controllers/directors or shadow directors).

6.122 When the prospective client is a company which is not listed, the following documents should be obtained from an official or recognised independent source to verify the identity of the business itself:-

- a copy of the Certificate of Incorporation (or equivalent); and
- evidence of the company's registered address and a list of shareholders and directors; and/or
- a Company Search from Companies House or an enquiry through a business information service (whether electronic or paper-based) to obtain the relevant information about the company, possibly including its latest filed accounts; and/or
- an undertaking from a firm of lawyers or accountants confirming the documents submitted to the relevant Companies Registry for registration.

Trust Vehicles

6.123 A trust is not a separate legal entity and so the prospective client may be a Settlor, Trustee or possibly Beneficiary.

6.124 UK trusts are in widespread use and will often pose limited risks. However, they can assume more risk, particularly if a client requests the use of a trust vehicle where there seems to be little reason to do so or the trust is established in an overseas or off-shore jurisdiction which has no or only limited AML/CTF regulation.

6.125 Whether acting as Trustees, Settlers or Beneficiaries, clients or their agents should be identified in accordance with their relevant type (eg natural person, company). Where acting for more than one trustee, it is preferable to verify the identity of at least two trustees. If the trustee is another regulated person, reliance may be placed on their listing with their own Supervisory Authority.

6.126 The beneficial ownership issues under Regulation 6 must be considered. If the risk is perceived to be higher, the identities checked and verified may need to be more extensive.

Deceased person's estates

6.127 A Practice will need to check and verify the identity of any executor or administrator of an estate using the procedures applicable to individuals or a company, depending on the nature of the personal representative appointed.

6.128 When acting for more than one executor or administrator, it is preferable to verify the identity of each of them.

6.129 Normally, a Practice instructed on a probate sale will see official copies of the death certificate and grant of probate or letters of administration which can form part of the verification evidence.

6.130 If a will trust is created, the procedures in relation to trusts are likely to need to be followed from the time the will trust comes into operation.

Other Legal Entities and Arrangements

Foundations

- 6.131** A foundation is a civil law equivalent to a common law trust and may operate in many EEA countries. Initially, a Practice will need to understand why it has been asked to act and to investigate the legal requirements for the establishment of the foundation in the relevant jurisdiction. It should then obtain similar information as for a trust.
- 6.132** If the founder is not identified, consideration will need to be given to whether any intermediary or agent acting on its behalf is regulated for AML/CTF purposes and whether the intermediary or agent can verify the identity of relevant persons involved with the foundation. A foundation established for charitable purposes can be verified as if it were a charity.

Charities and Other Bodies

- 6.133** Charities can take a number of forms. In the UK, there are broadly 5 types - (i) small; (ii) registered; (iii) unregistered; (iv) excepted (e.g. churches); and (v) exempt (e.g. museums and universities).
- 6.134** For registered charities, a record should be made of its 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 and the Office of the Scottish Charity Regulator at www.oscr.org.uk. Currently, there is no regulator for charities in Northern Ireland. Other countries may also have charity regulators which maintain a list of registered charities.
- 6.135** For all other types of charities, Practices should consider the business structure of the charity and apply the relevant CDD for that business structure. Confirmation of charitable status can sometimes be obtained from HM Revenue & Customs.
- 6.136** In applying the risk-based approach to a charity client, it is worth considering whether it is a well-known entity. The less known it is, the more likely it will be that a Practice will want to see its constitution document. As a result of the increased interest in some charities and not-for-profit organisations by terrorist organisations, the Practice may wish to consult the financial sanctions list which can be accessed on HM Treasury's website at <http://www.hm-treasury.gov.uk/financialsanctions> to ensure that the particular charity concerned is not a proscribed organisation.
- 6.137** Churches and places of worship may either be registered as a charity, have a registration certificate as a certified building of worship issued by the General Register Office (GRO), be registered with HM Revenue & Customs for charitable tax status or be listed and recorded by the headquarters or regional office of the denomination or religion concerned. They should be treated as a charity if they can be identified in one or more of these ways.
- 6.138** A School or College may be a registered charity, a private company, an unincorporated association or a government entity. The Department for Children, Schools and Families keeps lists of approved educational facilities at www.dcsf.gov.uk/providersregister.

Clubs and Associations

- 6.139** Most clubs and associations will normally present a low level of money laundering risk but particular care should be taken that such an association is not used for funding terrorism. Much will depend on the scope of the purposes, activities and geographical spread of the club or association concerned. In most circumstances, someone within the Practice will be familiar with its aims and activities. If not, greater scrutiny may be required.
- 6.140** The full name, legal status, purpose, any registered address and the names of all office holders may be relevant to the identity of the club or association. This may be verified by some or all of the following: Articles of Association or Constitution, a bank or building society statement, recent audited accounts and a listing in a local or national telephone directory.

What form should the evidence take?

Paper-based evidence

- 6.141** It is preferable for any documents produced for inspection to be originals. A Practice is not required to be expert in identifying forged documents, but should be able to identify obvious forgeries. Any concerns may be allayed by additional checks, possibly by using electronic means.
- 6.142** The evidence obtained is likely to be cumulative and provide a strong level of certainty that the natural or legal persons or other entities checked are who they say they are.
- 6.143** Once identification procedures have been satisfactorily completed, no further evidence of identity may be needed when transactions are subsequently undertaken as long as the identification evidence remains relevant and up-to-date (Regulation 8(2)(b)). Ongoing monitoring must be maintained and further action taken, if reasonably required.
- 6.144** Records of the supporting evidence and methods used to verify identity must be retained for 5 years from the date on which a business relationship ends (Regulation 19). Detailed guidance on the record-keeping requirements is contained in Chapter 10 page 64.
- 6.145** Copies of the supporting documentary evidence of identity or a reference of the full details must be taken and retained for that period and should be readily retrievable. The former may be preferable. HMSO has confirmed (6.148) that passports may be photocopied.
- 6.146** Where supporting documentary evidence cannot be copied or scanned at the time it is obtained, the reference numbers and other relevant details of the identification evidence obtained must be recorded. A Practice's procedures may require the record to include the method by which that evidence was obtained and for photocopies of original documents to be certified.
- 6.147** If any checks are made electronically, a record of the actual information obtained, or where it can be accessed, must be retained as part of the identification evidence. The underlying requirement is to be able to reproduce the actual information that was originally obtained.
- 6.148** HMSO Guidance Note No. 20 dated 5 December 2002 contains the following advice:

“Photocopies of the personal details page of a UK passport may be made for the purposes of record-keeping only by the following persons:-

- the holder/owner of the passport;
- notaries, solicitors, banks, UK government departments;
- any person or institution subject to the requirements of the Regulations for the purpose of certifying that identification checks required under those Regulations have been made.

These photocopies must be in black and white only, so that they cannot be mistaken for an actual passport page. Only the original document may be used as evidence of identity but a photocopy, or where necessary multiple copies, of the original may then be made to record/certify that identification checks have taken place. Such photocopying may be undertaken without applying for a licence or paying a fee.”

6.149 The term “copying” includes photocopying, scanning, filming and reproduction in any other medium, including the placing of materials on the internet.

Electronic Checks

6.150 A range of identification checks may be made electronically (as permitted in the CLC’s Guidance Note 13 – Acting for Lenders).

6.151 Licensed Conveyancers must obtain "satisfactory evidence of identity", which must be reasonably capable of establishing (and does in fact establish to the satisfaction of the person who obtains it) that the client is the person he claims to be. The CLC considers that verifying identity by appropriate electronic means is now an acceptable option, provided such means are relied on with caution.

6.152 Any system or product used must be sufficiently robust to provide the necessary degree of certainty by using data from a range of multiple sources, and across time, or must incorporate qualitative checks that assess the strength of the information supplied. The evidence base and level of verification must be composite and comprehensive. Data accessed from a single source (e.g. the Electoral Roll) will not normally be sufficient on its own. Some databases will offer a higher degree of confidence than others.

6.153 Before using a commercial agency for electronic verification, a Practice must be satisfied that:-

- (a) the information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate; and
- (b) the agency has processes which allow its users to capture and store the information that they have used to verify an identity.

6.154 Electronic evidence obtained must provide a strong level of certainty that any individual is the person he claims to be and that a person of that name lives at the address given using the client’s full name, address and date of birth as its basis.

6.155 The process needs to be cumulative and a Practice may consider it appropriate to seek additional evidence (eg a copy of a document bearing a signature and a date of birth) in all cases or, at least, where any client poses a higher risk of identity fraud, money laundering or terrorist financing or where the result of any electronic verification check gives rise to concern or uncertainty over the client’s identity.

- 6.156** A Practice should consider whether the provider meets each of the following criteria, namely that it:-
- (a) is recognised to store personal data through registration with the Information Commissioner's Office;
 - (b) uses a range of positive information sources that can be called upon to link an applicant to both current and previous circumstances;
 - (c) accesses negative information sources such as databases relating to identity fraud and deceased persons;
 - (d) accesses a wide range of alert data sources; and
 - (e) has transparent processes that enable a Practice to know what checks were carried out, what the results of these checks were and what they mean in terms of how much certainty they give as to the identity of the subject of the identity enquiry.
- 6.157** Data from more robust sources where inclusion is based on proof of identity, such as from government departments, ought to be included (under paragraph (b)). Negative information checks (under paragraph (c)) minimise the risk of impersonation fraud.
- 6.158** It is important for a Practice to make sure it understands the basis of the system it uses in order to be satisfied that the sources of the underlying data reflect the guidance and cumulatively meets the standard level of confirmation set out above. Commercial agencies use various methods of displaying results (eg by the number of documents checked or through scoring mechanisms, etc), so careful checks are needed.
- 6.159** It is also important for the process of electronic verification to meet a standard level of confirmation before it can be relied on. In circumstances which do not give rise to concern or uncertainty, the standard level expected is:
- (i) one match on an individual's full name and current address *and*
 - (ii) a second match on an individual's full name and *either* his current address *or* his date of birth.
- 6.160** If the result of a standard verification check gives rise to concern or uncertainty over the client's identity, additional matches are required to provide reasonable satisfaction of identity.

CHAPTER 7 - INTERNAL REPORTING PROCEDURES

Requirements of the Regulations and of the law

A relevant person must establish and maintain internal reporting procedures (Regulation 20(2)(d)(ii)) requiring anyone in his organisation who receives information as a result of which he knows or suspects or has reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing must make a report to the organisation's Nominated Officer (Part 7 POCA or Part 3 TACT).

There are no exceptions: the reporting requirements apply whatever the value; whatever the nature of the underlying crime generating the funds or assets; and whether or not there has been a conviction for that crime.

A person is to be taken to have committed a terrorist financing offence (ss.15 - 18 TACT) if he has taken any action or been in possession of an asset and would have committed the offence had he been in the UK at that time.

The requirements extend to attempted money laundering or terrorist financing even if the business has been turned away.

An internal report must be made as soon as is practicable (s.330(4)(b) POCA and s.21A(4) TACT).

It is an offence not to have an internal reporting procedure (Regulation 20(2)(d)(ii)).

Failure to report is an offence under POCA and TACT respectively carrying a penalty on summary conviction of a term of imprisonment of up to 6 months or to a fine not exceeding the statutory maximum or both or, on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine or both.

CLC Expectations

7.1 A Practice must establish and maintain clear internal reporting procedures for staff which:

- (a) require an internal report to be made to the Nominated Officer of any information or other matter coming to their attention in the course of their business activity within the Practice which, in the opinion of the person concerned, gives rise to a knowledge or suspicion or gives them reasonable grounds to know or suspect that another person is:-
 - (i) engaged in or has benefited from criminal conduct or money laundering; or
 - (ii) providing financial assistance for terrorism; or
 - (iii) facilitating the retention or control of terrorist funds.
- (b) require that such reports are made as soon as possible after the information has come to the attention of the person concerned;
- (c) ensure that, once a report has been made, the transaction does not proceed any further unless and until authorised by the Nominated Officer;

- (d) ensure that no steps are taken by them after such a report has been made which could amount to “tipping-off”; and
- (e) ensure that everyone in the Practice has been trained regularly in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

7.2 A Practice must monitor how these procedures work. It should be prepared to discipline any member of staff who fails, without reasonable excuse, to make an internal report.

Practical Considerations

7.3 All internal reports should reach the Nominated Officer. A Practice should have clear procedures which avoid the suppression of internal suspicion reports. There could be a temptation to do this if, for example:-

- (i) the fee-earner handling the transaction does not agree; or
- (ii) the client is considered to be too important; or
- (iii) the business is too profitable to turn away; or
- (iv) to seek consent from SOCA to go ahead with the transaction (see page 58) would cause delay.

7.4 Reporting lines should be kept as short as possible between those who might make internal reports and the Nominated Officer. This ensures speed of contact, confidentiality and accessibility to the Nominated Officer. A Nominated Officer should be required to make himself available and accessible to Principals and staff.

7.5 A supervisor may be able to supplement a report either by confirming or allaying any suspicion. This may help the Nominated Officer in investigating and assessing the internal report. If the report is not made, or is delayed, a member of staff may be prevented from relying on the defence (under POCA, but not under TACT) of having made a disclosure to a Nominated Officer as soon as was practicable.

7.6 All suspicions reported to the Nominated Officer should be documented. Reports made by telephone should be recorded by the Nominated Officer and as a matter of good practice followed by a written report. The internal suspicion report should include the full details of the client and as full a statement as possible of the information and circumstances giving rise to the suspicion (see template in AML/CTF Toolkit). The Nominated Officer will need this information to make his own internal assessment and in making a report to SOCA.

7.7 In each case, the Nominated Officer should acknowledge receipt of the report and give a reminder about the risks of “tipping off”. He should consider whether any other members of the Practice should be advised of the report.

7.8 Any new suspicions (whether of the same or a different nature) must also be reported to the Nominated Officer.

7.9 An internal report may need to be made, even if instructions have not been accepted.

Employee Protection

- 7.10 Employees who report their suspicions to the Nominated Officer will satisfy their statutory reporting obligations.

Transfer of Responsibility

- 7.11 Once an internal suspicion report has been made, the Nominated Officer is required to assess the report and, if appropriate, to make a SAR to SOCA (see Chapters 8, page 55 and 9, page 58).

What is meant by knowledge, suspicion and reasonable grounds to suspect?

Knowledge

- 7.12 "Knowledge" means actually knowing something to be true and can be inferred from the surrounding circumstances. A failure to ask obvious questions (e.g. wilful or reckless blindness) may imply knowledge.

Suspicion (subjective)

- 7.13 "Suspicion" is personal to an individual. It must be more than mere speculation and have some foundation (see *R -v- Da Silva (2006)*). It is not necessary to know the exact nature of the criminal offence or that the particular funds were generated by the crime.

Suspicion (Objective)

- 7.14 The test is whether there are facts or circumstances known to the individual from which a reasonable and honest person (working in a similar regulated sector business) would have inferred knowledge or formed the suspicion that another was engaged in money laundering or terrorist financing. For a Licensed Conveyancer Practice, the test is whether the circumstances would have aroused a suspicion for a reasonable and honest Licensed Conveyancer.

Examples of "Reasonable Grounds for Suspicion"

- 7.15 It is impossible to provide a catalogue of what might constitute suspicion in each individual set of circumstances. Some Warning Signs and examples are given in Chapter 1 (pages 9-11). A number of these areas of concern are specifically addressed by the extended CDD requirements covered in Chapter 6 on page 35.

CHAPTER 8 - ASSESSMENT OF INTERNAL REPORTS

Requirements of the Regulations

A Practice must have policies and procedures (Regulation 21(2)(d)(iii)) which provide that, where an internal disclosure is made (see Chapter 7, page 52), the Nominated Officer must consider it in the light of any relevant information which is available and determine whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering or terrorist financing.

Any failure by a Practice to establish and maintain such a policy and procedure will give rise to an offence committed by its Principals and render them liable to the standard penalty tariff.

CLC Expectations

- 8.1** A Practice must require in its AML/CTF policies and procedures that a Nominated Officer must:
- consider promptly any internal disclosure made to him in the light of any and all relevant information which is available within the Practice, and
 - on the basis of his assessment of that information, determine promptly whether the internal disclosure gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing.
- 8.2** A Practice must make sure that all CDD information, transaction records and any other information about any relevant client activities or any linked transactions are readily accessible or made available promptly to the Nominated Officer on request so that he can fully and properly assess every internal suspicion report.

Practical Considerations

- 8.3** The significance of the Nominated Officer's role needs to be promoted by the Principals and acknowledged by all members and staff of the Practice. The Nominated Officer needs to have full co-operation from the Principals and all the staff of the Practice to enable him to fulfil his statutory obligations.
- 8.4** A Nominated Officer will need to evaluate all the internal disclosure reports he receives as soon as reasonably practicable to decide whether or not there is knowledge, suspicion or reasonable grounds for suspicion. If so, a SAR must be made to SOCA without further delay (Chapter 9, page 58).
- 8.5** The factors a Nominated Officer is likely to take into account in evaluating an internal disclosure report include whether:-
- the client was seen by a member of the Practice;
 - the client was new to the Practice and the initial verification of identity was completed satisfactorily;

- the client's identity was satisfactorily verified at the outset of the business relationship (or other dealings) and that the verification records are still retrievable;
- the subsequent dealings with the client confirm that the original identification evidence was correct and remains current;
- the client would be categorised as being high, medium or low risk taking into account his personal circumstances, geographical location and any other relevant factors;
- the client was introduced by, or is a client acting on behalf of, a third-party and, if so, whether that third-party has also been satisfactorily identified; and
- any beneficial-owner checks and verification still match the original profile established at the start of the business relationship when viewed in the light of subsequent events and dealings.

8.6 The process may also include a review of:-

- other transaction patterns and the number of transactions carried out within the business relationship in the same client name or in linked names;
- any previous patterns of instruction;
- the length of the business relationship and the correlation with the identification records held.

8.7 As part of that review, other connected transactions or relationships may need to be examined, particularly if SARs have been previously made.

8.8 A Nominated Officer should be alert to any changes in the nature of the client relationship and whether there was a satisfactory reason why the client instructed the Practice rather than another which might have seemed more convenient or expedient.

8.9 The source and destination of funds used in the transaction may also be investigated:-

- to make sure that there is an audit trail and evidence of verification of the origin and ownership of the funds; and
- to establish whether the funds have been provided by a third-party or are coming from or likely to be going to a high-risk destination. This is particularly relevant if the funding for the transaction or the net proceeds of the transaction are to be received from or paid overseas.

8.10 If there are pressing deadlines to meet, a Nominated Officer will need to consider urgently whether to seek consent from SOCA for a pre-advised transaction (Chapter 9).

8.11 A Nominated Officer should not delay making a report to SOCA because not all relevant information is available. He should keep a record of any relevant information which has not been considered with an explanation of why it was not readily available. A supplementary report can be made, if required.

8.12 It is suggested that a Nominated Officer documents details of:-

- (i) the member of staff who made the internal disclosure report;

- (ii) the nature of the disclosure and the reasons for it having been made;
 - (iii) the evaluation process that he follows; and
 - (iv) the reasons for his conclusions.
- 8.13** Such records should be kept by the Nominated Officer and should be stored separately from the transaction file to avoid any danger of an original records (or indeed a copy) being released subsequently to the client or to new legal representatives. Such an oversight may amount to “tipping off”.
- 8.14** Providing that the Nominated Officer exercises sound judgement and acts in good faith in deciding not to submit a SAR, it is unlikely that any criminal liability will arise as a result of failure to report. However, any failure to report in circumstances where a SAR is warranted is a breach of “failure to disclose” (s.331 POCA or s.21A TACT).

CHAPTER 9 - EXTERNAL REPORTING TO SOCA

Requirements of the Law

Where he determines that an internal disclosure report gives rise to actual knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that another person is engaged in money laundering, then, to avoid committing an offence (s.331 POCA), a Nominated Officer must disclose such information by sending a suspicion report (SAR) direct to SOCA, as soon as is practicable after it came to him.

Similar reporting requirements are provided by s.21A TACT in respect of terrorist financing.

A Nominated Officer can apply to SOCA for consent to proceed with a transaction. If the consent request involves money laundering, there are provisions for deemed consent within certain timescales. However, there is currently no equivalent facility for obtaining deemed consent for a transaction where the knowledge or suspicion involves terrorist financing. The Home Office is currently consulting on changes to be made to TACT which, if made, will provide a limited deemed consent provision.

In the context of consent applications relating to money laundering, it is an offence for a Nominated Officer to give authority for a transaction to proceed if he determines in advance that there is actual knowledge or suspicion or reasonable grounds for suspicion and that a SAR should be made to SOCA.

CLC Expectations

- 9.1 A SAR must be made to SOCA as soon as possible after the Nominated Officer has determined that the Practice has actual knowledge or suspicion or reasonable grounds for such knowledge or suspicion of money laundering or terrorist financing. In practical terms, a short delay in making a SAR whilst taking legal advice or seeking other external guidance may be acceptable, provided action is taken promptly to obtain such advice or guidance.
- 9.2 A Practice should ensure that its Nominated Officer seeks consent from SOCA for the Practice to proceed with any suspicious transaction relating to money laundering or terrorist financing.
- 9.3 Applications for consent should not normally be dealt with by anybody else in the Practice other than the Nominated Officer (or possibly his Deputy).
- 9.4 The Nominated Officer should maintain direct responsibility for dealings with SOCA and other law enforcement agencies both before and after a disclosure is made.

Practical Considerations

SOCA Reporting Procedures

- 9.5 The external disclosure regime for money laundering and terrorist financing is operated by the Serious Organised Crime Agency (SOCA). Where he determines that there is knowledge or suspicion or that there are reasonable grounds to know or suspect that a person is engaged in money laundering or terrorist financing, a Nominated Officer must make a SAR to SOCA. In this context:

- A SAR (Suspicious Activity Report) is the report submitted by the Nominated Officer or his Deputy to SOCA under either POCA or TACT .
- The UK Financial Intelligence Unit of SOCA (UKFIU) is the national reception point for all disclosures under the relevant legislation. Reports made elsewhere could expose the Nominated Officer (or his Deputy) to a “failure to report” offence.
- The postal address of the UKFIU is PO Box 8000, London SE11 5EN.
- Its website is at www.soca.gov.uk
- The FIU Help Desk can be contacted by telephone during office hours on 020 7238 8282. Outside office hours, an answer-phone operates on that number. Help can be obtained about submitting a SAR, consent issues, assessing the risk of tipping-off and so on.
- The UKFIU Dialogue Team can be contacted 24/7 by e-mail at fiudialogue@socax.gsi.gov.uk. Any messages on SAR-related issues will be dealt with through the Proceeds of Crime Dialogue Office. This is not to be used for SAR reporting – it is a means of addressing concerns via e-mail.
- Urgent disclosures (e.g. those requiring consent) can be transmitted electronically or by fax on 020 7238 8256.

Form and Manner of External Reports

- 9.6** Copies of the current Standard Disclosure Report Form and the Limited Intelligence Value Disclosure Report Form with guidance notes are found at www.soca.gov.uk by clicking on “Suspicious Activity Reports” under proceeds of crime. The format of these templates may be changed periodically. There may also be a requirement to submit SARs online (though the timescale for this change is not yet known).
- 9.7** SOCA prefers reports to be made to “SAR Online” available at www.ukciu.gov.uk/saronline.aspx or via the SOCA website at www.soca.gov.uk. It is relatively easy to register for this service and the system is claimed to have high in-built levels of security to ensure confidentiality. The system provides various facilities – for example, on-line user groups to share information, the ability to save work-in-progress for up to 28 days and the ability to save any SARs up to the point of submission (but not after that point).
- 9.8** Once a Practice is registered, the Nominated Officer can make reports at any time. A clear indication that “consent” is being sought for a pre-advised transaction can be given and this will place the on-line SAR in a priority list. SARs filed electronically will be acknowledged.
- 9.9** SOCA suggests that standard SARs should be printed from the SOCA website and posted. Only SAR consent application requests should be faxed (there is no need for a hard copy to follow in the post). SOCA has advised that forms should not be completed in manuscript as this can lead to transcription errors when the information is input. Paper-based SARs will not be acknowledged.
- 9.10** SOCA asks that SARs cover the six key items required by the prescribed form and, where possible, that the codes appearing in its SARs Glossary posted on its website are used. This will speed up consideration.

- 9.11** Making a SAR provides protection and a defence against the failure to report offences. When there is doubt, it is preferable for a Nominated Officer to make a report rather than determine that no report should be made.
- 9.12** A Nominated Officer does not need to establish whether or not a person known or suspected of money laundering or terrorist financing is actually a client of the Practice before a disclosure is made. A SAR can be submitted for any person who is suspected of such involvement.

Standard versus Limited Intelligence Value Disclosure Report Forms

- 9.13** The Limited Intelligence Value Report Form can be used only in restricted situations (and then only for AML and not CTF purposes). SOCA reserves the right to call for a Standard Disclosure.
- 9.14** The CLC recommends that a Practice submits a Standard Report whenever an SAR is to be made. A Limited Intelligence Value Report may be appropriate only where the Practice knows that a particular law enforcement agency already has an interest in a particular matter, normally as a result of an earlier SAR.

Delayed Reports and Ongoing Vigilance

- 9.15** The receipt of a SAR that, exceptionally, could only be made after completion of a transaction, may be acknowledged by SOCA and, in the absence of any instruction to the contrary, a Practice should be free to continue with post-completion activity (e.g. payment of Stamp Duty Land Tax, Land Registry application) without seeking explicit consent.
- 9.16** A Practice should try to avoid reporting after the event since this could give rise to an offence of failure to disclose at the appropriate time in the absence of a reasonable excuse.
- 9.17** After making a suspicion report, a Practice should be alert to any additional or related activities in respect of that client or his business that may give grounds for suspicion. If there is a suspicion, the Nominated Officer may need to make further disclosures to SOCA.

Action following the making of a suspicion report

- 9.18** Following the making of a SAR, a Practice may wish to cease acting for a client as permitted in the Licensed Conveyancers' Conduct Rules 2005.
- 9.19** A Practice should take care not to take any action which might amount to "tipping-off". Rather, its Nominated Officer should try to agree with SOCA (or the Investigating Officer) how "tipping-off" can be avoided, and the Practice should work within that agreement.
- 9.20** It is advisable for records of external disclosures and any other relevant information to be kept. A law enforcement officer investigating the subject-matter of an SAR may ask for further information from the Practice. Similarly, a Practice may wish for feed-back on the progress of an investigation to decide how to manage a continuing client relationship.

Consent to undertake a pre-advised transaction

- 9.21** Where an instruction or information is received before a transaction takes place (e.g. before exchange or completion of a property transaction) and it raises a suspicion that

- the transaction itself or the funds involved in the transaction may relate to money laundering, a report must be made to SOCA and consent to proceed sought.
- 9.22** It will normally be too late to make a report after the event. A Practice or Nominated Officer that permits a transaction to proceed without a report having been made may be prosecuted.
- 9.23** When consent is needed, the SAR should be marked "CONSENT" and be faxed to the UKFIU or sent electronically immediately the suspicion is identified. Applications for consent should not normally be sent by post. Care should be taken to outline the outstanding specific steps that still need to be taken in the transaction because consent will be given by SOCA only to the extent for which it is sought.
- 9.24** No further work should be carried out on the transaction in the meantime which might amount to a prohibited act without the authority of SOCA. Failure to do so may be a breach of s.336(5) POCA.
- 9.25** SOCA will "fast-track" a report marked "CONSENT" and carry out the necessary enquiries (including contacting the appropriate law enforcement agency to seek a "consent" decision). Once SOCA and/or law enforcement has reached a positive decision, the disclosing Nominated Officer will be sent a copy of the consent letter and may be advised by telephone.
- 9.26** Under POCA, SOCA has 7 working days starting with the first working day after the SAR has been received either to provide or withhold consent. If it does not refuse consent within that period, there is deemed consent and the transaction can proceed once the period has expired. A consent letter from SOCA, or the absence of a refusal to consent within the 7 working day period, provides the person handling the transaction or the Nominated Officer of the reporting Practice with a defence in any prosecution for money laundering.
- 9.27** Again, under POCA only, if SOCA refuses consent within the 7-day period, the relevant law enforcement agency must obtain a Restraint Order within 31 calendar days (the moratorium period) from the day on which consent is refused if it wishes to prevent the transaction from proceeding after that date. Therefore, following receipt of a refusal, the transaction cannot proceed until the expiry of the 31-day period. If a Restraint Order is not obtained by the 32nd day, the transaction may proceed.
- 9.28** The timescales for deemed consent currently apply only for AML purposes. Currently, there are no equivalent time-related provisions for deemed consent under TACT for CTF purposes. No pre-advised transaction can therefore proceed until actual consent has been received. The Home Office has given notice that it intends to amend TACT to provide deemed consent for pre-advised transactions involving suspected terrorist financing.
- 9.29** In cases where consent is refused, SOCA has agreed to provide advice either directly or through law enforcement agencies as to what specific information can be provided to the client. In some cases, the law enforcement agencies may be keen to gather additional evidence as the transaction proceeds.
- 9.30** The consent provisions can apply only where there is prior notice of the transaction or instruction. SOCA can not provide consent after the transaction has occurred. Some examples of situations where consent would be required are:-
- where funds are received to fund a deposit or to complete a property transaction and there is a suspicion that the funds represent the proceeds of crime; or

- where funds are received into a client account from an unrecognised source with prior notice that the funds are to be paid away in whole or in part on a particular day and often to another party; or
 - other circumstances come to light to suggest that the transaction is not consistent with the knowledge of the client, the client's business or his lifestyle.
- 9.31** Where urgent consent is needed, the reasons should be included in the SAR and contact might be made with the UKFIU Help Desk to discuss the position. In pressing circumstances, SOCA can sometimes act very swiftly.
- 9.32** The importance of not proceeding with a transaction until such time as consent has been obtained from SOCA and the dangers of "tipping off" whilst such consent is awaited cannot be underestimated. The situation can be difficult to manage. Through its Nominated Officer, a Practice is encouraged to contact SOCA and/or any law enforcement agency and to maintain close liaison during the waiting period (or after the issue of any notice refusing consent) to assist both parties in handling the situation.

Feedback on Specific Disclosures

- 9.33** When an enquiry is under active investigation, the Investigating Officer may contact the Nominated Officer to ensure that he has all the relevant information or to seek documentation which supports the original disclosure. This may also include obtaining a Court Order requiring further information.
- 9.34** It is expected that the Investigating Officer will work closely with the Nominated Officer after an SAR has been made, though there are likely to be cases when this is not possible because of the confidential nature of the enquiry.

External Feedback

- 9.35** SOCA gives feedback, in an anonymous form, on the value of SARs received, particularly through its website (www.soca.gov.uk) under "Sanitised SAR Case Studies" in the Proceeds of Crime Section and in its annual reports. This is useful in providing a Practice with information as to the changing risks and vulnerabilities and in helping it to understand the intelligence value of different information included in SARs.

Internal Feedback

- 9.36** A Practice should ensure that all contact with the law enforcement agencies is controlled by the Nominated Officer so that he can understand what is going on.
- 9.37** Positive feedback to members of staff who made the internal reports which triggered the SARs will also be valuable in keeping them vigilant in the application of the requirements. If an arrest or conviction is reported, this will reinforce the effectiveness of the system and provide assurance that their suspicions were taken seriously.

Confidentiality of SARs

- 9.38** The source of any SAR leading to an investigation should remain confidential to avoid any risk to the reporter. SOCA is required to treat SARs confidentially and, where information from a SAR is disclosed for the purposes of law enforcement, it should take care to ensure that the identity of the reporter and the reporting Practice is not disclosed.

- 9.39** A Nominated Officer should raise with SOCA (either in the SAR or through its UKFIU Help Desk) any specific concerns about his safety or the safety of any member of staff following the making of a SAR.
- 9.40** Any breaches of confidentiality can be reported by telephone on 0800 234 6657 (in particular, to raise concerns about the inappropriate use of SARs by end users, such as law enforcement agencies).

CHAPTER 10 - RECORD-KEEPING

Requirements of the Regulations

Regulation 19 requires a relevant person to keep specified records for at least 5 years beginning with the date on which a business relationship ends or the date on which an occasional transaction is completed.

Insofar as they relate to a Practice, the specified records are:-

- (a) a copy of, or the references to, the evidence of a client's identity obtained under the application of CDD measures under Regulation 7, ongoing monitoring under Regulation 8 and any EDD measures and enhanced ongoing monitoring under Regulation 14;
- (b) the supporting records (consisting of the original documents or copies) in respect of a business relationship or occasional transaction which is the subject of CDD measures or ongoing monitoring.

A relevant person (as a third-party) who is relied on by another person under Regulation 17 must keep the specified records for 5 years beginning on the date on which he is relied on for the purposes of Regulations 7 (CDD) or 14 (EDD) and must, on request, make those records available to the person who is relying on him.

A relevant person who intends to rely on such a third party to apply CDD measures must take steps to ensure that the third party will, if requested, comply with the production requirement within the specified period.

However, these production and enquiry requirements do not apply where a relevant person applies CDD measures by means of an outsourcing service provider or agent. In such a case, the relevant person will need to obtain the information and copies of the documents or other verification data before forming a business relationship or carrying out an occasional transaction.

Failure to maintain records under Regulation 19 is an offence.

CLC Expectations

- 10.1** The AML/CTF policies and procedures of a Practice must set out (Regulation 20(1)(b)) what records will be kept, in what form and for what period.
- 10.2** Each Practice should maintain an appropriate system for retaining records and for available, as required, within the prescribed timescales. It is recommended that a Practice retains:-
 - (i) details of the CDD measures and supporting evidence obtained, the internal and external suspicion reports made, a record of the information considered by its Nominated Officer in the light of any internal disclosure report (whether or not an external report is made) and any further action taken in respect of internal and external suspicion reports; and

- (ii) records relating to all transactions undertaken within a relevant business relationship or as an occasional transaction.

10.3 The records should enable:-

- any transactions effected on behalf of any individual customer to be reconstructed;
- any client to be properly identified and located;
- all suspicion reports received internally and those made externally to be identified; and
- any enquiries received, within a reasonable time of the transaction being completed, from appropriate authorities and law enforcement agencies or any Court Orders for disclosure of information to be satisfied without undue delay.

Practical Considerations

10.4 One of the underlying purposes of the legislation is to provide evidence for use by law enforcement agencies in any subsequent investigation into money laundering or terrorist financing, and any resultant prosecution. Any Practice will need to be able to provide those agencies with its part of the audit trail. When drawing up its document retention policies, a Practice should balance the statutory requirements and the needs of the investigating authorities against normal commercial considerations.

Retention periods

10.5 In some cases, the regulatory AML/CTF retention period will be longer than the retention period prescribed under the CLC's Rules for accounting records and file retention. It is therefore vital that records required for AML/CTF purposes will not be destroyed before the end of the periods prescribed by the Regulations.

10.6 The record retention requirements are the same, regardless of the format in which they are kept, and whether the transaction was undertaken by paper or electronic means.

CDD records

10.7 The retention period for CDD material is either 5 years from the date on which a business relationship ends or 5 years from completion of an occasional transaction. Most transactions undertaken by a Practice will have an element of duration as part of a business relationship rather than forming a single or an occasional transaction. So deciding when the 5 year period starts needs to be made on a case by case basis.

10.8 In some circumstances, it may become clear that there is little or no prospect of any further contact with the client (e.g. the client has sold a property, his mortgage has been redeemed, all client funds have been accounted for and he has emigrated, or a Practice may become aware that a former client has died).

10.9 Where the client's retainer and instructions involve a number of connected or linked transactions, Regulation 19 provides that the CDD and EDD records for all transactions should be kept for a 5-year period from the completion of the last transaction.

10.10 Where a Licensed Conveyancer has reasonable grounds for believing that his client has become insolvent and has taken steps to recover all or part of a debt owed by the client, a record of the steps taken should be retained for 5 years from the date of the insolvency.

- 10.11** On the disposal of a Practice, systems will need to be established to ensure that its records for AML/CTF will be readily accessible for the specified period.
- 10.12** If a Practice is relied on under Regulation 17 to provide CDD information to another regulated sector business, it must keep the relevant documents for 5 years from the date upon which it was relied on as required by Regulation 19(4) and must be able and willing to produce that evidence if requested.

Transaction records

- 10.13** Where the records relate to a particular transaction (whether carried out as an occasional transaction or within a business relationship) the transaction records must be kept for a period of 5 years following the date on which the transaction was completed.

CDD

- 10.14** Practices will need to retain records of client and beneficial owner identification and verification in a form which satisfies the Regulations. To do this, they may keep either:
- a copy of the actual identification material produced (which is preferable), or
 - references to where a copy of the evidence of identity can be obtained, if required (only if it is necessary in the particular circumstances).
- 10.15** It may be prudent to have copies of any original documents certified as being true copies. Any evidence relied on should be admissible in court proceedings.
- 10.16** If electronic means for identity verification have been used as part of the CDD process, a copy of the information dataset result of the enquiry should be retained as the relevant evidence, or there must be a facility to enable the result to be accessed for the minimum periods prescribed by Regulations.
- 10.17** Where it is not possible to take a copy of the proof of identity (e.g. where no copying facilities are available), reference details must be recorded covering the type of document seen, its reference number, its date and place of issue and expiry or the date of writing, the issuer and any reference number on any letter or similar evidence and the relevant details recorded in the document or letter so that the document can be retrieved, if required.
- 10.18** A Practice must also retain evidence of the results of the enquiries made in the context of CDD, ongoing monitoring and any EDD. Any internal statement required by the Practice's AML/CTF policies and procedures for signing off before a person is accepted as a client (possibly under its Client Acceptance Policy) should be retained with the other evidence for the relevant period.
- 10.19** A Practice may consider retaining details of the risk assessment process applied for a particular transaction which determined the appropriate CDD or EDD measures. This note would indicate the level of risk attributed and why it was considered that sufficient information was held before or as the matter proceeded.
- 10.20** CDD and EDD records will need to be readily accessible to the Nominated Officer (or any MLRO appointed) and, for convenience, could be held separately from the client file, or as a separate folder within that file.

Transaction records

- 10.21** Transaction records supporting entries in the books of account, in whatever form they are produced (e.g. credit/debit slips, funds transfer authorities, cheque book stubs) should provide a satisfactory audit trail. Care should be taken to ensure that all supporting records and the actual entries made in the books of account are completed clearly and are as full as possible.
- 10.22** Records will need to be capable of distinguishing between transactions for different clients and identifying:-
- when and where the transaction took place;
 - in what form funds were received;
 - from where they were received;
 - to whom the settlement funds were paid;
 - in what form they were paid away;
 - the destination of any surplus funds and to whom they are paid; and
 - any other relevant information.
- 10.23** Following completion of a transaction, the client may call for the production and release of a transaction file or authorise its release to a third party (such as another lawyer). Care will need to be taken before releasing the file ensure that an appropriate record is retained, (eg a copy of the complete file or, as a minimum, a copy of the transaction and CDD record).

Internal and External Reports

- 10.24** Records should be made and retained of any activity under the internal and external reporting requirements, including a record (preferably copies) of all internal reports received and external reports.
- 10.25** Where he has considered an internal disclosure report but has not made a report to SOCA, a Nominated Officer should keep the other material that he considered in making his assessment and determination. This process should also apply to assessments which have resulted in an external report being made.
- 10.26** A Practice is recommended not to disclose such material to a client or any third party (i) to avoid “tipping-off” and prejudicing any existing or subsequent investigation and (ii) to preserve a good relationship with the client. A Practice may wish to maintain a separate file or section within a file or a central record which is cross-referenced to the transaction file.
- 10.27** Where it is aware there is a criminal investigation a Practice may wish to retain any records until the law enforcement agency has advised that they are no longer required.
- 10.28** Subject to internal procedures, if a Practice has not been advised that an investigation is under way by the end of 5 years after the conclusion of a business relationship or

completion of an occasional transaction where a SAR was made, the records will not normally need to be retained for any longer period. The JMLSG has suggested that records of all internal or external reports might be retained for 5 years from the date on which the report was made

Training Records

- 10.29** Chapter 5 (page 25) sets out the requirement for training records. The CLC AML Toolkit also provides guidance.
- 10.30** Records of all the AML/CTF training undertaken by the Principals and staff of any Practice should be kept for at least the equivalent 5-year period, if not longer, as
- (i) readily available evidence of compliance with Regulation 21,
 - (ii) a safeguard if any employee seeks to rely on the s.330(7) POCA defence, and
 - (iii) to assist the Practice in maintaining, monitoring and developing its training strategy as suggested in Chapter 5, page 25.

Privacy issues

- 10.31** There may be some tension between the provisions of the legislation and the data protection legislation, which applies to Practices and SOCA. The Nominated Officer/MLRO and a Practice must take into account both sets of obligations.
- 10.32** Under s.29 of the Data Protection Act 1998, a Practice does not need to provide personal data on request where such disclosure would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. Guidance issued by HM Treasury and the Information Commissioner confirms that the s.29 exception would apply where granting access to data held would amount to "tipping off". This may even extend to those suspicions which are only reported internally. If it is decided that the s.29 exception applies, a Practice may wish to document why this decision was made to enable a response to be made to any enquiries raised by the Information Commissioner.
- 10.33** The Treasury guidance can be found at:-
http://www.hm-treasury.gov.uk/media/D/F/money_laundering.pdf .
- 10.34** The Information Commissioner's Guidance can be found at:-
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf

How much to keep and where

- 10.35** Consistent with statutory requirements, a Practice may maintain records as a combination of:-
- original documents;
 - photocopies of original documents (preferably certified as true copies with confirmation that the originals were seen);
 - any certified copies accepted in hard copy under reliance or outsourced arrangements;

- scanned copies or original documents held electronically;
- microfiche copies taken of original documents;
- digital copy documents in computerised or electronic form. keeping electronic copies or hard copies of the results of any electronic verification checks made; or
- recording adequate reference details of the CDD materials seen

10.36 There is no requirement to retain original documents evidencing transactions or other activity.

10.37 The Regulations do not prescribe where relevant records should be kept. They may be kept either on individual transaction files or, for ease of reference and retrieval, in a central record of CDD measures. The overriding objective is for Practices to be able to access and retrieve relevant information without undue delay.

10.38 A central record may help:-

- the Nominated Officer to check easily on any earlier records should the need arise;
- the Practice to make records available to any law enforcement agency in response to the service of a Production Order; and
- the Practice to have the existing records readily available, if it receives further instructions from the client, although they may need to be updated.

10.39 Production Orders obtained under s.345 POCA by an Investigating Officer will usually require that information specified in the Order should be made available within 7 calendar days of the date of the service of the Order, although a longer period may be provided.

CHAPTER 11 - MONEY LAUNDERING AND TERRORIST FINANCING OVERVIEW

Overview of Money Laundering

11.1 The aim of money laundering is to obscure the source of illegally acquired funds through a succession of transfers and transactions until they appear to be legitimate.

Process

11.2 The laundering process is often accomplished in three distinct phases which may or may not overlap. These are:-

(a) Placement

Funds generated from crime are placed into the financial system either directly or indirectly. This is the point at which the proceeds of crime are most apparent and are therefore most at risk of detection. Because banks and major financial institutions have developed AML procedures, deposit takers, bureaux de change and other cash and money-based businesses (eg Licensed Conveyancers) are now the most vulnerable. A Practice must determine a policy on handling receipts of cash (see AML Toolkit).

(b) Layering

The proceeds of crime are separated and distanced from their original source by a series of transactions. The funds may pass through different business sectors and through different entities (e.g. companies and trusts) in different jurisdictions.

(c) Integration

The funds are integrated into the economy through different channels, including property. This can be the most difficult stage to detect.

11.3 Businesses dealing with property transactions are particularly vulnerable at the “layering” and “integration” stages.

The Need for Prevention

11.4 The main purpose of AML/CTF procedures is to place obstacles in money laundering and terrorist financing processes and take the profit out of crime. All property transactions are vulnerable.

Professional services and abuse of client accounts

11.5 Money laundering strategies have developed in response to AML measures since they were introduced in 1993. Professionals such as accountants and lawyers, including Licensed Conveyancers and Solicitors who undertake conveyancing transactions, have been used as conduits for criminal funds.

11.6 Client accounts have been used for the placement, layering and integration of criminal funds by taking advantage of legal professional privilege and professional secrecy attaching to such accounts, making them immune to normal checks carried out by financial institutions.

- 11.7** Lawyers are required to co-operate with law enforcement agencies in the detection and prevention of financial crime. They are “gatekeepers” expected to carry out checks on their clients. They are also required to identify suspicious circumstances by ongoing monitoring of the transactions which they undertake on behalf of clients.

Overview of Financing of Terrorism

- 11.8** Like any criminal organisation, a successful terrorist group is one that is able to build and maintain an effective financial infrastructure. Terrorists and their organisations need finance for a variety of purposes (e.g. recruitment, training, travel, accommodation, materials and safe-haven protection). Tracking and intercepting the flow of funds is vital in combating terrorism. Knowledge of business dealings of terrorist networks is critical in protecting national and international security and in upholding the integrity of national and international financial systems.
- 11.9** Terrorists often control funds from a variety of sources around the world which are moved between jurisdictions. In so doing, they use the services of professionals (such as bankers, accountants and lawyers).
- 11.10** Although the total funds required by terrorist networks may be large, the funding required to finance individual terrorist attacks may be relatively small. The ‘Bishopsgate bomb’ in the City of London in 1993, which caused loss of life and over £1 billion of damage to property, is estimated to have cost only £3,000. The US authorities have estimated the total cost of the planning and execution of the September 11 attacks in America at US\$ 200,000.
- 11.11** The financing of terrorism is closely linked with money laundering. Although the risk of involvement in terrorist financing may seem more remote than money laundering, a Practice must be aware of the dangers, particularly because terrorists and terrorist organisations buy property as part of their support activities.

Understanding the Financing of Terrorism

- 11.12** An approach from an individual involved in terrorist financing may not give rise to suspicion until an event occurs which highlights the probability of such activity (e.g. arrest of client or associate of a client). At this point, a Practice may need to make an external disclosure report (SAR).
- 11.13** Terrorism is funded not only from the financial proceeds of illegal activities but also from donations and contributions originating from lawful sources. The methods used to transfer funds or to conceal the sources which fund terrorism are similar to those used in the laundering of the proceeds of crime.
- 11.14** The laundering of money for terrorist financing often involves smaller sums of money coming from sources which may be legitimate. This is sometimes been called “reverse money laundering”, because “clean” money is converted into “dirty” money by virtue of its intended destination. This alone makes it far harder to identify.

Sources of terrorist financing

- 11.15** Terrorist financing is believed to come from two major primary sources.
- 11.16** Financial support is provided by Nation States or organisations with sufficiently large infrastructures to collect and then distribute funds to terrorists. ‘State-sponsored

terrorism' has declined in recent years. Some Non-Governmental Organisations (NGOs) have been involved in the funding of terrorist activity.

- 11.17 The second source for terrorist organisations is their own revenue-generating activity, which may or not be legitimate.

Recognition

- 11.18 Most suspicion reports to SOCA are made on the basis of suspicion of criminality and may not necessarily appear to be related to the financing of terrorist activity at all. Nevertheless, the number of SARs based on suspected criminal activity which have provided valuable information about terrorist groups is evidence of the important link between crime and terrorism.
- 11.19 Business relationships with individuals or entities that support or commit acts of terror will expose a Practice to a number of risks, not least to its reputation. The risk is even more serious if a terrorist is later shown to have exploited ineffective systems of internal control or a lack of effective CDD, EDD or ongoing monitoring.

International Action

- 11.20 International action against terrorist financing has focused on:-

- sanctions to sever money flows to individual terrorists and terrorist organisations;
- development of international standards to stop the financing of terrorism; and
- technical assistance to aid countries to develop the measures and infrastructure necessary to root out the financing of terrorism.

- 11.21 In November 2001 the International Monetary Fund (IMF) issued a communiqué calling on all member countries to ratify and fully implement the UN instruments to counter terrorism. The UN Sanctions Committee requested each member within its jurisdiction to:

“freeze the assets of terrorists and their associates, close their access to the international financial system and consistent with its laws, make public the list of terrorists whose assets are subject to freezing”.

- 11.22 FAFT is an inter-governmental body bringing together the legislators, financial sector regulators and law enforcement agencies from Member States. It has made 49 recommendations for national and financial sector strategies to prevent money laundering which are the accepted worldwide benchmarks. As part of its activities, the FATF maintains a current list of Countries with equivalence status and Non-Co-operative Countries and Territories (NCCTs) which are reviewed periodically.

LEGAL OBLIGATIONS, OFFENCES AND PENALTIES

Summary of The Current Law

- 11.23 The sources of the law affecting the Principals, Directors and staff of any Practice for the prevention of money laundering and combating the financing of terrorism are found in:-

- a) Proceeds of Crime Act 2002 www.opsi.gov.uk/acts/acts2002/20020029.htm (amended by the Serious Organised Crime and Police Act 2005 www.opsi.gov.uk/acts/acts2005/20050015.htm)
- b) Terrorism Act 2000 www.opsi.gov.uk/acts/acts2000/20000011.htm (as amended by the Anti-Terrorism Crime & Security Act 2001 www.opsi.gov.uk/acts/acts2001/20010024.htm)
- c) Money Laundering Regulations 2007 www.opsi.gov.uk/SI/SI2007/20072157.htm

11.24 The primary source for the new 2007 Regulations and amending legislation is the Third EU Money Laundering Directive of October 2005 which implemented the global standards produced by FATF in 2003.

11.25 The Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 have yet to be made although they are due to come into force on 15 December 2007. The changes will therefore need to be incorporated into this Guidance at a later stage

Statutory Offences - Money Laundering

11.26 Under Part 7 POCA, “money laundering” has been extended to include laundering the proceeds of all crime whether generated as a result of a person’s own criminal activity or as the result of the criminal activity of another. An objective test of knowledge or suspicion has been introduced for offences of “failure to disclose” in the regulated sector.

11.27 POCA created three principal money laundering offences which identify the behaviour that directly constitutes money laundering, simplifying and widening their scope.

11.28 All three offences depend upon the property being laundered falling within the definition of “criminal property” as contained in s.340 (11.38). Offences are not committed when the property in question is held legitimately.

11.29 An offence (“predicate” offence) must have been committed to generate criminal property which is being laundered. No conviction is necessary for the predicate offence for a person to be prosecuted for a money laundering offence.

11.30 The offences are:-

- (a) Concealing, disguising, converting or transferring criminal property, or removing criminal property from the jurisdiction (s.327 POCA). “Concealing” or “disguising” includes concealing or disguising the nature, source, location, disposition, movement, ownership or any rights connected with criminal property;
- (b) Making or entering into any arrangement to facilitate the acquisition, retention, use or control of criminal property by or on behalf of another person (s.328 POCA). The test for an “arrangement” (which is not itself defined) is whether it has the effect of facilitating the acquisition, retention, use or control of criminal property by or on behalf of another person in the present rather than in the future. Sham structures often fall within this category;
- (c) Acquiring, using or having possession of criminal property (s.329 POCA).

Inchoate Offences - Money Laundering

- 11.31** Money laundering (s. 340(11) POCA) also includes the inchoate offences (i.e. acts which anticipate a further criminal act) of:-
- (a) attempting, conspiring, or inciting someone to commit a principal money laundering offence; and
 - (b) aiding, abetting, counselling or procuring the commission of a principal money laundering offence.
- 11.32** A Practice will have to consider whether to make a SAR even if instructions are not accepted (e.g. where the business or transaction has been turned away or has not been proceeded with because money laundering was suspected or funds arrived from a suspicious source).
- 11.33** This contrasts with the situation where attempted crime (e.g. attempted fraud) is not reportable to SOCA because there has been no gain and, consequently, no criminal proceeds available for laundering. However, if a person or firm is suspicious of an attempted money laundering transaction where funds have been received, no funds should be returned until a SAR has been made and either SOCA has agreed to the transfer of funds or the 7 working-day period has passed since the consent application was made and no refusal of consent has been received from SOCA.

Penalties for Money Laundering Offences

- 11.34** The maximum penalty on conviction on indictment for any of these offences (either principal or inchoate) is a term of up to 14 years' imprisonment or a fine or both. On summary conviction, the maximum penalty is 6 months' imprisonment or a fine not exceeding the statutory maximum or both.

Defences against the Principal Money Laundering Offences

- 11.35** A person will not commit an offence under ss.327 – 329 POCA if:-
- he makes an authorised disclosure under s.338 to SOCA before the offence is committed (eg before he undertakes the transaction) and the necessary consent has been obtained from SOCA; or
 - he intended to make the authorised disclosure but had “reasonable excuse” for not doing so before the offence was committed. It is unclear what amounts to reasonable excuse;
 - (in the case of an acquisition offence under s.329 only), he acquired, used or had possession of the property for adequate consideration, provided that he did not know or suspect that the goods or services may help another to carry out criminal conduct.
- 11.36** The "adequate consideration" defence is primarily intended for retailers. However, according to the CPS guidance for prosecutors, it may also apply where professional advisers receive money for or on account of costs or disbursements, whether from the client or from another person on the client's behalf provided that the fees charged are reasonable and the value of the work undertaken is not significantly less than the money received. It will not apply where funds are returned to a client if the Licensed Conveyancer knows or suspects that the money is “criminal property” for which an authorised disclosure may need to be made and consent obtained.

Criminal Conduct

11.37 The definition of “criminal conduct” in s.340(2) of POCA as applied to each of the principal and inchoate money laundering offences is any conduct which constitutes an offence in any part of the UK or would constitute an offence in the UK. The two key points to note are that:-

- (a) the conduct need not be committed in the UK; and
- (b) it need not necessarily be illegal in the jurisdiction in which it is committed.

Criminal Property

11.38 Under s.340(3) of POCA, “criminal property” is property that the alleged offender knows or suspects falls into one of the following categories:-

- (a) property that constitutes a person’s benefit from criminal conduct; or
- (b) property that represents such property (whether in whole or in part and whether directly or indirectly).

11.39 It is immaterial:-

- (a) who carried out the criminal conduct; or
- (b) who benefited from it; or
- (c) when the conduct occurred (e.g. it could have taken place before POCA was implemented).

Criminal Conduct outside the UK

11.40 Neither POCA nor the Regulations impose a duty on Licensed Conveyancers to consider the criminal law of any other country in which the criminal conduct may have occurred. The basis for reporting suspicions that criminal conduct has arisen or that funds arise from criminal conduct is that the activity would be a criminal offence in the UK. A basic knowledge of what constitutes a criminal offence in the UK is therefore required.

Failure to Disclose Offences – Money Laundering

Regulated Sector Generally

11.41 Under s.330 POCA, a person working in the regulated sector will commit an offence if he fails to make a disclosure in circumstances where:-

- he knows or suspects, or has reasonable grounds to know or suspect that another person is engaged in money laundering; and
- the information on which the knowledge, suspicion, or reasonable grounds to know or suspect is based came to him in the course of business in the regulated sector; and

- he did not make the required disclosure as soon as was practicable to a Nominated Officer or SOCA.

11.42 The test for "reasonable grounds" is: were there factual circumstances from which an honest and reasonable person engaged in a business in the regulated sector would have inferred knowledge or formed the suspicion that another was engaged in money laundering?

Nominated Officer

11.43 A Nominated Officer must be appointed within a regulated business to receive internal reports of known or suspected money laundering and has a statutory duty to make disclosure reports (SAR) to SOCA where appropriate (Chapter 4, page 21). Breach of that duty constitutes an offence (s.331 POCA).

Fiscal Offences and Money Laundering

11.44 Tax-related offences (where illegal benefit has been gained by any person) are reportable offences under the money laundering legislation. This includes tax offences committed outside the UK that would amount to an offence if committed in the UK and where the knowledge or suspicion came to a person in the course of his business within the UK regulated sector and where there is a UK link (e.g. the 'taxpayer' is resident in the UK) or where the proceeds of the foreign tax fraud have entered or passed through a UK institution.

Penalties for Non-Disclosure in Regulated Sector

11.45 The maximum penalty for failure to disclose on indictment is a term of 5 years' imprisonment or a fine or both. On summary conviction, the maximum penalty is 6 months' imprisonment or a fine not exceeding the statutory maximum or both.

Defences against Failure to Disclose

11.46 There are three principal defences against a charge of failing to report. The first applies to any failure to disclose but the other two are specifically provided only for those in the regulated sector who are not Nominated Officers. Since they have not been tested, the effect of these defences remains uncertain.

11.47 There is now a limited reporting exemption if the property is derived from "overseas criminal conduct".

Reasonable Excuse

11.48 No offence is committed if there is a reasonable excuse for not making a disclosure. It is unclear what constitutes a "reasonable excuse".

11.49 Where a decision is made not to report, it is suggested that a full written record is made of how this decision was arrived at, so this can be produced in any prosecution.

Privileged Circumstances

11.50 No offence is committed if the information or other matter giving rise to suspicion comes to a professional legal advisor in privileged circumstances. 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 seeking legal advice from the

lawyer or by a person in connection with legal proceedings or contemplated legal proceedings. It will rarely apply to property transactions. It is not available under s.330(11) POCA if the information is communicated or given with the intention of furthering a criminal purpose.

- 11.51** "Privileged circumstances" derives from POCA and the EU Directive. It is distinct from "legal professional privilege". Further guidance is found in Chapter 6 of the Law Society's AML Practice Note.

Lack of Training

- 11.52** Employees in the regulated sector who have no knowledge or suspicion of money laundering, even though there were reasonable grounds for suspicion, may have a defence if they have not received training from their employers. Employers may be prosecuted for a breach of the Regulations if they fail to train their staff in accordance with the requirements of Regulation 21.

Exemption from Disclosure Requirements - Overseas Criminal Conduct

- 11.53** No offence of failing to report will be committed if the property is derived from exempted "overseas criminal conduct".

- 11.54** By s.102 SOCPA, if conduct would be a criminal offence if it occurred in the UK, but it is known or believed on reasonable grounds that:-

- the relevant conduct occurred in a particular country or territory outside the UK where such conduct was not in fact unlawful under the criminal law then applying in that country or territory, and
- the conduct would have attracted a maximum sentence of 12 months' imprisonment or less if the conduct had occurred in the UK,

no report need be made to SOCA (except for certain gaming and other FSMA offences).

Consent for Pre-Event Disclosures

- 11.55** By s.336 POCA, a Nominated Officer must not give consent to a prohibited act being undertaken (as specified by ss.327, 328 and 329) unless he has specific authorisation from SOCA.

- 11.56** SOCA has 7 working days, starting with the first working day after the date of the disclosure to refuse consent (s.335 POCA). If nothing is heard within that time, the person who made the disclosure can proceed with an otherwise prohibited act without committing an offence. No-one can disclose to the client the reason for any delay since this may constitute "Tipping-Off" (s.333 POCA).

- 11.57** If consent is withheld and a "refusal" is notified under s.335(6) POCA, SOCA will have a further 31 calendar days (not working days) from the date on which the notice of refusal of consent is received by the person who made the disclosure in which to take further action, such as seeking a Court Order to restrain the assets in question. If nothing further is heard after the end of that 31-day period, the person who made the disclosure can proceed with the transaction without risk of committing an offence. No-one can disclose the reason for the further delay to the clients during this extended period, since this is likely to amount to "tipping-off" under s.333.

11.58 If a Nominated Officer permits the prohibited act to proceed without having obtained the appropriate consent from SOCA, he commits an offence (s.335 POCA).

11.59 A Nominated Officer does not commit an offence under s.335 if he gives consent to a transaction taking place when he genuinely does not know or suspect that money laundering is taking place.

Defence against Breach of Confidentiality - Protected Disclosures

11.60 A regulated person may make disclosure (s.337 POCA), where information is received which must be disclosed, even if he would otherwise be prevented from making disclosure because of the client's entitlement to privilege or confidentiality.

11.61 The protection also applies to those exercising a profession in a voluntary capacity, such as accountants or lawyers giving free advice (s.338(4) POCA).

Tipping-Off Offence

11.62 A person will commit the offence of tipping-off (s.333 and s.342 POCA) if he discloses information to any other person that is likely to prejudice an existing or future investigation, if he knows or suspects that a disclosure has been made, either to a Nominated Officer or by a Nominated Officer to SOCA, or if he knows or suspects that a money laundering investigation is being, or will be, carried out. The principal offence is due to be changed slightly under the TACT Regulations on 15 December 2007. The new law under s.333A-D will be incorporated into this Guidance after the Regulations have been made.

Penalties for Tipping-Off

11.63 The maximum penalty on conviction on indictment is term of 5 years' imprisonment or a fine or both. On summary conviction, the maximum term is 6 months' imprisonment or a fine not exceeding the statutory maximum or both.

Defences against Tipping-Off

11.64 There are two defences available against tipping off for those working in the regulated sector where:-

- the person can show that he did not know or suspect that the disclosure was likely to prejudice an investigation;
- a professional legal adviser makes a disclosure to a client or a client's representative in privileged circumstances in the context of giving advice or to any person in connection with legal proceedings or contemplated legal proceedings. This is unlikely to be available in a conveyancing transaction.

11.65 Making normal commercial enquiries (e.g. as part of CDD or EDD measures) prior to any report being made will not constitute "tipping off".

11.66 It is not tipping-off to notify a client about a Practice's reporting obligations under the AML legislation in its Terms of Engagement and/or its initial letters when accepting instructions.

- 11.67** Care must be taken not to “tip off” if it is known or suspected that a report has already been made or that an investigation is current or impending and enquiries are made in a way which discloses those facts. A Practice may wish to provide that only a Nominated Officer makes or directs any enquiries.
- 11.68** SOCA or the investigating law enforcement agency can be approached for advice if a Practice wishes to terminate a retainer after a SAR has been made or needs help to manage post-SAR situations to avoid the risk of “tipping-off”.

Statutory Offences - Terrorist Financing

- 11.69** Terrorist organisations require funds to plan and implement attacks, train militants, pay their operatives and promote their causes. TACT criminalises not only the participation in terrorist activities but also the provision of financial support for terrorist purposes.
- 11.70** Everyone is required to comply with TACT but there is a specific offence of failure to disclose knowledge or suspicion which applies to the regulated sector (including Licensed Conveyancers).

Principal Offences – Terrorist Financing

- 11.71** There are four principal terrorism offences in ss.15 - 18 of TACT. These are "fundraising", "use or possession", "arrangements" and "money laundering".

Fundraising

- 11.72** It is an offence under s.15 for any person to be involved in fundraising if he has knowledge or reasonable cause to suspect that the money or other property raised may be used for terrorist purposes. This offence can be committed by inviting others to make contributions, receiving contributions or making contributions towards terrorist funding, including gifts and loans. It is no defence that the money or other property passed as payment for goods and services.

Use or Possession

- 11.73** It is an offence under s.16 for any person to use or possess money or other property knowingly for terrorist purposes. This includes situations where a person has reasonable cause to suspect that these may be used for such purposes.

Arrangements

- 11.74** It is an offence under s.17 for a person to become involved in any arrangement which makes money or other property available to another if he knows or has reasonable cause to suspect that it may be used for terrorist purposes.

Money Laundering (Terrorism)

- 11.75** It is an offence under s.18 for a person to enter into or become concerned in any arrangement facilitating the retention or control of terrorist property by or on behalf of another person including, but not limited to, concealment, removal from the jurisdiction and transfer to nominees.

11.76 It is a defence if the person did not know nor had reasonable cause to suspect that the arrangement related to terrorist property.

Terrorist Property

11.77 "Terrorist Property" is defined as being:-

- money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation);
- proceeds of the commission of acts of terrorism (whether in whole or in part or whether directly or indirectly); and
- proceeds of acts carried out for the purposes of terrorism.

Defences

11.78 No offence is committed under s.15 – 18 if:-

- the act was done with the express consent of a constable, including civilian staff of SOCA; or
- a disclosure is made on a person's own initiative as soon as reasonably practicable after becoming involved in a transaction or dealing with terrorist property; and
- the disclosure is made to a constable or SOCA and discloses suspicion or belief that the money or other property is terrorist property; and
- the information is provided on which the suspicion or belief is based.

Penalties

11.79 The maximum penalty on conviction on indictment for any of these offences is a term of 14 years' imprisonment or a fine or both. On summary conviction, the maximum penalty is 6 months' imprisonment or a fine not exceeding the statutory maximum (or both).

Failure to Disclose Offences

11.80 The law on disclosures for knowledge or suspicion of terrorist financing will be changed by The Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 which are due to be made and implemented on 15 December 2007.

Regulated Sector

11.81 A person commits an offence under s.21A TACT if:-

- he knows or suspects, or has reasonable grounds for knowing or suspecting, that another person has committed an offence under any of ss.15 -18 TACT; and
- the information or other matter on which the knowledge or suspicion is based or which gave him reasonable grounds for such knowledge or suspicion, came to him in the course of a business in the regulated sector; and

- he did not disclose the information to a Constable (includes a member of staff of SOCA) or a Nominated Officer as soon as was practicable after it came to him.

Defences against failure to disclose

11.82 A person charged with these offences may have a defence if he can show that he had a reasonable excuse for not disclosing the information or other matter or the information on which the belief or suspicion is based was received in privileged circumstances without any intention of furthering a criminal purpose. There is also a defence under s.19 TACT if the person concerned makes an internal report in accordance with his employer's internal reporting procedures.

Penalties

11.83 The maximum penalty for failure to disclose on conviction on indictment is 14 years' imprisonment or a fine or both. On summary conviction, the maximum term is 6 months' imprisonment or a fine or both.

Consent for Pre-Event Disclosures

11.84 Currently, if a report is made, a transaction cannot proceed further without the actual consent of law enforcement or SOCA. If TACT is amended as anticipated on 15 December 2007 there will be a limited opportunity for deemed consent to be obtained from SOCA to proceed with a pre-advised transaction under s.21ZA on a 7-day deemed consent basis. The new law will be incorporated into this Guidance when the final form of the Regulations has been settled and the Regulations have been made.

Tipping Off Offence

11.85 When made, The Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 will introduce a tipping off offence identical in terms to s.21D TACT (as prospectively amended)

Other Terrorist Offences

11.86 Various other terrorist offences have been created.

11.87 The Al Qaeda and Taliban (United Nations Measures) Order 2006 and the Terrorism (United Nations Measures) Order 2006 created offences of providing funds or economic resources to terrorists.

11.88 Terrorists can be funded from income obtained legitimately, which can include charitable donations. As such, it will always be difficult to know or establish at what stage legitimate earnings actually become terrorist assets. Reference might be made to:-

- the consolidated Sanctions List including the names of sanctions targets and other information maintained by HM Treasury Asset Freezing Unit at www.hm-treasury.gov.uk/financialsanctions; and
- the list of proscribed organisations maintained by the Home Office at www.homeoffice.gov.uk.

The Money Laundering Regulations 2007

11.89 The Money Laundering Regulations 2007 (S.I. No. 2007/2157) are at www.opsi.gov.uk/SI/SI2007/20072157.htm and come into force on 15 December 2007.

GLOSSARY OF TERMS AND DEFINITIONS

ATCSA	Anti-Terrorism Crime & Security Act 2001
AML	Anti-money laundering
Beneficial Owner(s)	An individual or individuals or other legal person or persons who ultimately own or control the client on whose behalf a transaction or activity is being conducted (Regulation 6)
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.
CDD	Customer Due Diligence measures (including verification of the identity of any client or beneficial owner and investigations and enquiries made to obtain information about a potential client or beneficial owner and the nature of the business to be transacted to establish that it is consistent with the normal activities anticipated of a client or beneficial owner of that type and ongoing monitoring) (Regulation 5)
CLC	The Council for Licensed Conveyancers
Client	For a Practice of Licensed Conveyancers, a client is a person who is using, or may be contemplating using, any of the services provided by the Practice and, for the purposes of interpreting the Regulations, can be used interchangeably with the term "customer" in the Regulations.
CPS	Crown Prosecution Service
Criminal Conduct	Conduct which constitutes an offence in any part of the United Kingdom or would constitute an offence in the United Kingdom if it had occurred here - s.340(2) POCA (notwithstanding the limited exemption from the disclosure requirements for overseas criminal conduct under SOCPA)
Criminal Property	Property (of whatever nature or type and whether it is real or personal property) which constitutes a person's benefit from criminal conduct or which represents such a benefit (in whole or part and whether directly or indirectly) and the alleged offender knows or suspects that the property constitutes or represents such a benefit - s.340(3) POCA
CTF	Combating terrorist financing
Director	A person who is a director of a Recognised Body (including a Licensed Conveyancer)

Disclosure	The term (as used in POCA and TACT) for <ul style="list-style-type: none"> • an external report made to SOCA of actual or suspected money laundering or terrorist financing also known as Suspicious Activity Report (SAR) or • an internal report made to a Nominated Officer
EDD	Enhanced Customer Due Diligence (including enhanced ongoing monitoring) Regulation 14
EEA	European Economic Area
FATF	Financial Action Task Force: the international inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing
FSA	The Financial Services Authority
HM Treasury	the Government Department responsible for safeguarding the integrity of the financial system from exploitation by criminals and terrorists
Identification	Ascertaining the name of and other relevant information about a client or beneficial owner
Inchoate Offence	Action which anticipates a further criminal act
Independent Legal Professional	A firm or sole practitioner who, by way of business, provides legal or notarial services to other persons when participating (which includes assisting in the planning or execution of or otherwise acting for or on behalf of a client in the transaction) in financial or real property transactions concerning (i) the buying and selling of real property or business entities; (ii) the managing of client money, securities or other assets; (iii) the opening or management of bank, savings or securities accounts; (iv) the organisation of contributions necessary for the creation, operation or management of companies; or (v) the creation, operation or management of trusts, companies or similar structures (Regulation 3(9))
Internal Report or Internal Disclosure Report	A report made by a person working within a business in the regulated sector to the Nominated Officer appointed for that business
JMSLG	The Joint Money Laundering Steering Group
Law Society	Law Society of England and Wales
Licensed Conveyancer	Any person holding a Licence issued by the CLC (unless the context indicates otherwise)
MLRO	Money Laundering Reporting Officer

Money Laundering	An activity that would constitute an offence under ss. 327, 328 or 329 POCA (and, technically, an activity that would constitute an offence under s.18 TACT)
NCCT	Non Co-operative Country and Territory
Nominated Officer	A person in a regulated business nominated on behalf of that business to receive internal reports (disclosures) of known or suspected money laundering under Regulation 20(2)(d)(i) for the purposes of Part 7 POCA and Part 3 TACT and with responsibility to assess whether a SAR should be made
Occasional Transaction	A transaction (carried out other than as part of a business relationship) amounting to €15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked
Ongoing monitoring	Scrutiny of transactions undertaken throughout the course of a business relationship (including where necessary the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the client, his business and risk profile and keeping the documents, data or information obtained for the purposes of applying CDD measures up-to-date (Regulation 8(2))
PEP	Politically Exposed Person: an individual who is or has at any time in the preceding year been entrusted with prominent public functions and an immediate family member or known close associate of such a person (Regulation 14(5) and Paragraph 4 Schedule 2).
POCA	The Proceeds of Crime Act 2002 (as amended by The Serious Organised Crime and Police Act 2005 and as will be amended by The Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007)
Practice	A Licensed Conveyancer who is a Sole Practitioner or two or more Licensed Conveyancers in Partnership, a Recognised Body or a limited liability partnership (and includes any licensed conveyancer owner or manager in a Recognised Body or limited liability partnership)
Principal	Any Sole Practitioner; any Partner; (whether or not he is a Licensed Conveyancer) any Director of a Practice or any senior manager with AML/CTF responsibilities
Recognised Body	A body corporate recognised by the CLC under s.32 Administration of Justice Act 1985
Regulations	The Money Laundering Regulations 2007 (S.I. No. 2157)
Regulated Business	A business of a type and nature to which the Regulations are applied

Regulated Sector	The full range of the various types of persons, firms and companies carrying out businesses which are covered by and are subject to the Regulations
Relevant Person	A person to whom the obligations under the Regulations are applied by Regulations 3 and 4 (which includes independent legal professionals)
SAR	Suspicious Activity Report: a report made to SOCA
SDD	Simplified Due Diligence
Senior Management	The Principals and any other senior managers (or the equivalent) of a Practice who are responsible, either individually or collectively, for the management and supervision of the business of the Practice
Senior Manager	An individual, other than a Principal or Director, who is employed by the Practice and to whom responsibility has been given, either alone or with others, by the Principals or Directors for management and supervision within the Practice
SOCA	The Serious Organised Crime Agency
SOCPA	The Serious Organised Crime and Police Act 2005
TACT	The Terrorism Act 2000 (as amended by the Anti-Terrorism, Crime and Security Act 2001 by the addition of s.21A and as will be amended by The Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007)
Terrorist Financing	Any activity that would constitute an offence under ss.15 - 18 of TACT
Terrorist Property	Money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation) or the proceeds of the commission of acts of terrorism or the proceeds of acts carried out for the purposes of terrorism
Third EU Directive	The Third European Money Laundering Directive adopted in October 2005 (2005/60/EC) which updated European Community legislation in line with the revised FATF 40 + 9 Recommendations and repealed and replaced the earlier First and Second Directives
Tipping-Off	A tipping-off offence will be committed either:- <ul style="list-style-type: none"> • under s.333A POCA in the regulated sector if a person discloses that a disclosure falling under s.337 or s.338 POCA has been made or that an investigation into allegations that an offence under Part 7 of POCA has been committed is being contemplated or is being carried out; or

- under s.21D TACT if a person discloses that a disclosure falling under s.19 or 21A TACT has been made or that an investigation into allegations that an offence under Part 3 of TACT has been committed is being contemplated or is being carried out

UKFIU

The United Kingdom Financial Intelligence Unit of SOCA: the Unit which receives and analyses SARs concerning suspected proceeds of crime and terrorist financing and makes them available to law enforcement agencies for appropriate action.

Verification

Verifying the identity of a client by reference to reliable, independent source documents, data or information or of a beneficial owner through carrying out risk-based and adequate measures

Acknowledgments

In the context of the preparation of this Guidance for the profession of Licensed Conveyancers, sincere thanks and gratitude are extended to:-

- (i) The British Bankers' Association and the Joint Money Laundering Steering Group for their permission for the CLC to draw on the content of the Consultation Draft of its Guidance prepared for the Financial Sector in tailoring and applying its general principles to the type of services provided by Practices of Licensed Conveyancers;
- (ii) The Law Society for England & Wales for its co-operation in making its pre-consultation draft AML Practice Note available to assist the CLC in drafting guidance which is comparable with the guidance to be applied to Solicitors providing conveyancing services to the public; and
- (iii) The representatives of the various Supervisory Authorities in the Lawyers' Affinity Group of the AML Supervisors' Forum for their mutual support, co-operation and counsel.

