The purpose of this booklet is to provide a summary guide for ACCA practising members and their staff on their responsibilities as accountants with regard to money laundering and terrorist financing.

As members will be aware, comprehensive guidance on the responsibilities of practising accountants in these matters has been produced by the Consultative Committee of Accountancy Bodies (CCAB) and has been made available to ACCA members as Technical Fact Sheet 145, which is available at http://www.accaglobal.com/members/publications/technical_factsheets. That guidance has been formally approved by HM Treasury. The significance of official approval is that, in the course of any legal proceedings that might take place, the courts are obliged to take into account an accountant’s compliance (or otherwise) with the guidance in determining whether or not he has complied with the requirements of the law. Therefore, a member who complies with the CCAB guidance will be able to make reference to the fact of having done so in the course of any proceedings. For this reason members are strongly advised to consult the full guidance.

While similar responsibilities with regard to money laundering and terrorist financing are now imposed on a wide range of businesses and advisors, this booklet assumes a readership which is involved in the provision to clients of accountancy, audit and tax advisory services through practising firms. Inevitably, it does not contain the same level of detail as the CCAB guidance but is designed to be consistent with it. It will, hopefully, provide a useful outline of the issues involved for practitioners and all those members of their staff who are expected to be conversant with the law’s requirements on these issues. Members are reminded that, under the Money Laundering Regulations 2007, accountants in practice are required to be supervised for their compliance with their various legal obligations: in the case of ACCA firms, this supervision will be carried out by ACCA itself.

The references to legislation in this booklet are to provisions, including updated provisions, which are in force as at October 2008.

Thanks to David Duvall (Training Manager, Chantrey Vellacott DFK) for contributing summaries and examples.
abbreviations used in this booklet

AML      Anti-Money Laundering
CDD      Client due diligence (CDD)
CTF      Counter-terrorist financing
FATF     Financial Action Task Force
LLP      Limited Liability Partnership
ML       Money Laundering
MLRO     Money Laundering Reporting Officer
PEP      Politically Exposed Person
POCA     Proceeds of Crime Act 2002
SAR      Suspicious Activity Report
SOCA     Serious Organised Crime Agency
TA 2000  Terrorism Act 2000
TF       Terrorist Financing
contents

1 THE BACKGROUND
2 THE NATURE OF MONEY LAUNDERING
3 MONEY LAUNDERING UNDER UK LAW
4 COMPLIANCE RESPONSIBILITIES: CLIENT DUE DILIGENCE
5 COMPLIANCE RESPONSIBILITIES: IN-HOUSE PROCEDURES
6 REPORTING OF SUSPICIONS
7 DIRECT INVOLVEMENT BY ACCOUNTANTS IN THE MONEY LAUNDERING OFFENCES
8 THE FINANCING OF TERRORISM
9 TIPPING OFF
10 PROTECTION FROM LIABILITY

ANNEXE 1 THE OFFENCES AND PENALTIES
ANNEXE 2 RELIANCE ON CDD OBTAINED BY OTHERS
ANNEXE 3 SUGGESTED SOLUTIONS TO ‘ASK YOURSELF QUESTIONS’
The anti-money laundering (AML) and counter-terrorist financing (CTF) requirements which are now set down in UK law, and which form the basis for guidance issued by many different regulatory, professional and trade bodies, all derive from the establishment, in 1989, of the Financial Action Task Force (FATF). This international body was set up by the major economic powers in response to a growing concern about the internationalisation of financial crime, especially in connection with drug smuggling. It was considered that there was a pressing need for the creation of an authoritative international body which could take the lead in investigating the increasing sophistication of money laundering methodologies, and which could co-ordinate the international response to the problem.

The key element of FATF’s remit since its formation has been to issue high-level recommendations – The 40 Recommendations – on what governments around the world should be doing to tackle money laundering. These recommendations, which are updated periodically, identify the key elements which should be incorporated into national legal systems to fight money laundering and the steps which individual businesses should be taking to deter and detect money laundering activity. From the outset, the FATF Recommendations have enjoyed strong political support from most national governments. As a result the Recommendations have encountered little difficulty in becoming transposed into national law.

In Europe, the European Union (EU) has enthusiastically embraced the FATF agenda. The EU has issued three Directives on money laundering, in 1991, 2001 and, most recently, in 2005. Each of these Directives has been prepared soon after the publication of successive versions of the FATF Recommendations and has faithfully adopted the updated guidance in them. As it is obliged to do as a member state of the EU, the UK has proceeded to incorporate the various provisions of these Directives into UK law.

As far as practising accountants are concerned, the key development has been the updating of the FATF Recommendations in 2000 to extend the scope of the
recommended AML controls from the banking sector only to a much wider range of what are called ‘designated non-financial businesses’ (DNFBs). By virtue of this change, controls and responsibilities which were previously directed solely at the banking sector have been extended to cover accountants and auditors, tax advisors, lawyers, company formation agents, estate agents and many other categories of advisor and business. This extension of the scope of the FATF recommendations was quickly reflected in the EU’s Second Money Laundering Directive, enacted in 2001, and not long after that in new UK legislation, namely the Money Laundering Regulations 2003, made under the Proceeds of Crime Act 2002 (referred to hereafter as POCA). It was this legislation, which came into full effect in March 2004, that first obliged practising accountants to assume the extensive AML/CTF responsibilities which are outlined in this booklet.

The Third EU Directive, that enacted in 2005, has resulted in a number of changes being made to the requirements that were introduced in the UK in 2004 – some of these have the effect of increasing the burden on practising accountants, while others do the opposite. To accommodate these changes, the 2003 Regulations have been replaced by the Money Laundering Regulations 2007 (SI 2007/2157), hereafter referred to as the Regulations.

POCA is a wide-ranging piece of legislation and deals with much else apart from money laundering. But in this specific context, POCA addresses the following matters:

- It sets out the legal definition of the term ‘money laundering’ and specific money laundering offences
- It establishes the ‘regulated sector’, i.e. the collection of individuals and businesses that have AML/CTF responsibilities in the UK
- It creates responsibilities for all those in the ‘regulated sector’ to disclose relevant information relating to money laundering to the authorities
- It prohibits those who disclose information to the authorities from ‘tipping off’ clients in ways that might prejudice any investigations conducted into them.

The Regulations supplement these fundamental legal rules. They specify the range of individuals and businesses which comprise the ‘regulated sector’ for AML/CTF purposes and set out detailed compliance responsibilities for all those in the sector. The list of those in the ‘regulated sector’ includes any person who acts, as an individual or through a firm, as a statutory auditor, a tax advisor (someone who provides tax advice to other persons by way of business), or an external accountant (someone who provides accountancy services to other persons by way of business). This booklet is aimed at all those in these categories, always remembering that individual firms of ‘accountants’ might conduct accountancy, audit and tax work, as well as other activities that are regulated by POCA, such as company formation work.

Similar disclosure responsibilities to those contained in POCA apply, via the Terrorism Act 2000, to the reporting of information in circumstances where involvement in terrorism is suspected.
In broad terms, the concept of money laundering refers to the process whereby those who have acquired financial benefit from criminal activity seek to distance, or dissociate, that benefit from the criminal activity that gave rise to it. By the use of various techniques which have the aim of ‘cleansing’ criminal property of its criminal origins, the object is to enable the perpetrators to retain the financial benefit of their crimes by making it impossible for the judicial authorities to establish conclusively the criminal origins of the funds. In short, the process of money laundering is about making crime pay.

The above is a general description of what the process of money laundering is about. It is not, of course, a legal definition. The FATF Recommendations have gone some way to standardising the way in which different countries define money laundering for legal purposes. The Recommendations suggest that individual countries should seek to define money laundering as activity which involves dealing with the proceeds either of a crime which is specified in FATF’s list of ‘serious’ offences – these include fraud, bribery and drug smuggling – or, alternatively, of a crime which carries with it a minimum jail sentence of one year. This approach has been adopted in the EU Directives.

The UK has gone further than this minimum standard and has adopted an ‘all-crimes’ approach to the definition of money laundering. Under POCA, money laundering is treated as being, essentially, the conscious dealing with the proceeds of any crime on the statute book, regardless of the materiality of the particular crime concerned and regardless of the materiality of the proceeds themselves: if a perpetrator knows or suspects that the property he is dealing with represents the benefit of a crime of any kind, then he is likely to be committing a money laundering offence in the UK.

What this means is that accountants (and all others who have AML responsibilities under UK law) have to be alert to a far wider range of potential criminal activity than do their counterparts in other countries. This has implications for, in particular, their responsibilities to report suspicions of money laundering activity to the authorities (chapter 6 of this booklet).
money laundering under UK law

The legal understanding of the term money laundering in POCA revolves around the central concept of ‘criminal property’.

Property for this purpose is defined very broadly as any sort of property, wherever it is situated, including money, all forms of property (real, personal and intangible) and things in action. Property is ‘criminal property’ if it constitutes or represents a person’s benefit from criminal conduct AND the alleged offender knows or suspects that it constitutes or represents such benefit. And criminal conduct is – subject to chapter 6 below - any conduct which constitutes an offence in any part of the UK or would be an offence if it occurred here.

Thus, if a person commits a criminal offence in the UK, or commits an offence outside the UK which would be an offence if it were committed here, and that offence leads to the acquisition of benefit – whether by the perpetrator of the crime or someone else – and some person knows or suspects that the benefit has derived from the commission of the offence, then the basic elements of money laundering are present.

If, on the other hand, a crime is committed which produces no ‘benefit’ for the offender or anyone else, for example an assault, or if the person who acquires property genuinely does not know or even suspect that the property has criminal associations, the matter will not qualify as a money laundering matter. This latter point is especially important in the context of formulating ‘suspicions’ of money laundering on the part of clients or others: unless a person is consciously aware of the actual or possible criminal origins of the property in question, that person can not commit a money laundering offence, and that needs to be borne in mind in deciding whether or not you have a ‘suspicion’ about that person’s activities.

This central concept of criminal property, however, is only the starting point for the real definition of ‘money laundering’ as it affects accountants and others. The term ‘money laundering’, for the purposes of all the responsibilities of regulated persons under POCA and the Regulations, is explained in section 340(11) of POCA as follows:
money laundering under UK law (continued)

i) an act which constitutes an offence under section 327, section 328 or section 329 of POCA

ii) an act which constitutes an attempt, conspiracy or incitement to commit an offence under i)

iii) an act which constitutes aiding, abetting, counselling or procuring the commission of an offence under i) or an act which would constitute an offence under i) ii) or iii) if carried out in the UK (but, again, see the clarification in chapter 6).

The specific offences referred to in section 340(11) are as follows:

- section 327 – it is an offence to conceal, disguise, convert or transfer criminal property or to remove criminal property from England, Scotland, Wales or Northern Ireland. Concealing or disguising property includes concealing or disguising its nature, source, location, disposition, movement or any rights attaching to it.

- section 328 – it is an offence to enter into, or become involved in, any arrangement which one knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

- section 329 – it is an offence to acquire, use or possess criminal property (other than for ‘adequate consideration’).

Examples of the more serious offences that will be caught by section 327 are:

- tax evasion
- theft
- bribery
- fraud
- smuggling, including drug trafficking
- illegal arms sales

As has been previously explained, however, because of the UK’s ‘all crimes’ approach to money laundering, the popular conception of money laundering as involving large-scale operations and the transfer of money through several countries is far from being the whole picture. That sort of activity certainly happens; but there are many, more common matters that risk being caught. For example when:

- laundered funds are used to buy an expensive car, which is then sold on to another dealer, and a ‘respectable’ cheque is received from that dealer

- an investment is bought and sold through a stockbroker or financial adviser in a similar way

- tax is deliberately overpaid and a refund obtained from HM Revenue & Customs

- money is deposited for safe-keeping with a firm of advisors and subsequently withdrawn.

A practising accountant might be in a position to facilitate any of the above, and could thus commit an offence under section 328: However, even when this happens, an offence will not be deemed to have been committed if the accountant reports the
transaction he is involved in to the Serious Organised Crime Agency (SOCA) – see chapter 7 - and SOCA's consent is received.

An accountant could also take possession of a client’s assets – for example, while acting as an insolvency practitioner – and commit an offence under section 329 if those assets had been procured by the client illegally. Again, no offence will be committed if the accountant reports to SOCA.

Accordingly, and to summarise the above, any person will commit a ‘money laundering’ offence under POCA if he deals, in any of the ways covered in sections 327-329, with property that he knows or suspects is the result of criminal conduct as committed either in the UK or elsewhere (provided it would amount to criminal conduct here). A person will also commit a money laundering offence if he attempts, conspires or incites a person to commit one of the offences, or aids, abets, counsels or procures the commission of any of them. A number of exemptions from and defences against these offences are set out in the legislation and they are discussed later on.

Having introduced the definition of money laundering under UK law, the specific responsibilities of accountants under the law are dealt with in the remainder of this booklet as follows:

- the duty to carry out Client due diligence (CDD)
- the duty to put in place in-house policies and procedures to guard against money laundering
- the duty to report known or suspected involvement in money laundering
- the responsibility to seek consent to act in respect of actual or possible involvement in money laundering activity
- the duty not to ‘tip off’
- the duty to report known or suspected involvement in the financing of terrorism
Client due diligence, or CDD, is the key operational responsibility of practising accountants under the UK law on money laundering. The overriding purpose of these requirements is to ensure that accountants are able to comply with the dictum ‘Know your Client’ - they should not only know who their clients are but they should also understand the motives of the client and the nature of his business. Only if the accountant understands what is normal and usual in the client’s business will he be in a position, later on, to recognise things which are abnormal or unusual, and hence potentially ‘suspicious’. Accordingly the rules on CDD are essentially intended to ensure that accountants are able to remain in control of the engagement and that their offices are not used for criminal purposes. An indirect aim of the rules on CDD is to make those who may be trying to launder money aware that, should they approach an accountant for help, the accountant will be obliged by law to take steps which may lead to the detection of their criminal activities.

What does CDD amount to?
The essential element of CDD is that the accountant must take steps to identify who the prospective client is and verify the person’s identity by reference to independent and reliable source material. Such material may include documents issued by local authorities (e.g. council tax bills), by Government departments or agencies (e.g. company and personal details held on file at Companies House) and bank statements. For the purpose of verifying the identity of individuals, any materials which include photographic identification as well as other relevant details (e.g. passports) are considered to be particularly strong evidence. As part of the verification process, members may, if they think fit, make use of electronic identification services which contain databases of information on identity. However, before placing reliance on such data they should seek to satisfy themselves as to whether it is likely to be sufficiently reliable, comprehensive and accurate.

In the case of a client that is a limited company, an LLP, a trust or any other sort of legal entity, information must also be acquired on the ownership and control
structure of the entity. The rules require the accountant to identify the ‘beneficial owner’ of the entity – this will be, in the case of a company, any person who owns or controls, directly or indirectly, more than 25% of the shares or voting rights (or who otherwise exercises control over the directors, in other words a person who acts as a ‘shadow director’).

Establish the nature of the engagement
CDD also involves acquiring information on the purpose and intended nature of the business relationship which the prospective client wishes to have with you. So you must invite the client to specify exactly what services he is asking you to provide.

The risk-based approach
Under the 2007 Regulations, the carrying out of CDD checks is made expressly subject to the assessment of risk. What this ‘risk-based approach’ means is that individual firms are expected to weigh up the perceived risk of dealing with particular clients and prospective clients and take this assessment into account in determining the extent and range of information that is likely to be needed in order to enable them to satisfy themselves about the identity of the client concerned (and indeed in deciding whether or not they wish to act for that client at all). By virtue of this approach, CDD is not to be approached on a ‘one size fits all’ basis – the determination of risk is now an integral element of the process of taking on new clients and the assessment you make of the level of risk will have implications for the amount of work you have to do to establish identity. Firms may decide to identify a risk threshold and avoid doing business altogether with clients which are likely to pose a risk over a certain level.

When must CDD be carried out?
The Regulations specify the occasions on which CDD checks must be carried out.

The first such occasion, and the most obvious and logical time for carrying out such checks, is when you are approached for the first time by a new prospective client.

But the rules also say that you are required to carry them out at the following other times:

- when you carry out an ‘occasional transaction’ (i.e. an ad hoc transaction of a value of over 15,000 euros)
- when you suspect ML/TF is going on
- when you have doubts about the ID information that you have previously obtained.

In the case of new clients, the checks should normally be completed before you formally enter the relationship and undertake work for that client. That being said, the Regulations do accept that, in some cases, it is acceptable for the checks to be completed ‘during the establishment of a business relationship’ but only if delay is necessary not to interrupt the normal conduct of business and if there is a low risk of money laundering or terrorist financing. Such a scenario is likely to apply in respect of urgent insolvency appointments but not generally.

Maintenance of CDD records
All the documents that you obtain for the purpose of carrying out CDD checks must be retained for a minimum of five years from the end of the business relationship or the date of any occasional transaction which might have been carried out. Where you provide CDD information to other persons (see under ‘Reliance on CDD

compliance responsibilities: client due diligence (CDD)
client due diligence (CDD) (continued)

carried out by others’, below) you are required to retain those records for five years from the date on which you provide them.

‘Simplified’ due diligence
As a rule, the standard CDD checks are not required to be carried out where the client is of a type which is specified in regulation 7 of the Regulations, namely

• a listed company
• a credit or financial institution which is subject to AML requirements
• a UK public authority and certain specified public authorities elsewhere in the European Economic Area (EEA)

In respect of clients which fall within any of these categories, you are not required to carry out the CDD checks at the outset of a new relationship, when carrying out occasional transactions or (obviously) when you have doubts about the information you have previously obtained. That notwithstanding, you are still expressly required to carry out CDD checks when you suspect ML/TF is going on.

‘Enhanced’ due diligence
As part of the risk-based approach referred to above, firms are expected to approach the CDD process with a view to identifying situations which by their nature can present a higher risk of ML or TF. For example, a client which is a company which is owned by an offshore trust may be considered to offer higher risk than an individual client who is well known to you. For higher-risk situations, the Regulations require accountants to carry out what is referred to as ‘enhanced’ due diligence (EDD), meaning that they should take extra care and carry out additional checks in the process of verifying identity.

There are two specific types of ‘high-risk’ situation where the Regulations actually require accountants to carry out EDD. These are:

• where the new client has not been physically present for identification purposes
• where the new client is a ‘politically exposed person’ (PEP) – a PEP is someone who is or has in the last year exercised a prominent public function in a foreign country, an EU institution or an international body, or a family member or known close associate of such a person.

In the latter case, the accountant is required to take ‘adequate measures’ to establish the source of wealth and funds of the PEP, and senior management approval for the taking on of the PEP must be sought and given within the firm.

The purpose of making special provision for PEPs is, quite clearly, to recognise the possibility that persons holding political power may have or have had means of access to public funds, and means of transporting them, that other citizens will not have, and to ensure that accountants are doubly aware of the heightened risk that such persons may consequently present.

But as long as you carry out the EDD and the checks are completed to your satisfaction, there is no hard and fast rule to prevent you from acting in respect of either a client whom you have not met or a PEP, should you wish to do so.
Reliance on CDD carried out by others
Carrying out the required CDD checks will invariably involve a degree of administrative work and may, depending on the amount of information you think you need in individual cases, delay the commencement of work for the new client.

The Regulations say, however, that you are not obliged to undertake all the CDD work yourself, and that you may seek to rely on the CDD checks that have been carried out by another person, such as, for example, the new client’s previous accountant. Any decision on whether to seek to rely on someone else’s CDD work is your own to make, but you should remember that, if you do place reliance in this way, you will remain liable under the Regulations for any failure to comply with the CDD requirements.

Reliance can only be made on certain classes of person, namely those that are covered by regulation 17 and Schedule 3 of the Money Laundering Regulations 2007 – the principal classes for this purpose are listed in Annexe 2 of this booklet.

Should you wish to rely on another person’s CDD information in respect of a particular client, you as an ACCA member have the right to approach the person concerned for permission to rely on it. If the other person consents, then he is required under the Regulations to supply you, as soon as is practicable, with any information obtained on the client (and any beneficial owner) when carrying out CDD checks, together with copies of identification and verification data on the client’s identity (and any beneficial owner). The same applies in reverse if you are approached with a view to placing reliance on your own CDD data – if you consent to the other person relying on your data, you are obliged to pass on the aforementioned information. It is an offence not to comply.

Since accountants who rely on other persons’ CDD records retain residual responsibility for satisfying themselves about the identity of clients, the decision as to whether or not to rely on others may be a difficult one to make. They should bear in mind that they will continue to have to carry out their own CDD checks where they begin to form suspicions and where they begin to doubt the veracity of the data that has been obtained.

Where another person seeks to rely on your CDD data, you should first obtain the consent of the client (or former client) to you doing so, and remember that you will need to retain the original CDD records for a further five years after the transfer date. But even if the client or former client agrees, it is still your decision as to whether or not to give your consent.

Ongoing monitoring of the business relationship
In keeping with the spirit of the ‘Know your Client’ concept, the Regulations require accountants to monitor the transactions being carried out by and on behalf of the client throughout the business relationship – this is referred to as ‘ongoing monitoring’. The aim behind this is to enable the accountant to remain aware of the scale and nature of the client’s business affairs and to enable him to become aware of transactions which are so unusual, in size or nature, that they might give him cause to suspect ML/TF. Ongoing monitoring may also help to ensure that CDD data is kept up-to-date, as is required by the Regulations.
client due diligence (CDD) (continued)

AT A GLANCE

• Client due diligence (CDD) is the procedure whereby a relevant person (including an accountant in practice) takes steps to identify a prospective client and verify that identity.

• It involves acquiring information on the nature and purpose of the engagement.

• It must also be performed:
  • In respect of non-recurring business worth over 15,000 euros
  • when money laundering or terrorist financing is suspected
  • when there are doubts about the quality of the information received from the prospective client.

• Extra procedures are required where the client is not physically present or is a politically exposed person (‘enhanced due diligence’).

• In certain situations reliance may be placed on other professionals who have already carried out CDD procedures on a prospective client.

Ask yourself – CDD (suggested solutions can be found at Annexe 3)

1 A well-established client recruits a new finance director. Do you think that he should provide the auditors with proof of identity?

2 Your firm has been asked to carry out some accounting work for a local authority. Do you need to confirm the authority’s identity, and if so, how?

• Standard CDD procedures are not necessary in cases where the client is of a certain low-risk type (‘simplified due diligence’).
Part 3 of the Regulations contains a number of detailed requirements for firms to put in place in-house systems and controls. While CDD checks are carried out in order to enable the firm to establish the credentials of individual clients, the systems and controls specified in Part 3 are aimed at creating an overall environment that is hostile to ML/TF activity and at equipping the firm as a whole with the skills and information that will help it to detect ML/TF where it goes on.

(i) The Money Laundering Reporting Officer (MLRO)

All firms of practising accountants are required to appoint a person to act as the firm’s ‘nominated officer’, a role more commonly known as Money Laundering Reporting Officer (MLRO). This person acts as the liaison point between the firm and the Serious Organised Crime Agency (SOCA) in respect of suspicious activity reports (SARs) and requests for consent under section of the Proceeds of Crime Act.

The MLRO performs the key role within the firm on all matters relating to AML/CTF activity. He is the person to whom all other staff must submit any reports they might need to make regarding suspicious activity. The MLRO is then personally responsible under POCA for making final decisions on behalf of the firm concerning whether matters need to be reported to SOCA in the form of SARs. The MLRO also acts as the liaison point between the firm and SOCA with regard to applications for ‘consent’ for the firm to act in respect of matters which it considers might constitute money laundering offences under sections 327-329 of POCA.

(ii) AML/CTF Policies

A firm must have policies and procedures on the following matters

- CDD measures/ongoing monitoring
- reporting of suspicious transactions
- internal control
- risk assessment and management
- compliance monitoring
- the identification of complex or unusually large transactions, or unusual patterns of transactions which have no apparent economic or visible lawful purpose
In practice, the preparation of policies and procedures on these matters, and the communication of them to partners and staff of the firm, will be the responsibility of the firm’s MLRO.

(iii) Education and training of staff

All ‘relevant’ employees in a firm must be made aware of the law on ML/TF and given regular training on how to recognise and deal with transactions which may be related to ML/TF.

The question of who, within a firm, is to be considered to be a ‘relevant’ employee is not dealt with further in the Regulations and is left to individual firms to decide in the context of their own circumstances. The firm’s MLRO should certainly be given support to undergo all necessary training. Otherwise, it is considered that the requirements regarding awareness and training should be applied at least to all partners (including sole practitioners) and all ‘client-facing’, qualified staff. In addition, firms should consider providing training to those who look after the firm’s finances and those who procure and manage client services. Firms may decide to provide the same training to all ‘relevant’ staff, or else they may choose to provide training which is tailored to the particular roles of the individual staff members concerned.

It should be borne in mind that, for an employee of an accountancy firm, it is a defence against any charge of failing to make a suspicious activity report (see chapter 6) that their employer had failed to provide them with the required training.

AT A GLANCE

Firms are required to implement in-house systems and controls to ensure ML and TF are prevented as far as possible. These should include:

- the appointment of a Money Laundering Reporting Officer
- the adoption of detailed policies and procedures for complying with the Regulations
- relevant employees of firms must be given regular training to ensure awareness of the law and ability to recognise suspicious transactions.

Ask yourself – in-house procedures

1. As MLRO of your firm, what advice should you give to new staff about reporting suspicious activities?

2. A new manager joins your firm and tells you that he has had recent anti-money-laundering training in his previous firm. Does your firm need to give him any further training?
The aspect of the FATF-derived rules which impacts most directly on professional advisers is the requirement for them to report to the authorities when they come across information which gives them cause to believe or suspect that money laundering activity is going on.

The legal requirement to report applies to all accountants within practising firms but the way they comply with this obligation will differ. For all except the firm’s MLRO, the requirement to report will mean making a report ‘in-house’ to the MLRO: the responsibility to make suspicious activity reports (SARs) direct to the Serious Organised Crime Agency (SOCA), on behalf of the firm, is the personal responsibility of the MLRO.

When must you report?
The key requirement, found in section 330 of POCA, is for accountants to make a report if – and only if – all the three conditions below are met:

i) if you know or suspect, or have reasonable grounds for knowing or suspecting, that some person is engaged in money laundering

ii) if the information on which you base your knowledge or suspicion has come to you in the course of your business (which will be, in the case of a practising accountant, your work in providing accountancy services by way of business) and

iii) if either a) you can identify the person who you think may be engaged in money laundering or can provide information concerning the whereabouts of the laundered property or b) you believe that the information you have may assist in the identification of the person engaged in the laundering or the whereabouts of the laundered property.

Where these three conditions are met, a report must be made ‘as soon as is practicable’. The same conditions apply both to the reporting of information, in-house, to the firm’s MLRO, and to the making of SARs by the MLRO to SOCA.

The various elements contained in these paragraphs are discussed further overleaf.
Criterion i) - Suspicion and ‘reasonable grounds’

The first criterion provides that, before you become obliged to report, you must know or suspect, or have reasonable grounds for knowing or suspecting, that some other person is engaged in money laundering.

If you actually ‘know’ that your client, or someone else, is engaged in money laundering, then your situation is quite straightforward – the first criterion is met. The situation will be more complicated if you only have a ‘suspicion’ that it is going on, or if the objective test - of reasonable grounds - applies to what the law expects that you should know or suspect in the circumstances of your case.

Taking the concept of ‘suspicion’ first, the law does not offer any further explanation or definition of this term. Therefore, it falls to be interpreted by reference, primarily, to case law precedents and the settled understanding of the concept of suspicion which has developed in association with those precedents.

Case law suggests that, to have a valid ‘suspicion’, one needs to have a state of mind which is somewhere between simple speculation and knowledge based on evidence. Simple, unfounded speculation on your part that a client may be laundering money, or that low-level crime is endemic in particular business sectors – and therefore is ‘probably’ being carried on by a client who works in such a sector - is not sufficient to create a valid suspicion for the purposes of POCA.

The following extracts from case law may be helpful in this context:

‘A suspicion that something exists is more than a mere idle wondering whether it exists or not: it is a positive feeling of actual apprehension or mistrust, amounting to a slight opinion, but without sufficient evidence.’ (Queensland Bacon Pty Ltd v Res [1966] 115 CLR 266)

‘It seems to us that the essential element in the word ‘suspect’ and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.’ (Da Silva [2006] EWCA Crim 1654)

So when it comes to considering whether you as the external accountant, auditor or tax advisor actually have a suspicion, which would require you to make a report, you need to consider whether the information you have fulfils this test of amounting to more than a hunch (but falling short of actual knowledge).

But even if you neither know nor consciously suspect money laundering is going on, you are also required to report if you have ‘reasonable grounds’ for doing so. By virtue of this second, ‘objective’ test, the requirement to report will probably apply to you if the facts of the particular case suggest that a person of your qualifications, experience and standing would be expected to draw the conclusion that those facts amount to either knowledge or suspicion of money laundering. The main purpose of the objective test is to ensure that accountants (and other regulated persons) are not able to argue that they failed to report because they had no conscious awareness of the money laundering activity, for example by having turned a blind eye to incriminating
information which was available to them, or by claiming that they simply did not realise that the activity concerned amounted to money laundering.

The presence of the objective test, as well as the subjective test, encourages accountants who are not sure whether the information they have stands up as credible knowledge or suspicion, to err on the side of caution and treat the matter as being reportable. Accountants are encouraged to adopt a healthy level of professional scepticism and to make reasonable enquiries if they come across information which potentially forms the beginning of a suspicion. If they are unsure of the action to be taken, they should discuss the matter with their firm’s MLRO (or the ACCA’s advisory help line).

While, to date, there has been no case law to expand on exactly what is covered by the term ‘reasonable grounds’, it is considered that the presence of higher than usual risk factors in a particular scenario should not in itself amount to reasonable grounds for the purposes of formulating suspicions. Thus, just because particular business models, e.g. cash-based businesses, or particular business structures, such as complex overseas trusts and company structures, are widely thought to offer the potential for criminals to launder money, that in isolation would not amount to ‘reasonable grounds’.

Criterion ii) – in the course of your business

The second condition which must be met for you to be required to report is that the information on which you base your knowledge or suspicion under i) above must have come your way in the course of your regulated business.

Where information on potential money laundering activity comes your way during your leisure activities and is unrelated to your business, the second pre-condition for the reporting requirement is not met.

Criterion iii) – information on the identity of the launderer and the whereabouts of the laundered property

The third condition is that you must have information which can either identify the person who is responsible for the alleged money laundering activity or determine the whereabouts of the property itself.

Alternatively, the condition is met if you think that the information you have, while not meeting the foregoing test, will help SOCA to identify the offender or the trace the property.

It is essential that reporting decisions are made on the strength of an accurate assessment of whether the three conditions apply. This is because the protection from civil liability for breach of trust or breach of confidentiality that the firm enjoys courtesy of section 331 POCA (see chapter 10 below) only applies if the report as been made on the grounds set out in the Act. Therefore, a firm which reports client information to SOCA when the three conditions are not met may expose itself to legal action from the client concerned.

When may you not report?

If the three pre-conditions for reporting are met in your case, then on the face of it you have a legal responsibility to make a report under section 330, whether it be an in-house report or – in the case of an MLRO - a report to SOCA. But the following provisions should be borne in mind:
It is a defence for an employee against a charge of failing to report that he did not know or suspect that money laundering was going on and that his or her employer had not complied with the obligation under the Regulations (see chapter 5 above) to provide adequate and regular training on money laundering/terrorist financing matters to staff. By virtue of this defence, there is no presumption that the untrained employee should have known or suspected that money laundering was going on. This defence is not available to the MLRO.

It is a defence against any charge of failing to report that you have a ‘reasonable excuse’ for not doing so. Thus far, there has been no case law to interpret what sort of excuses would be accepted but it has been widely suggested that a defence might be successful where the accountant has been subjected to threats from the alleged wrongdoer that there would be violent consequences if he did choose to report. This defence applies both to the MLRO and everyone else with reporting responsibilities in a firm.

Professional legal advisors are exempt from reporting if the information on which they would otherwise base their knowledge or suspicion came their way in ‘privileged circumstances’, which means in the course of either giving legal advice to the client or in connection with actual or contemplated legal proceedings. So if an advisor comes across information, in such circumstances, which would otherwise cause him to form a reportable suspicion, the usual requirement to report does not apply and the advisor should not file a SAR. The exception to this is where the information is given to the advisor with the intention (on the part of the client or any other person) to further a criminal purpose – what is often referred to as the crime/fraud exception): in this situation, the exemption is lost and the usual rules will apply.

This exemption, originally applied to lawyers only, has since been extended to those accountants, auditors and tax advisors who qualify as ‘relevant professional advisors’. The test is met if an accountant, auditor or tax advisor is a member of a professional body which:

a) tests the competence of those seeking admission to membership, and

b) imposes and maintains professional and ethical standards for its members, and imposes sanctions for non-compliance with those standards.

This definition is sufficient to cover ACCA (and the Institutes of Chartered Accountants and the Chartered Institute of Taxation). Accordingly, ACCA members in practice qualify as ‘relevant professional advisors’ and hence qualify for the privilege reporting exemption.

Since the privilege reporting exemption rests on the advisor being in ‘privileged circumstances’, care should be taken to determine whether you are in fact in that situation. Examples of situations where an accountant might meet the ‘legal advice’ condition are where you:

• give advice to a client on the
ACCOUNTANTS AND MONEY LAUNDERING

interpretation or application of an element of tax law and thereby aim to assist the client to understand his or her tax position

• give advice to directors on their legal duties and liabilities, e.g. on wrongful trading under the Insolvency Act 1986

• give advice to a client on employment law

An accountant might meet the ‘litigation advice’ condition if he represents a client at a tax tribunal or assists a client by taking witness statements in respect of litigation.

iv) it was stated in chapter 3 above that property is ‘criminal property’, and thereby liable to lead to the commission of a money laundering offence, if it results from the commission of an act abroad which would be a criminal offence if committed in the UK. A derogation from this hard and fast rule, which was introduced subsequent to the introduction of POCA in 2002, is that certain, relatively minor acts can be ignored for this purpose. By virtue of the derogation, property is not to be deemed criminal property if the accountant knows, or believes on reasonable grounds, that the acts concerned were lawful in that other country, even if they would be criminal offences if committed here. The only qualification to this is that the derogation only applies if the criminal act concerned would attract a maximum prison sentence of 12 months or less in the UK. So if the act in question, even if legal abroad, would attract a jail sentence of more than one year in the UK, then any property which arises from it would always amount to ‘criminal property’ for the purposes of POCA and could lead to the commission of a money laundering offence and hence a reporting responsibility.

Also, remember that, for property to be criminal property, it must constitute or represent benefit which the alleged offender knows or suspects derives from criminal conduct. So if you are satisfied that any offence your client may have committed, and which has produced what would technically be deemed to be ‘criminal property’, has been innocent or accidental, then this would not, at this stage at least, amount to a potential money laundering matter. Where, however, a client refuses to correct an innocent error which gave rise to proceeds or benefit, or unreasonably delays doing so, this may suggest criminal intent on the part of the client, and at that stage the accountant would need to reconsider whether or not the conditions for reporting the matter have been met. Examples of incidents which may result in you having to advise a client to correct innocent or accidental defects include the following:

• Offences which do not give rise to financial proceeds or other benefits, such as the late filing of annual accounts. However, a persistent failure to file accounts within the time allowed, or at all, may disguise a larger offence, such as fraudulent trading or credit fraud involving the concealment of a poor financial position.

• Mis-statements in tax returns, but which are corrected before the tax becomes due.
The materiality of knowledge and suspicions for reporting purposes
If the tests which give rise to the reporting duty are met, and no derogation or exemption is available, then a report must be made under section 330 of POCA. There is no threshold of materiality which applies either to the nature of the criminal activity which has been undertaken or to the amount of proceeds or benefit which has derived from that activity. The following extract from a court ruling in a family law case makes this very clear:

‘The Act [POCA] makes no distinction between degrees of criminal property. An illegally obtained sum of £10 is no less susceptible to the definition of “criminal property” than a sum of £1million. Parliament clearly intended this to be the case. Whatever may be the resource implications, the legal profession would appear to be bound by the provisions of the Act in all cases, however big or small.’ (P v P [2003] EWHC Fam 2260)

Submitting SARs
SOCA has devised a pro-forma Suspicious Activity Report form, which can be downloaded from the SOCA web site (www.soca.gov.uk). SOCA prefers these forms to be completed and submitted electronically, although they may also be filled in hard copy form and delivered by post to UK FIU, PO Box 8000, London SE11 5EN. SAR Online, SOCA’s web-based reporting mechanism, can be used by anyone with access to the internet. In addition to the ‘standard’ SAR form, there is also available, from the SOCA website, a Limited Intelligence Value SAR form, which is designed to be appropriate in respect of situations where the known or suspected criminal activity is not of substantial intelligence value.

Guidance on how to complete both the standard and the limited intelligence value SAR forms, and guidance on the circumstances in which the latter form might be more appropriate, is also available from the SOCA website.

Continuing to work for the client after making a SAR
There is nothing to prevent a firm continuing to work for a client after submitting a SAR on that client to SOCA. After all, the contents of a SAR are only required to be based on a suspicion of money laundering on the part of a client, rather than an allegation. But, in addition to heeding the rules on tipping off the client that a SAR has been filed (see chapter 9), your firm’s MLRO will also need to consider whether continuing to act for the client in respect of the activities covered by the SAR may cause it to commit any of the offences set out in sections 327-329. If there is such a risk, then the MLRO would need to consider making an authorised disclosure and applying for consent to act (see next chapter), in which case work related to the transaction concerned should not be carried out until express or implied consent is received from SOCA.

Forming suspicions and the CCAB guidance
It is important to note that, under section 330(8) POCA, in determining whether or not an accountant should have made a report of his suspicions, either to the firm’s MLRO or to SOCA, the courts are bound to take into account whether that accountant has followed the guidance issued by CCAB (ACCA Fact Sheet 145). Therefore, if members do follow that guidance in the process of making their decisions as to whether or not they have a suspicion which
needs to be reported, that will have the effect of providing a justification for their actions which the courts are obliged to consider.

**AT A GLANCE**

- Accountants in practice must report to SOCA as soon as possible if:
  - they know or suspect that someone is engaged in ML or TF; and
  - the information has come to them in the course of their business; and
  - they can identify or assist in identifying the person or people under suspicion on the laundered property.
- Suspicion may fall short of actual knowledge but is more than a vague hunch.
- Accountants are not obliged to report if:
  - They have a reasonable excuse for not doing so (this might involve a threat of violence)
  - professional legal privilege applies.
- There is no threshold of materiality for either the nature of the criminal activity or the amount of the associated proceeds.
- Report forms can be downloaded from [www.soca.gov.uk](http://www.soca.gov.uk) and should normally be submitted online.
- Reporting a suspicious activity to SOCA does not in itself prevent an accountant from continuing to provide services to the client who is the subject of the report.

**Ask yourself – suspicion**

1. One of your clients, a builder, always requires payment in cash. You have no evidence that he is evading income tax, although he may be. Should this be reported as a suspicion?

2. You have completed and submitted an income tax return for a sole trader. When you complete the return for his wife, you discover that they have joint rental income which has been omitted from the husband’s return. You are satisfied that it was an oversight on the husband’s part not to have told you about this, and you inform HM Revenue and Customs of the error. Do you also have to report this to SOCA?

3. A client tells you over a business lunch that he is having a swimming pool installed at his home. The contractors have asked for payment in cash, which he suspects is because they will not be declaring it to HM Revenue and Customs. Do you have a duty to disclose this to SOCA? Would your answer be different if the swimming pool owner was a friend rather than a client?

4. You are carrying out a due diligence investigation. The owners of the target company have been regularly putting personal expenditure through the business and claiming it as tax-allowable. Do you need to report this to SOCA now, or only if the company were to become your client?
The money laundering offences referred to in chapter 6 above can be committed by any person. They are clearly intended to apply, primarily, to those who are consciously involved in criminal activities and dealing with the material proceeds of crime. The responsibilities assigned to accountants and others under POCA are essentially designed to ensure that they deter, detect and report such activity.

But given the way that the money laundering offences are framed, it is possible that accountants (and other professional advisors) may fall foul of them at one time or another by dealing with clients who try to involve them in their criminal activities. While the potential for most practising accountants to commit these offences may not be great, accountants might, conceivably, become involved with ‘transferring’ criminal property on behalf of a client (an offence under section 327 POCA); they might become ‘concerned in an arrangement’ that they know or suspect facilitates the processing of criminal property (an offence under section 328 POCA); or they might at some point ‘possess’ criminal property (an offence under section 329 POCA).

Examples of situations which might cause you to fall foul of these provisions are cases where clients ask you to place funds in client accounts, where clients ask you to design and implement trust and company structures for them, and where criminal funds are used to fund corporate acquisitions.

**Authorised disclosures**

Where an accountant considers that he has already committed a breach of any of the money laundering offences, or may get into a situation where a breach could occur, he must make an ‘authorised disclosure’ of the relevant circumstances under section 338 POCA. Where the disclosure is made as required, the reporting accountant will not commit any of the offences covered by the disclosure.

That is so whether or not the breach has already occurred. Where the breach has already taken place, the reporter must have a good reason for failing to make the disclosure beforehand – it is conceivable, for example, that an accountant may not realise, when he starts to conduct a transaction, that criminal property is involved - and the disclosure must be made...
on his own initiative and as soon as it is practicable for him to make it. If these conditions are not met, the disclosure will not be treated as an authorised disclosure and the accountant may be held to have committed the offence that he sought to avoid.

Thus, the onus is on the accountant, wherever possible, to make an authorised disclosure before the act which would give rise to the offence actually occurs. POCA says that you can proceed to involve yourself in what you suspect may be a breach of the law as long as you make the required disclosure and receive official ‘consent’ to continue acting. On the other hand, if consent is applied for in respect of a particular matter, but the accountant goes ahead and becomes involved in the activity concerned before consent is forthcoming, or in spite of a refusal, he risks committing the offence.

Procedure
The request for consent is made by means of selecting the ‘consent required’ option which is a standard element of the pro-forma suspicious activity report (see chapter 6). The request should be clear about the intended activity and the nature of the consent being requested. It should be framed carefully so that it makes clear to SOCA exactly what is being requested. Too narrow a request may mean repeated requests will be required, causing issues of cost and efficiency to your firm and possibly unnecessary complications for your relationship with the client. Too broad or ill-defined a request could, in the worst-case scenario, result in SOCA having to refuse consent or conclude that it is outside its authority to deal with.

The required procedure for making the authorised disclosure depends on whether or not you are the firm’s MLRO (see chapter 5). If you are not the firm’s MLRO, then the request you make for consent should be directed to your firm’s MLRO, and you are entitled to rely on that person to tell you whether your request is or is not granted. If you are the MLRO, then you will make any request for consent you consider necessary, on behalf of your firm, to SOCA, and you must only pass on ‘consent’ to continue acting to other members of your firm if you yourself receive that consent in accordance with the rules set out in POCA.

Pre-emptive disclosures
In respect of pre-emptive disclosures, the accountant can continue to an act in relation to the matter which is the subject of the authorised disclosure provided he receives consent to do so. The most satisfactory way of acquiring consent is for it to be given to you expressly - note that where internal requests to the firm’s MLRO are concerned, the consent must always be given expressly. But in respect of requests from the MLRO to SOCA, the consent to the MLRO, assuming it is forthcoming, can be given expressly or implicitly. Where consent is given expressly, it can be done over the telephone, in which case it is advisable for the MLRO who receives the call to make a note of the name and contact number of the case officer and the consent reference.

There are two bases on which a firm can rely on the implied consent of SOCA for it to continue acting in respect of a matter covered by an authorised disclosure. First, if you apply for consent, and no notice of refusal is received within seven working days starting from the first working day after the disclosure, then you are treated as having received the appropriate consent...
Second, even if you receive a formal notice of refusal during the seven day period, you are deemed to have the ‘appropriate consent’ if the ‘moratorium period’ has expired. The moratorium period is the period of 31 days starting with the day on which you receive notice from SOCA that the request for consent is refused. Accordingly, SOCA is given a fixed period of time to act upon the intelligence that is provided to it via authorised disclosures; beyond that period, reporters are allowed to continue acting.

It is the MLRO’s responsibility not to give the appropriate consent to any member of his firm unless express or implied consent is forthcoming from SOCA. Accordingly, the employee or partner is required to put on hold any client work which is covered by the request for consent until such time as the MLRO says it can continue. Where express or implied consent is given, the MLRO should inform relevant partners and staff as soon as is practicable so that they can continue with their work.

**Reasonable excuse**

Even if the accountant does not make the required authorised disclosure at all, he or she will not be regarded as committing an offence if he intended to make the disclosure but has a ‘reasonable excuse’ for not doing so. There is as yet no case law with respect to what circumstances might give rise to a reasonable excuse, so this should be regarded as being a defence of last resort.

**Acting for clients while waiting for consent**

In practice, the requirement not to continue involvement in a particular matter until consent for that involvement is forthcoming can present a significant challenge to the accountant. This will be especially so when the 31-day ‘moratorium period’ is in progress. In some cases, the client may ask directly why the delay is occurring. In response to such requests, members are advised to decline to enter into discussions on the matter but to explain that, regrettfully, they cannot at this point discuss the matter further. The danger is that, if the client discovers or suspects that the reason for the hold-up in attending to his affairs is that you are waiting for consent following the making of an authorised disclosure under POCA, this could cause the client to take steps to cover up the criminal activity concerned or to remove the criminal property itself. You as the accountant should be careful not to contribute to any such deduction on the part of the client. This is because you are subject to separate obligations not to ‘tip off’ the client about any disclosure that you or you or your firm might have made or to prejudice any investigation that might be undertaken into his affairs (see chapter 9). If you feel that the circumstances are exceptional, and that the delay is likely to cause harm to members of your firm or to alert the client in a way that could materially undermine a criminal investigation, your MLRO is advised to contact SOCA and ask to be put in touch with the law enforcement body that is dealing with the matter concerned.

**Limits of authority of SOCA regarding consent**

When considering whether you need to make authorised disclosures and to apply for consent, it should be remembered that SOCA’s authority is restricted to giving consent in respect of matters which would constitute an offence under sections 327-329 POCA. It cannot give any wider authority and, specifically, it cannot override any of the other offences that accountants might commit under POCA, including the tipping-off offence.
AT A GLANCE

- Accountants in practice are at risk of offending under sections 327-329 POCA through being involved, perhaps inadvertently, with clients’ property
- They will not commit an offence if their involvement is disclosed to SOCA
- In ongoing cases, the accountant should ask for consent, following the required procedure, from SOCA before proceeding further with a transaction which has raised suspicions - this should be done by the firm’s MLRO.
- Consent from SOCA may be given expressly or implicitly
- Accountants should not enter into discussions with clients pending consent being received from SOCA

Ask yourself – direct involvement

You have been asked by a client to transfer cash from the client to a third party. You are suspicious of the origin of these funds and seek consent from SOCA. SOCA invokes its moratorium period and the client’s managing director asks you why there is a delay in transferring the funds. What would you say in reply?
In the same way as accountants (and others in the regulated sector) are obliged to report knowledge and suspicions of money laundering, they are also required to report information about offences committed under the Terrorism Act 2000 (TA 2000). The circumstances in which this requirement applies, via section 21A of TA 2000, are as follows:

- when they know or suspect, or have reasonable grounds for knowing or suspecting, that one of a number of specified offences have been committed (or have been attempted to be committed) by another person

and

- the information on which the knowledge or suspicion is based comes to him or her in the course of ‘a business in the regulated sector’

(Incidently, a similar responsibility is imposed, by section 19 TA 2000) on any person who acquires information on one of the specified offences via his trade, profession, business or employment).

As is the case with disclosures under POCA, reports are made, within a firm, to the firm’s MLRO. It is then the responsibility of the MLRO to pass the information on to SOCA. As from 26 December 2007, the privileged circumstances exemption from the obligation to report is extended to cover ‘relevant professional advisors’ as well – the definition of this term is the same as the one used in POCA, and explained in chapter 6 above.

The ‘specified offences’ for reporting purposes are:

- inviting another person to provide money or other property with the intention that it should be used for the purposes of terrorism (or with reasonable cause to suspect that it would be so used) (section 15 TA 2000)

- using money or other property for the purposes of terrorism, or possessing money or other property with the intention that it should be used for the purposes of terrorism (or with reasonable cause to suspect
that it would be so used) (section 16 TA 2000)

- entering into or becoming concerned in an arrangement where one knows or has reasonable cause to suspect that money or other property will or may be used for the purposes of terrorism (section 17 TA 2000)

- entering into or becoming concerned in an arrangement which facilitates the retention or control by (or on behalf of) another person of ‘terrorist property’ by concealment, removal or transfer (section 18 TA 2000)

For the purposes of these provisions, ‘property’ is defined on the same wide basis as it is in POCA. ‘Terrorist property’ comprises money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation), the proceeds of the commission of acts of terrorism and proceeds of acts carried out for the purposes of terrorism.
Both POCA and the TA 2000 contain strict rules regarding the disclosure of information by those who come across money laundering and terrorist financing activity respectively. The purpose of these rules is, essentially, to ensure that those who are suspected of involvement in such activity are not given the opportunity to escape, or to remove evidence, before the authorities are able to catch up with them.

The AML offence
The basic tipping-off offence is contained in section 333A of POCA (which took effect on 26 December 2007 and replaces the previous section 333). This says that an accountant in a practising firm (or any other person in the regulated sector) must not

- disclose that a disclosure has been made of information obtained in the course of the practice either to an MLRO or to SOCA (or to the police or Her Majesty’s Revenue and Customs (HMRC)) where the disclosure is likely to prejudice any investigation that might be conducted following the disclosure referred to, or
- disclose that an investigation into allegations that a money laundering offence (which came to light in the course of the accountancy practice) has been committed, is being contemplated or is being carried out and the disclosure is likely to prejudice that investigation.

The offence will not be committed if the person making the disclosure does not know or suspect that it is likely to prejudice any resulting investigation.

Exceptions
There are a number of exceptions to the offence in section 333A, as follows:

i) a person does not commit the offence if he makes the disclosure to a member of the same firm (section 333B)

ii) a ‘relevant professional advisor’ (see definition in chapter 6 above) does not commit the offence if the disclosure is made to another relevant professional advisor or to an ‘independent legal professional’ where both are based in the UK (or another EAA state or a state imposing equivalent AML requirements)
and they operate within different undertakings which share common ownership, management or control (section 333B)

iii) a relevant professional advisor does not commit the offence if

- he makes a disclosure to another relevant professional advisor from a different undertaking where the disclosure relates to the same client or a former client of both advisors and involves a transaction or services provided by them both

and

- the disclosure is made only for the purpose of preventing a money laundering offence

and

- the disclosure is made to a person in an EU member state or a state imposing equivalent AML requirements (section 333C

iv) a person does not commit the offence if the disclosure is made to a ‘money laundering supervisory authority’ under the Money Laundering Regulations 2007 or for the purpose of detecting, investigating or prosecuting a criminal offence in the UK or elsewhere, an investigation under POCA or the enforcement of any court order under POCA (section 333D POCA)

v) a relevant professional advisor does not commit the offence if he makes the disclosure to his client for the purpose of dissuading the client from engaging in conduct amounting to an offence.

The CTF offence
Under section 21D of the TA 2000 – in force from 26 December 2007 - a person in the regulated sector commits an offence if he discloses the fact that he has made a disclosure relating to a TF offence and that disclosure is likely to prejudice any investigation that might be conducted into the matter.

It is also an offence, under the same section, for a person in the regulated sector to disclose that an investigation into allegations into possible TF offences is being contemplated or is being carried out (and disclosure is likely to prejudice that investigation).

Exceptions
But, as with the AML offence, there are exemptions on the same lines as those listed above. A person in the regulated sector will not commit the offence under section 21D if

- the disclosure is made to another professional legal adviser or ‘relevant professional advisor’ where both parties carry on business in an EEA state which imposes equivalent AML requirements and both operate in different undertakings that share common ownership, management or control

- the disclosure is made by one relevant professional advisor to another of the same kind, i.e. from one accountant to another, where the all the following conditions apply:

- the disclosure relates to a client of them both, or a transaction
involving them both, or the provision of a service involving them both

- the disclosure is made only for the purpose of preventing an offence under Part III of the TA 2000

- the other advisor is also based in an EEA state or some other state where equivalent AML requirements are imposed

- both advisors are subject to equivalent duties of professional confidentiality and the protection of personal data.

- the disclosure is made to his ‘supervisory authority’ under the Money Laundering Regulations 2007 or for the purpose of detecting, investigating or prosecuting a criminal offence (whether in the UK or elsewhere), an investigation under POCA or the enforcement of any court order under POCA

- the disclosure is made, by a relevant professional advisor, to his client for the purpose of dissuading the client from engaging in conduct amounting to an offence

- The person making the disclosure does not know or suspect that the disclosure is likely to prejudice any resulting investigation.

**Ask yourself – tipping off**

Is an offence under s 333 POCA committed in the following circumstances?

1. A zealous trainee, believing that he has spotted money laundering, rings up his manager from the client’s accounts department in the full hearing of some of the clerks, who inform the chief accountant.

2. An auditor enquires of a client’s accountant about a suspiciously excessive number of credit balances on the sales ledger.

3. An ACCA member enquires of the ACCA’s technical advisory staff whether a specific situation at a client constitutes money laundering, and gives details.

**AT A GLANCE**

- No disclosure to a client should be made which might prejudice any subsequent investigation
- There is no offence if the discloser does not know or suspect prejudice to the investigation
- There are a number of detailed exceptions to the basic offence
- There is a similar offence in section 21D of the Terrorism Act, with similar exceptions
The provisions in POCA and the TA 2000 regarding the reporting of suspicions involving the affairs of clients override the fundamental professional principle contained in statement 3.2 of the ACCA Code of Ethics to the effect that members should not disclose to third parties information acquired as a result of a professional or business relationship without the client’s consent.

Members may still be concerned that disclosure of client information will leave them open to action for breach of trust or breach of confidentiality. To address this issue, section 337 of POCA makes it clear that any disclosure which satisfies the three reporting conditions discussed in chapter 6 will not breach any restriction on the disclosure of information – a report made in these circumstances will be a ‘protected disclosure’. Where a member makes a report in circumstances where any one of the conditions are not met, for example where a member makes a report on the basis of information which has not come his way during the course of his business, the member may leave himself open to action by the client. Much the same applies to reports filed under section 21A of the TA 2000 – provided the information on which the reporter’s knowledge or suspicion was based came his way in the course of a business in the regulated sector, the report will count as a ‘protected disclosure’.
annexe 1 – the offences and penalties

1. **PROCEEDS OF CRIME ACT**

- To conceal, disguise, convert or transfer criminal property or to remove criminal property from England, Scotland, Wales or Northern Ireland (section 327 POCA)

- To enter into, or become involved in, any arrangement which one knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person (section 328 POCA)

- To acquire, use or possess criminal property (other than for ‘adequate consideration’) (section 329 POCA)

The penalty for breach of any of the above three offences is, on summary conviction, imprisonment for up to six months and/or a fine and, on indictment, imprisonment for up to 14 years and/or a fine.

- To fail to make a suspicious activity report (section 330 POCA)

Penalty – on summary conviction, imprisonment of up to six months and/or a fine and, on indictment, imprisonment for up to five years and/or a fine.

- To fail, as an MLRO, to make a suspicious activity report (section 331 POCA)

Penalty – on summary conviction, imprisonment of up to six months and/or a fine and, on indictment, imprisonment for up to five years and/or a fine.

- To breach the rules on tipping off (section 333A POCA)

Penalty – on summary conviction, imprisonment of up to three months and/or a fine and, on indictment, imprisonment for up to two years and/or a fine.

- To give, as an MLRO, consent for the undertaking of prohibited acts when consent has not been forthcoming (section 336 POCA)

Penalty – on summary conviction, imprisonment of up to six months and/or a fine and, on indictment, imprisonment for up to five years and/or a fine.
2. **THE TERRORISM ACT 2000**

- Failing to report knowledge or suspicion of a terrorist offence under sections 15-18 of the TA 2000

*Penalty – on summary conviction, imprisonment of up to six months and/or a fine and, on indictment, imprisonment for up to five years and/or a fine.*

3. **THE MONEY LAUNDERING REGULATIONS 2007**

- Failing to apply CDD procedures when required by regulation 7 of the Regulations

- Failing to carry out ongoing monitoring as required by regulation 8 of the Regulations

- Failing to verify the identity of clients and beneficial owners before the establishment of a new business relationship as required by regulation 9 of the Regulations

- Entering into a business relationship, or carrying out transactions circumstances where CDD procedures have not been carried out, and failing to terminate any existing business relationship where required CDD procedures have not been carried out, as required by regulation 11 of the Regulations

- Failing to carry out enhanced due diligence and enhanced ongoing monitoring as required by regulation 14 of the Regulations

- Failing to keep the required CDD records for at least five years as required by regulation 19 of the Regulations

- As a person who has agreed to allow another regulated person to rely on his CDD data, failing to keep those CDD records for five years from the date on which that data is relied on by the other person, failing to pass on the relevant information to the person who intends to rely on it, as required by regulation 19 of the Regulations

- Failing to establish and maintain appropriate and risk-sensitive policies and procedures on specified matters as required by regulation 20 of the Regulations

- Failing to take appropriate measures to provide training to relevant employees as required by regulation 21 of the Regulations

*The penalty for all the above offences under the Regulations is, on summary conviction, a fine and, on indictment, imprisonment of up to two years and/or a fine. Where an offence is committed by a firm which is a body corporate, i.e. a company or an LLP, or a partnership, and the offence is held to have been committed with the consent or connivance of a company director, LLP member or partner of the firm, or can be attributed to the neglect of any such person, then that person will also commit the offence on a personal basis. A defence against any of these charges is that the person charged took all reasonable steps and exercised all due diligence to avoid committing the offence.*
Under reg 17 of the Money Laundering Regulations, ACCA members may rely on CDD data obtained by the following persons:

- A credit or financial institution which is an ‘authorised person’ under the Financial Services and Markets Act 2000 or

- an auditor, insolvency practitioner, external accountant or tax adviser or independent legal professional who is supervised for AML purposes by any of the following bodies:
  - ACCA
  - Council for Licensed Conveyancers
  - Faculty of Advocates
  - General Council of the Bar
  - General Council of the Bar of Northern Ireland
  - Institute of Chartered Accountants in England and Wales (ICAEW)
  - Institute of Chartered Accountants in Ireland (ICAI)
  - Institute of Chartered Accountants of Scotland (ICAS)
  - Law Society

NB the consent of the party providing the CDD data must be obtained, and in the event of any failure to comply with the CDD rules, the person placing reliance will be liable in default.
39

ACCOUNTANTS AND MONEY LAUNDERING

CLIENT DUE DILIGENCE (CDD)

The standard CDD procedures require that, before entering into a business relationship, accountants take the necessary steps to understand the ownership and control structure of a business, and subsequently they must monitor the activities of their clients on an ongoing basis to ensure that their information on the client is kept up-to-date and their documentation regarding the client, the relationship is up-to-date. In the light of this, the CCAB guidance (paragraph 5.19) says that changes in the appointment of new senior managers or shareholders should prompt businesses to re-apply CDD procedures.

The Finance Director of a company will play a key role in the direction and management of the affairs of a company, so it makes sense to identify such individuals and keep their details on file.

As a UK public authority, the prospective client comes within the range of entities for which 'simplified due diligence' is appropriate, in which case the standard procedures on CDD need not apply (see paragraph 5.23 of the CCAB Guidance). However, the standard procedures should still be followed where any suspicion of money laundering or terrorist financing arises.

COMPLIANCE RESPONSIBILITIES: IN-HOUSE PROCEDURES

The Regulations say that firms must ensure that all 'relevant' staff must be made aware of the law on money laundering and terrorist financing and given regular training on how to recognise and deal with transactions which may be related to money laundering or terrorist financing. Firms choose to provide this training to all members of their staff. The CCAB guidance suggests that firms should consider not only those employees who are involved in client work but also those who deal with the firm's finances and those who deal with procuring services for the firm. In practice, many firms choose to provide this training to all members of their staff.
In the light of the above, new staff should receive AML/CTF training, and as part of this training they should be advised:

- to read the firm’s AML manual and in particular to understand the firm’s internal procedures regarding the discussion of queries and the reporting of suspicions
- not to be afraid to report suspicions to the MLRO (or deputy)
- to be vigilant at all times
- not on any account to tell the client – even inadvertently – that they are informing the MLRO of their suspicions.

The firm should also be satisfied that the staff actually understand the information they are given and can be relied upon to apply it in practice.

Paragraphs 3.16 and 3.17 of the CCAB Guidance provide additional advice on the education and training of staff.

2. It is not possible to prove the quality of any previous training that a new member of staff may have undergone, even at manager level; so the new manager should attend an induction course which includes an AML training session, and be given a copy of the firm’s AML manual to read. See also the response to question 5.1 as regards the required scope of training.

6 REPORTING OF SUSPICIONS

1. Most professionals would take the view that on its own this need not be regarded as suspicious. The builder may need to pay his workers in cash each week or find it convenient to buy supplies for cash. However, if there is any additional reason to suppose (even without ‘hard’ evidence) that he is evading tax, this should be reported.

2. For proceeds of crime to exist, and hence for a money laundering offence to be committed, there must be knowledge or suspicion on the part of a person that those proceeds derive from criminal activity: in this case, the omission appears to be an innocent oversight, with no criminal intent, so there are no proceeds of crime. If the return has been submitted before the deadline and that has not yet expired, no tax is any case payable.

3. If the information comes to the accountant during the course of his business, this must be reported. The intention to commit a crime (in this case tax evasion) can itself be a crime, and although you do not know for a fact that the contractor intends to evade tax it should probably provide reasonable grounds for you to form that suspicion. You should not inform the client of your action, as this could constitute ‘tipping off’ as per s333 POCA 2002. Your report to SOCA can name only your client: if SOCA decides to investigate, they can ask for the information from your client. If the information concerned came to you through a friend, with whom you do not have any business relationship, you would not need to make a report, although your friend might be advised either to refuse to deal with the contractor or at least not to talk about it to anyone.
4. Report it now. This is unlikely to be an innocent error, and you have come across it in the course of your professional work. It does not have to be a client who is committing the crime.

7 DIRECT INVOLVEMENT BY ACCOUNTANTS IN THE MONEY LAUNDERING OFFENCES

Until consent has been granted, either expressly or implicitly, the transaction cannot continue – hence the client's anxiety. Accountants should not enter into any discussions on the matter, in case the client suspects that disclosure has been made to SOCA and then attempts to destroy evidence and/or cover their traces. It cannot be helped if the lack of comment in itself makes the client suspicious; SOCA may be prepared to help if the circumstances are exceptional and if the delay may cause harm to the firm or undermine a criminal investigation.

8 TIPPING OFF

1. The amendments to the original section 333 of POCA now probably exempt a trainee in this situation from committing an offence – both on the grounds of not knowing that the conversation might prejudice an investigation and because the disclosure is made to a member of the same firm. However, trainees should be warned against carelessness of this nature, since the client's chief accountant in this case could well take steps to destroy evidence or in other ways prejudice an investigation. Firms should also be aware that the communication of information in such a careless way might suggest that the trainee has not been trained properly by the firm so as to understand the importance of discretion. Remember that reg 21 of the Money Laundering Regulations requires firms to ensure that all their relevant staff are ‘made aware’ of the law; breach of this requirement can lead to criminal penalties.

2. The CCAB guidance says that normal audit enquiries will not be classed as tipping off. This guidance is now approved by HM Treasury and will therefore be followed by a court – a prosecution would be most unlikely.

3. Disclosure to a supervisory authority such as ACCA is also an exception under section 333D POCA, and hence no offence is committed.