

Money Laundering – A Review of the JMLSG Guidance Notes 2007

Overview

The guidance provided by the Joint Money Laundering Steering Group (JMLSG) in January 2006 was revised in December 2007 following the implementation of the 3rd EU Money Laundering Directive. While the majority of the guidance notes remained the same, this document outlines the latest state of play as a result of the implementation of this directive. This document contains the summary of the guidance that was released in January 2006, and the changes that were introduced in December 2007.

The JMLSG guidance emphasises the responsibility of senior management to manage the firm's money laundering and terrorist financing risks, and how this should be carried out on a risk-based approach. It introduces a standard approach to the identification and verification of customers, separating out basic identity from other aspects of knowing the customer, as well as giving guidance on the need to monitor customer activity.

Part One

Introduction

Money laundering takes many forms, including:

- trying to turn money raised through criminal activity into 'clean' money (that is, classic money laundering);
- handling the benefit of acquisitive crimes such as theft, fraud and tax evasion;
- handling stolen goods;
- being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property;
- criminals investing the proceeds of their crimes in the whole range of financial products.

The UK approach to fighting money laundering and terrorist financing is based on a partnership between the public and private sectors. Objectives are specified in legislation and in the FSA Rules, but there is usually no prescription about how these objectives must be met. Key elements of the UK Anti Money Laundering / Combating Terrorist Financing (AML/CTF) framework are:

- Proceeds of Crime Act 2002 (as amended);
- Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001);
- Money Laundering Regulations 2003;
- Bank of England Sanctions Notices and News Releases;
- FSA Handbook.

- Compliance
- Internal Audit
- Risk Management
- Corporate Governance

Visit our online bookshop or access our revolutionary on-line Money Laundering training system at www.cpaaudit.co.uk

CPA Audit is a trading name of CPA Audit LLP, a Limited Liability Partnership registered in England and Wales.
Partnership number: OC314819. Registered office: Peek House, 20 Eastcheap, London, EC3M 1AL.

Offences

There are three broad groups of offences related to money laundering that firms need to avoid committing. These are:

- knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of, criminal property;
- failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering;
- tipping off, or prejudicing an investigation.

It is also a separate offence under the AML Regulations not to have systems and procedures in place to combat money laundering, regardless of whether or not money laundering actually takes place.

Status of the Guidance

The Proceeds of Crime Act (POCA) requires a court to take account of industry guidance that has been approved by a Treasury minister when considering whether a person within the regulated sector has committed the offence of ‘failing to report, where that person knows, suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering.’ Similarly, the Terrorism Act requires a court to take account of such approved industry guidance when considering whether ‘a person within the financial sector has failed to report’ under that Act. The ML Regulations also provide that a court must take account of similar industry guidance in determining whether a person or institution within the regulated sector has complied with any of the requirements of the ML Regulations.

When considering whether to take disciplinary action against an FSA-regulated firm in respect of a breach of the relevant provisions of the Senior Management, Systems and Controls Sourcebook (SYSC), FSA will have regard to whether a firm has followed relevant provisions in this guidance. When considering whether to bring a criminal prosecution in relation to a breach of the ML Regulations, FSA may also have regard to whether the person concerned has followed this guidance.

Senior Management Responsibility

Senior management has a responsibility to ensure that the firm’s control processes and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of the firm being used in connection with money laundering or terrorist financing.

Under a risk-based approach, firms start from the premise that most customers are not money launderers or terrorist financiers. However, firms should have systems in place to highlight those customers who, on criteria established by the firm, may indicate that they present a higher risk of this.

Senior management must be fully engaged in the decision making processes, and must take ownership of the risk-based approach, since they will be held accountable if the approach is inadequate.

Obligations on All Firms

The ML Regulations place a general obligation on firms within its scope to have appropriate systems and controls to forestall and prevent money laundering. Failure to comply with this obligation risks a prison term of up to two years and/or a fine.

The offences of money laundering under POCA and the Terrorism Act, and the obligation to report knowledge or suspicion of possible money laundering, affect members of staff of regulated firms. Firms, however, have an obligation under the ML Regulations to take appropriate measures so that employees are made aware of the relevant provisions of the ML Regulations, POCA and the Terrorism Act, and are given training in how to recognise and deal with transactions which may be related to money laundering or terrorist financing.

FSA-Regulated Firms

In FSA-regulated firms a director or senior manager must be allocated overall responsibility for the establishment and maintenance of the firm's anti-money laundering systems and controls. Also, an individual must be allocated responsibility for oversight of a firm's compliance with FSA's Rules on systems and controls against money laundering: this is the firm's Money Laundering Reporting Officer (MLRO).

MLRO's Report

At least once in each calendar year, an FSA-regulated firm must commission a report from its MLRO on the operation and effectiveness of the firm's systems and controls to combat money laundering. When senior management receives reports from the firm's MLRO, it should consider them and take any necessary action to remedy any deficiencies identified in a timely manner.

Exemptions from Legal and Regulatory Obligations

General insurance firms and mortgage intermediaries are regulated by FSA, but are not covered by the ML Regulations, or the provisions of SYSC specifically relating to money laundering. They are, therefore, under no obligation to appoint an MLRO.

They are, however, subject to the general requirements of SYSC, and so have an obligation to have appropriate risk management systems and controls in place, including controls to counter the risk that the firm may be used to further financial crime.

AML/CTF policy

A statement of the firm's AML/CTF policy, and the procedures to implement it will clarify how the firm's senior management intends to discharge its responsibility for the prevention of money laundering and terrorist financing. The policy statement might include, but not be limited to, such matters as:

- Guiding principles:
 - an unequivocal statement of the culture and values to be adopted and promulgated throughout the firm towards the prevention of financial crime;
 - a commitment to ensuring that customers' identities will be satisfactorily verified before the firm accepts them;
 - a commitment to the firm 'knowing its customers' appropriately - both at acceptance and throughout the business relationship - by taking appropriate steps to verify the customer's identity and business, and his reasons for seeking the particular business relationship with the firm;
 - a commitment to ensuring that staff are trained and made aware of the law and their obligations under it, and to establishing procedures to implement these requirements;
 - recognition of the importance of staff promptly reporting their suspicions internally.

- Risk mitigation approach:
 - a summary of the firm's approach to assessing and managing its money laundering and terrorist financing risk;
 - allocation of responsibilities to specific persons and functions;
 - a summary of the firm's procedures for carrying out appropriate identification and monitoring checks on the basis of their risk-based approach;
 - a summary of the appropriate monitoring arrangements in place to ensure that the firm's policies and procedures are being carried out.

Group Policies

A group may have a policy that all overseas branches and subsidiaries undertake identification and record-keeping procedures at least to the standards required under UK law or, if the standards in the host country are more rigorous, to those higher standards.

The ML Regulations require firms to appoint a nominated officer to receive internal reports relating to knowledge or suspicion of money laundering.

Financial Sanctions

The Bank of England maintains a Consolidated List of targets listed by the United Nations, European Union and United Kingdom under legislation relating to current financial sanctions regimes. It is a criminal offence to make payments, or to allow payments to be made, to targets on the list maintained by the Bank of England. This would include dealing direct with targets, or dealing with targets through intermediaries (such as lawyers or accountants). Firms therefore need to have an appropriate means of monitoring payment instructions to ensure that no payments are made to targets or their agents.

The FSA Handbook

SYSC requires FSA-regulated firms to have effective systems and controls for countering the risk that a firm might be used to further financial crime, and specific provisions regarding money laundering risks. A regulated firm's systems and controls are required to cover (as appropriate to their business):

- senior management accountability, including allocation to a director or senior manager overall responsibility for the establishment and maintenance of effective AML systems and controls and the appointment of a person with adequate seniority and experience as MLRO;
- appropriate training on money laundering to ensure that employees are aware of, and understand, their legal and regulatory responsibilities and their role in handling criminal property and money laundering/terrorist financing risk management;
- appropriate provision of regular and timely information to senior management relevant to the management of the firm's criminal property/money laundering/terrorist financing risks;
- appropriate documentation of the firm's risk management policies and risk profile in relation to money laundering, including documentation of the firm's application of those policies;
- appropriate measures to ensure that money laundering risk is taken into account in the day-to-day operation of the firm, including in relation to:
 - the development of new products;
 - the taking-on of new customers;
 - changes in the firm's business profile.

Outsourcing

Where UK operational activities are undertaken by staff in other jurisdictions, they should be subject to the AML/CTF policies and procedures that are applicable to UK staff, and internal reporting procedures implemented to ensure that all suspicions relating to UK-related accounts, transactions or activities are reported to the nominated officer in the UK. Service level agreements will need to cover the reporting of management information on money laundering prevention, and information on training, to the MLRO in the UK. Procedures should also be in place to meet local AML/CTF regulations and reporting requirements.

The Role of MLRO

The MLRO is responsible for oversight of the firm's compliance with the FSA's Rules on Systems and Controls in relation to money laundering. An MLRO should be able to monitor the day-to-day operation of the firm's AML/CTF policies, and respond promptly to any reasonable request for information made by FSA or other law enforcement agencies. The individual appointed as MLRO therefore, must have a sufficient level of seniority within the firm.

Obtaining and Using National and International Findings

An MLRO should ensure that the firm obtains, and makes appropriate use of, any government or FATF findings concerning the approach to money laundering prevention in particular countries or jurisdictions.

Awareness and Training

The MLRO is responsible for oversight of the firm's compliance with its requirements in respect of staff training, including ensuring that adequate arrangements for awareness and training of employees are in place. The MLRO is responsible for ensuring that the training is offered, that the standards and scope of the training are appropriate, and that appropriate records are kept.

Monitoring Effectiveness of Money Laundering Controls

A firm is required to carry out regular assessments of the adequacy of its systems and controls to ensure that they manage the money laundering risk effectively.

Reporting to Senior Management

At least annually the senior management of an FSA-regulated firm must commission a report from its MLRO which assesses the operation and effectiveness of the firm's systems and controls in relation to managing money laundering risk. The firm's senior management should consider the report, and take any necessary action to remedy deficiencies identified in it, in a timely manner.

Risk-based approach

A risk-based approach takes a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the firm. These steps are to:

- identify the money laundering and terrorist financing risks that are relevant to the firm;
- assess the risks presented by the firm's particular
 - customers;
 - products;
 - delivery channels;
 - geographical areas of operation;
- design and implement controls to manage and mitigate these assessed risks;
- monitor and improve the effective operation of these controls;
- record appropriately what has been done, and why.

Identifying and Assessing the Risks Faced by the Firm

The firm should assess its risks in the context of how it might most likely be involved in money laundering or terrorist financing. In this respect, senior management should ask themselves a number of questions; for example:

- What risk is posed by the firm's customers?
- What risk is posed by a customer's behaviour?
- How does the way the customer comes to the firm affect the risk?
- What risk is posed by the products/services the customer is using?

Customer Risk

Many customers, by their nature or through what is already known about them by the firm, carry a lower money laundering or terrorist financing risk. These might include:

- Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken; (this applies equally to pensioners or benefit recipients, or to those whose income originates from their partners' employment);
- Customers with a long-term and active business relationship with the firm; and
- Customers represented by those whose appointment is subject to court approval or ratification (such as executors).

Design and Implement Controls to Manage and Mitigate the Risks

As regards money laundering and terrorist financing, managing and mitigating the risks will involve measures to verify the customer's identity; collecting additional KYC information about the customer; and monitoring his transactions and activity, to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing may be taking place.

A customer identification programme that is graduated to reflect risk could involve:

- a standard information dataset to be held in respect of all customers;
- a standard verification requirement for all customers;
- more extensive due diligence for higher risk customers;
- more limited identity verification measures for specific lower risk customer/product combinations; and an approach to monitoring customer activities and transactions that reflects the risk assessed to be presented by the customer, which will identify those transactions or activities that may be unusual or suspicious.

Where a customer is assessed as carrying a higher risk, then depending on the product sought, it may be appropriate to seek additional information in respect of the customer, to be better able to judge whether or not the higher risk that the customer is perceived to present is likely to materialise.

Customer Due Diligence(CDD)

The due diligence carried out on new customers is in two distinct parts. As well as verifying identity, the risk-based approach will lead to a need, in appropriate cases, to obtain additional information in respect of some customers; this is referred to as Know your Customer(KYC) information.

Firms should take a combination of appropriate steps, on the basis of their assessment of the money laundering/terrorist financing risk that each customer, or class/category of customer, presents, addressing:

- ID - verifying the customer's identity;
- KYC - obtaining appropriate additional information.

A firm must apply CDD measures when it either establishes a business relationship; carries out an occasional transaction; suspects money laundering or terrorist financing; or doubts the veracity of documents, data or information previously obtained for the purpose of identification or verification.

When a firm is unable to apply the CDD measures in relation to a customer, the firm must not carry out a transaction with or for the customer through a bank account or establish a business relationship or carry out an occasional transaction with the customer. The firm must also terminate any existing business relationship with the customer, and consider whether it ought to be making a report to SOCA, in accordance with its obligations under POCA and the Terrorism Act.

The firm identifies customers by obtaining a range of information, and comparing this to documents, data or information obtained from a reliable and independent source. In general, the customer will be the party, or parties, with whom the business relationship is established, or for whom the transaction is carried out.

An "occasional transaction" is a transaction carried out other than in the course of a business relationship that amounts to €15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked. A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. The Firm has an obligation to verify the identity of a beneficial owner using risk-based and adequate measures until it is satisfied that it knows who the beneficial owner is. Any beneficial owners owning or controlling more than 25% of body corporates, partnerships or trusts must be identified, and risk-based and adequate measures must be taken to verify their identities.

Customers With Whom Firms Have a Business Relationship on 15 December 2007

Firms must apply CDD measures at appropriate times to its existing customers on a risk-sensitive basis. Firms must also apply CDD measures to any anonymous accounts or passbooks as soon as possible after 15 December 2007, and in any event before they are used. Firms must take steps to ensure that they hold appropriate information to demonstrate that they are satisfied that they know all their customers.

If a firm acquires the business and customers of another firm it is not necessary for the identity of all existing customers to be re-verified, as long as all underlying customer records are acquired with the business; or a warranty is given by the acquired firm. It is recommended that some sample testing is completed on a risk sensitive basis.

Nature and Purpose of Proposed Business Relationship

A firm must ensure it is clear about the purpose and intended nature of the business relationship or transaction with all clients. In some instances this will be self-evident, but in many cases the firm may have to obtain information until it is satisfied. This information might include the nature and details of the business; a record of changes of address and the expected source and origin of the funds to be used in the relationship; the initial and ongoing source(s) of wealth or income; copies of recent and current financial statements; the various relationships between signatories and with underlying beneficial owners or the anticipated level and nature of the activity that is to be undertaken through the relationship. This information must be kept up to date, and should be made clear to the customer at the start of the business relationship that they are responsible for informing the firm if any details change.

Characteristics and Evidence of Identity

The identity of an individual has a number of aspects: e.g., his/her given name (which of course may change), date of birth and place of birth. Other facts about an individual accumulate over time (the so-called electronic “footprint”). Evidence of identity can take a number of forms such as passports and photo card driving licences, and these are often the easiest way of being reasonably satisfied as to someone’s identity. It is, however, possible to be reasonably satisfied as to a customer’s identity based on other forms of confirmation, including, in appropriate circumstances, written assurances from persons or organisations that have dealt with the customer for some time.

How much identity information or evidence to ask for, and what to verify, in order to be reasonably satisfied as to a customer’s identity, are matters for the judgement of the firm, which must be exercised on a risk-based approach, taking into account factors such as:

- The nature of the product or service sought by the customer (and any other products or services to which they can migrate without further identity verification).
- The nature and length of any existing or previous relationship between the customer and the firm.
- The nature and extent of any assurances from other regulated firms that may be relied on.
- Whether the customer is physically present.

Evidence of identity can be in documentary or electronic form. An appropriate record of the steps taken, and copies of, or references to, the evidence obtained, to identify the customer must be kept.

Firms should recognise that some documents are more easily forged than others. If suspicions are raised in relation to any document offered, firms should take whatever practical and proportionate steps are available to establish whether the document offered has been reported as lost or stolen.

Electronic Evidence

Electronic data sources can provide a wide range of confirmatory material without involving the customer. Where such sources are used for a credit check, the customer’s permission is required under the Data Protection Act. A number of commercial agencies which access many data sources are accessible online by firms, and can provide firms with a composite and comprehensive level of

electronic verification through a single interface. For an electronic check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time.

Persons Firms Should Not Accept as Customers

The United Nations, European Union, and United Kingdom are each able to designate persons and entities as being subject to financial sanctions. Such sanctions normally include a comprehensive freeze of funds and economic resources, together with a prohibition on making funds or economic resources available to the designated target. Firms will not normally have any obligation under UK law to have regard to lists issued by other organisations or authorities in other countries; although a firm doing business in other countries will need to be aware of the scope and focus of relevant financial sanctions regimes in those countries. Firms need to ensure that they have some means of monitoring payment instructions to ensure that proposed payments to targets or their agents are not made. Where a firm freezes funds under financial sanctions legislation, or where it has suspicions of terrorist financing, it must make a report to HM Treasury, and/or to SOCA.

A number of organisations have been proscribed under UK anti-terrorism legislation. Where such organisations are also subject to financial sanctions (an asset freeze), they are included on the Consolidated List maintained by HM Treasury.

Shell Banks and Anonymous Accounts

Firms must not enter into, or continue a correspondent banking relationship with a shell bank, or set up an anonymous account or an anonymous passbook for any new or existing customer. As soon as possible after 15 December 2007, all firms carrying on business in the UK must apply CDD measures to all existing anonymous accounts and passbooks, and in any event, before such accounts or passbooks are used in any way. Firms should also pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that may favour anonymity and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

Private Individuals

The firm should obtain the following information in relation to a private individual:

- full name
- residential address
- date of birth

If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the firm reasonable confidence in the customer's identity, although the firm should weigh these against the risks involved.

If identity is to be verified from documents, this should be based on:

- Compliance
- Internal Audit
- Risk Management
- Corporate Governance

Either a government-issued document which incorporates:

- the customer's full name and photograph,
- and either
 - his or her residential address, or
 - his or her date of birth.

Such documents include:

- Valid passport
- Valid photocard driving licence (full or provisional)
- National Identity card (non-UK nationals)
- Firearms certificate or shotgun licence
- Identity card issued by the Electoral Office for Northern Ireland

If none of these is available, a government-issued document (without a photograph) which incorporates the customer's full name, supported by a second document, either government-issued, or issued by a judicial authority, a public sector body or authority, or another FSA-regulated firm in the UK financial services sector, or in a comparable jurisdiction, which incorporates:

- the customer's full name
- and either
 - his or her residential address, or
 - his or her date of birth

Such documents include:

- a) Government-issued documents without a photograph include:
 - Valid (old style) full UK driving licence
 - Recent evidence of entitlement to a state or local authority-funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grant
- b) Other documents include:
 - Instrument of a court appointment (such as liquidator, or grant of probate)
 - Current council tax demand letter, or statement
 - Current bank statements, or credit/debit card statements, issued by a regulated financial sector firm in the UK, EU or comparable jurisdiction (but not ones printed off the internet)
 - Utility bills (but not ones printed off the internet)

Non Face-to-Face Identification and Verification

Firms are required to take account of the greater potential for money laundering or terrorist financing which may arise when the customer is not physically present when being identified. This would include assessing the possibility that the customer is deliberately avoiding face-to-face contact. It is therefore important to be clear on the appropriate approach in these circumstances. The extent of verification in respect of non face-to-face customers will depend on the nature and

characteristics of the product or service requested and the assessed money laundering risk presented by the customer.

Mitigation of Impersonation Risk

Non face-to-face identification and verification carries an inherent risk of impersonation fraud. Where identity is verified electronically, or copy documents are relied on, a firm should apply an additional verification check to manage the risk of impersonation fraud. The additional check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or another measure, such as:

- requiring the first payment to be carried out through an account in the customer’s name with a UK or EU regulated credit institution or one from a comparable jurisdiction;
- verifying additional aspects of the customer’s identity, or of his or her electronic ‘footprint’;
- telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a “welcome call” to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;
- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);
- internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;
- requiring copy documents to be certified by an appropriate person (that is, someone in a position of responsibility, who knows, and is known by, a customer, and may reasonably confirm the customer’s identity).

Source of Funds as Evidence

Under certain conditions, where the money laundering or terrorist financing risk in a product is considered to be at its lowest, a payment drawn on an account with a UK or EU regulated credit institution, or one from a comparable jurisdiction, and which is in the sole or joint name of the customer, may satisfy the standard identification requirement. Whilst the payment may be made between accounts with regulated firms or by cheque or debit card, the accepting firm must be able to confirm that the payment (by whatever method) is from a bank or building society account in the sole or joint name(s) of the customer. Firms will need to be able to demonstrate why they considered it to be reasonable to have regard to the source of funds as evidence in a particular instance.

Customers Who Cannot Provide the Standard Evidence

Some customers may not be able to produce identification information equivalent to the standard, for example some low-income customers in rented accommodation, customers with a legal, mental or physical inability to manage their affairs, individuals dependent on the care of others, dependant spouses or minors, students, refugees and asylum seekers, migrant workers and prisoners.

The FSA Rules adopt a broad view of financial exclusion, in terms of ensuring that, where people cannot reasonably be expected to produce standard evidence of identity, they are not unreasonably denied access to financial services. Where a firm concludes that an individual customer cannot reasonably meet the standard identification requirement, it may accept as identification evidence a letter or statement from an appropriate person who knows the individual, that indicates that the person is who he or she says they are.

Where a firm has concluded that it should treat a customer as financially excluded for the purposes of customer identification, and the customer is identified by means other than standard evidence, the reasons for doing so should be documented.

In cases where the available evidence of identity is limited, and the firm judges that the individual cannot reasonably be expected to provide more, but that the business relationship should nevertheless go ahead, it should consider instituting enhanced monitoring arrangements over the customer's transactions and activity.

Non-Private Individuals

Depending on the nature of the entity, a relationship or transaction with a customer who is not a private individual may be entered into in the customer's own name, or in that of specific individuals or other entities on its behalf. Beneficial ownership may, however, rest with others, either because the legal owner is acting for the beneficial owner, or because there is a legal obligation for the ownership to be registered in a particular way.

In deciding who the beneficial owner is in relation to a customer who is not a private individual, the firm's objective must be to know who has ownership or control over the funds which form or otherwise relate to the relationship, and/or form the controlling mind and/or management of any legal entity involved in the funds. Verifying the identity of the beneficial owner(s) will be carried out on a risk-based approach, following the guidance already provided, and will take account of the number of individuals, the nature and distribution of their interests in the entity and the nature and extent of any business, contractual or family relationship between them.

Standard Evidence

A firm should obtain the following in relation to the non-private individual concerned:

- full name
- registered number
- registered office in country of incorporation
- business address

and, additionally, for private companies:

- names of all directors
- names of beneficial owners holding over 25% (where a principal owner is another corporate entity or trust, the firm should take measures to look behind that company or trust and

establish the identities of its beneficial owners or trustees, unless that company is publicly quoted)

The firm should verify the identity from:

- either a search of the relevant company registry
- or confirmation of the company's listing on a regulated market
- or a copy of the company's Certificate of Incorporation

In respect of trusts, the firm should obtain the following information:

- Full name of the trust
- Nature and purpose of the trust (e.g., discretionary, testamentary, bare)
- Country of establishment
- Names of all trustees
- Name and address of any protector or controller

KYC - Additional Customer Information

A firm may conclude, under its risk-based approach, that the standard evidence of identity is insufficient in relation to the money laundering or terrorist financing risk, and that it should obtain additional information about a particular customer.

Information additional to the customer's identity, for a personal or non-personal customer, as appropriate, might include some or all of the following, depending on the firm's risk assessment of the customer:

- nature and details of the business/occupation/employment;
- record of changes of address;
- the expected source and origin of the funds to be used in the relationship;
- initial and ongoing source(s) of wealth or income (particularly within a private banking or wealth management relationship);
- copies of recent and current financial statements;
- the various relationships between signatories and with underlying beneficial owners;
- the anticipated level and nature of the activity that is to be undertaken through the relationship.

Monitoring Customer Activity

In addition to carrying out customer due diligence, a firm may need to monitor customer activity to identify, during the course of a continuing relationship, unusual activity. If unusual events cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions throughout a relationship helps give greater assurance that the firm is not being used for the purposes of financial crime.

Nature of Monitoring

Monitoring may be by reference to specific types of transactions, to the profile of the customer, or by comparing their activity or profile with that of a similar, peer group of customers, or through a combination of these approaches. Effective monitoring is likely to be based on a considered identification of transaction characteristics, such as:

- the unusual nature of a transaction: e.g., abnormal size or frequency for that customer or peer group; the early surrender of an insurance policy;
- the nature of a series of transactions: for example, a number of cash credits;
- the geographic destination or origin of a payment: for example, to or from a high-risk country;
- the parties concerned: for example, a request to make a payment to or from a person on a sanctions list.

Suspicious Activities and Reporting

Persons in the regulated sector are required to make a report in respect of information that comes to them within the course of a business in the regulated sector:

- where they know or
- where they suspect or
- where they have reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing.

Internal Reporting

The obligation to report to the nominated officer within the firm where they have grounds for knowledge or suspicion of money laundering or terrorist financing is placed on all relevant employees in the regulated sector. All financial sector firms therefore need to ensure that all relevant employees know who they should report suspicions to.

If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to NCIS [now SOCA] as soon as is practicable. If the nominated officer decides not to make a report to NCIS, the reasons for not doing so should be clearly documented, or recorded electronically, and retained with the internal suspicion report.

External Reporting

Firms should include in each suspicious activity report (SAR) as much relevant information about the customer, transaction or activity that it has in its records. In particular, the law enforcement agencies have indicated that details of an individual's occupation/company's business and National Insurance number are valuable in enabling them to access other relevant information about the customer.

Tipping Off, and Prejudicing an Investigation

POCA contains two separate sections creating offences of tipping off and prejudicing an investigation. This means that a firm:

- cannot, at the time, tell a customer that a transaction is being delayed because a report is awaiting consent from SOCA;
- cannot later – unless law enforcement/SOCA agrees, or a court order is obtained permitting disclosure – tell a customer that a transaction or activity was delayed because a report had been made under POCA;
- cannot tell the customer that law enforcement is conducting an investigation.

Staff Awareness and Training

FSA specifically requires the MLRO to have responsibility for ensuring that the firm's systems and controls include appropriate training for the firm's employees in relation to money laundering. Where a staff member is held to have had reasonable grounds for knowing or suspecting money laundering, but failed to make a disclosure, he will have a defence under POCA if he does not know or suspect, and has not been provided with AML training by his employer. No such defence is available under the Terrorism Act.

Firms should take reasonable steps to ensure that relevant employees are aware of:

- their responsibilities under the firm's arrangements for the prevention of money laundering and terrorist financing, including those for obtaining sufficient evidence of identity, recognising and reporting knowledge or suspicion of money laundering or terrorist financing;
- the identity and responsibilities of the nominated officer and the MLRO;
- the potential effect on the firm, on its employees personally and on its clients, of any breach of that law.

Record Keeping

Firms must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement. FSA-regulated firms must take reasonable care to make and keep adequate records appropriate to the scale, nature and complexity of their businesses.

Part Two

Wealth Management

The firm must endeavour to understand the nature of the client's business and consider whether it is consistent and reasonable, including:

- Compliance
- Internal Audit
- Risk Management
- Corporate Governance

- the origins of the client's wealth
- the nature and type of transactions
- the client's business and legitimate business structures
- for corporate and trust structures - the chain of title, authority or control leading to the ultimate beneficial owner, settler and beneficiaries, if relevant and known
- the use made by the client of products and services
- the nature and level of business to be expected over the account

The firm must then be satisfied that a client's use of complex business structures and/or the use of trust and private investment vehicles, has a genuine and legitimate purpose.

A relationship manager who undertakes a client visit should make a record by documenting:

- the date and time of the visit
- the address or addresses visited
- a summary of both the discussions and assessments
- any commitments or agreements
- any changes in client profile
- the expectations for product usage, volumes and turnover going forward
- any international dimension to the client's activities and the risk status of the jurisdictions involved

Non-Life Providers of Investment Fund Products

In this sector, the obligation to verify a customer arises at the point when it is clear that they wish to enter into an arrangement with the firm, either to buy or sell units in a fund or to establish some form of investment scheme or account.

Firms must verify a customer's identity as soon as practicable after first contact with the customer, but are not prevented from entering into a relationship or transaction before the checks are completed. Where the firm is unable to verify the identity of the investor within a reasonable time it may, if satisfied that there is a minimal risk of money laundering, return any monies received to the investor. Alternatively, the firm may decide in any event to retain control of any funds or assets until verification is completed or, where there are grounds to suspect money laundering, until consent has been obtained.

Discretionary and Advisory Investment Management

The identity of any trustees with authority to give instructions regarding the portfolio should be verified. For corporate customers, the identity of the owners and controllers of the company should be verified as appropriate. A firm must carry out appropriate due diligence on third party investment vehicles to establish and verify their form, status, purpose, and the identity of any persons who are in positions of control.

Financial Advisers

Financial advisers should bear in mind that they are often the party which is carrying out the initial customer identification and verification process. As such, it is they who will be asked to confirm to a product or service provider that such verification has been carried out.

Execution-Only Stockbrokers

The risk level of execution only broking depends on whether the services are offered and operated on a face-to-face or non face-to-face basis. The ML Regulations identify non-face-to-face business as a higher risk for money laundering than face-to-face business. In view of this, firms need to have in place additional measures to neutralise the higher risk when opening and operating accounts for non face-to-face business. It may be appropriate for a firm to subject non face-to-face applications to increased scrutiny by a review of the account applications by a senior manager, who should document their approval to the account being opened.

Private Equity

Where the manager is regulated and subject to supervision in the UK, the EU or a comparable jurisdiction, no further identification work would normally be required. Where the manager is not from a comparable jurisdiction, even though it may be regulated, or where the manager is unregulated but operates in a comparable jurisdiction (as is often the case in the US venture capital industry, for example) the firm needs to exercise its judgement as to the likely risk presented by investors in the fund. Factors to take into consideration include:

- the profile of the manager;
- its track record in the private equity industry; and
- its willingness to explain its identification procedures and provide confirmation that all underlying investors in the fund have been identified and are known to the manager.

Where a corporate investor is not well-known to the private equity firm and is quoted on a regulated market or exchange which is not located in the UK, the EU or in a comparable jurisdiction, the firm should seek to establish, where possible, who the corporate investor's external accountants, lawyers and brokers are, and their reputation in the market, before making a decision on what, if any, further verification of identity is required.

Wholesale Markets

It is very important to distinguish the relationship that exists between the various parties associated with a transaction. In particular, the firm should be clear whether it is acting as agent or principal on behalf of the customer, and whether the firm has a responsibility to verify the identity of any underlying customers involved in transactions.

The money laundering or terrorist financing risks for firms operating within the wholesale markets sector can be mitigated by the implementation of monitoring procedures. Monitoring in wholesale firms will be affected by the fact that firms may only have access to a part of the overall picture of their customer's trading activities. The fact that many customers spread their activities over a

number of financial firms will mean that many firms will have a limited view of a customer's trading activities and it may be difficult to assess the commercial rationale of certain transactions.

Unregulated Funds

The level of risk actually posed by the unregulated fund will depend upon the nature of the fund and its transparency. Where the fund is the customer of a firm, the requirements for identification and verification of corporate structures, trusts, and individuals should be applied to the fund. A firm should also undertake due diligence on the entities involved with the fund, namely: the investment manager that has direct contact with the firm; 'relevant investors' (investors who have a 25% or more interest in the fund); and the ultimate controller(s) where they are not the investment manager.

© CPA Audit LLP. Version 2, April 2008