Discussion Paper

22

Financial Services Authority

Reducing money laundering risk

Know Your Customer and anti-money laundering monitoring

August 2003

Contents

The Financial Services Authority invites comments on this Discussion Paper. Please send us your comments to reach us by 30 January 2004.

Comments may be sent by electronic submission using the form on the FSA's Website (at www.fsa.gov.uk/pubs/dp/dp22_response.html).

Alternatively, please send comments in writing to:

Daniel Shonfeld
Financial Crime Policy Unit
Prudential Standards Division
25 The North Colonnade
Canary Wharf
London E14 5HS

Telephone: 0207 066 5644
Fax: 0207 066 5645
E-mail: dp22@fsa.gov.uk

It is the FSA's policy to make all responses to discussion papers available for public inspection unless the respondent requests otherwise.

1 Executive summary

1.1 The purpose of this Discussion Paper (DP) is to stimulate debate on two important anti-money laundering controls:

- 'Know Your Customer' (KYC) (that is, obtaining and using information about a customer[1] over and above the basic identification information); and
- monitoring (that is, being alert to how a customer is using a firm's products and services and therefore to signs of money laundering).

1.2 This debate will help us decide whether to make any changes to our Handbook and also help the industry make well-informed decisions about risk management practices.

1.3 For both KYC and monitoring, there are no specific legal or regulatory requirements. But both are relevant to an effective contribution to the fight against money laundering, crime and terrorism, as well as to the high-level legal and regulatory obligations. And authoritative good practice guidance sets expectations that firms will collect and use KYC information in appropriate cases and will have an active approach to monitoring. We raise the question of whether firms can adequately manage their money laundering risks and meet their high-level legal and regulatory obligations without fulfilling these expectations.

1.4 On both topics, current practice varies, partly because of differences in risk profile, but also through differences in the professionalism of risk management techniques.

1.5 On KYC we refer to existing good practice standards concerning the scope of KYC information that firms might obtain. We also highlight the importance of firms using information about their customers that they have obtained for

1 In this DP we use the term 'identification' to mean the basic information (name and address) collected to meet the legal and regulatory identification requirements. We use the term 'Know Your Customer' or 'KYC' to refer to the additional information (e.g. occupation) that a firm may obtain for anti-money laundering risk management purposes. We use the term 'customer' to refer to both customers and clients (the term more usually used in some kinds of business).

other regulatory, or for their own business, purposes. And we touch on some practical issues, such as:

- the difficulty of keeping information up to date;
- the problem of verification;
- cost;
- the need to maintain data protection standards; and
- the need to retain consumer confidence.

1.6 In our discussion of monitoring we refer to the varied industry practice and suggest a model for a firm's approach to monitoring. We also discuss practical issues, including cost and customer privacy. We recognise that what monitoring involves in practice will vary according to the kind of business a firm does – for example, whether the business is retail or non-retail and the kind of service provided. This DP is about both automated and non-automated approaches to monitoring, but we specifically discuss the former in view of the significant development and increased use of automated systems.

1.7 This DP sets out four possible options. These are:

- to make new specific rules and/or guidance on KYC and/or monitoring (which could include a direct link to the Joint Money Laundering Steering Group (JMLSG) Guidance Notes);
- to make new high-level rules and/or guidance, to promote better money laundering risk management by firms;
- to make no new rules or guidance; and to rely on the JMLSG Guidance Notes to promote adequate standards in regulated firms; or
- to make no decision now and review the position again in, say, two years time.

1.8 In this paper, we also ask for responses to these questions.

Q1: How necessary is the collection of KYC information and an active approach to monitoring in reducing money laundering risk and in meeting legal and regulatory obligations, in particular reporting?

Q2: How should firms pursue a risk-based approach to anti-money laundering?

Q3: What type of monitoring (and reports) would be most useful to law enforcement agencies?

Q4: What are, or may be, the costs and benefits of KYC and monitoring?

Q5: Which options presented do you prefer and why?

1.9 We welcome feedback on any aspect of this paper, but in particular on the areas where we have raised questions. **The deadline for comments is 30 January 2004.**

Who should read this paper?

1.10 This paper is relevant to regulated firms, specialist anti-money laundering advisers and suppliers of automated monitoring systems. It is also of interest to law enforcement agencies and government, in terms of setting the UK's anti-crime agenda and priorities, and in the latter's role as arbiter of the balance between individual privacy and the fight against crime and terrorism.

CONSUMERS

The purpose of anti-money laundering controls is to help deter, detect, investigate and prosecute crime (generally, not just financial crimes) and terrorism. This is important to consumers as citizens.

Anti-money laundering controls may also help detect fraud, including identity fraud, at an early stage. This may help prevent consumers suffering financial loss.

This paper will be of interest to consumers of all regulated firms. They may be concerned about privacy and data protection issues if firms acquire, keep and use personal information as part of their increased anti-money laundering monitoring. These issues need to be balanced against the benefits of more effective crime and terrorism prevention and detection.

2 Introduction

2.1 The objective of this paper is to stimulate debate about two important areas of anti-money laundering practice, to help us decide whether to make changes to our Handbook and to help the industry to make well-informed risk management decisions.

Structure of this DP

2.2 In **Chapter 3** we address issues about Know Your Customer (KYC).

In **Chapter 4** we address issues about monitoring.

In **Chapter 5** we summarise the options and ask for responses to specific questions.

Annexes provide relevant background information.

Why this DP will be relevant to all firms

2.3 All regulated firms[2] are subject to high-level obligations to take reasonable care to set up and maintain effective systems and controls for countering the risk that they might be used for a purpose connected with financial crime. This DP is relevant to all firms, retail and wholesale, whatever regulated business they do and however many customers they have.

Our approach to anti-money laundering

2.4 Our approach in this DP reflects in particular:

- our reduction of financial crime objective (which requires us to have particular regard to firms' systems, controls and risk management) (see **Annex 1**);

2 General insurance and pure reinsurance business are exempt from the government Money Laundering Regulations 1993 (and 2003) and from our Money Laundering Sourcebook.

- the principles of good regulation[3] (in particular those dealing with the responsibilities of senior management, proportionality, and international competitiveness);
- our risk-based approach to regulation (see below); and
- international and national law and industry good practice standards.

A risk-based approach

2.5 This DP is, to a significant degree, about the practical application of a risk-based approach to anti-money laundering.

2.6 We have set out in several publications our risk-based approach to regulation[4]. A risk-based approach applies not only to our own activities; it is also what we expect of firms. In the case of anti-money laundering controls, without a risk-based approach firms' costs will be disproportionate, the effectiveness of the UK's regime will be diluted, and the regime will also be overly burdensome for customers.

2.7 The new Financial Action Task Force (FATF) Recommendations[5], the JMLSG Guidance Notes[6] and the Basel Committee[7] explicitly endorse a risk-based approach. Our Handbook already requires it[8].

2.8 A risk-based approach is not a soft option. It puts the responsibility on firms – and their boards and senior management – to identify, assess, mitigate and monitor their money laundering risks on a considered and continuing basis. These include the legal, regulatory and reputational risks to a firm caught laundering money or failing to have adequate controls in place.

2.9 A risk-based approach is a systematic approach to risk management. It involves:

- **risk identification and assessment –** identifying the money laundering (and associated legal, regulatory and reputational) risks facing the firm, given its customer, product and service profile and having regard to available information including published typologies[9] etc. And assessing the potential scale of those risks and of the possible impact if they crystallised;
- **risk mitigation –** identifying and applying measures effectively to mitigate the material risks emerging from the assessment;

3 See the Financial Services and Markets Act section 2(3).

4 For more information see: Building the new regulator – Progress report 1 (December 2000), Building the new regulator – Progress report 2 (February 2002) and the Firm risk assessment framework (February 2003).

5 Published in June 2003.

6 See, for example, paragraph 4.9 of the December 2001 edition.

7 See Part II of Customer due diligence for banks. Basel Committee on Banking Supervision. October 2001.

8 See Senior Management Arrangements, Systems and Controls (SYSC) 3.1.2 G

9 Typologies have been published by FATF and the Egmont Group of Financial Investigation Units (both available on the FATF Website) and by the JMLSG in the Guidance Notes (Appendix B).

- **risk monitoring** – putting in place management information systems and keeping up to date with changes to the risk profile through changes to the business or to the threats; and
- **documentation** – having policies and procedures that cover the above and deliver effective accountability from the board and senior management down.

The legal, regulatory and good practice framework

2.10 We need to develop our policy having regard not only to what is in (or might be put in) our own Handbook. We also need to have regard – as do regulated firms – to a complex framework of EU and UK law, international standards, industry-developed guidance and indicators of evolving industry good practice. Moreover, the effectiveness of our, and the industry's, contribution is critically dependent on input from the law enforcement agencies who are the front line. **Annex 2** (**a**) summarises the international and UK legal and regulatory framework and (**b**) summarises the UK anti-money laundering institutional framework. For ease of reference, our own relevant existing rules and guidance are set out in **Annex 3** and **Annexes 4** and **5** summarise other relevant authoritative sources of obligation and guidance on KYC and monitoring, respectively.

3 Know Your Customer

3.1 In this chapter we focus on KYC, covering:

- current legal and regulatory obligations and industry good practice standards;
- what KYC information firms might obtain;
- why firms may have existing KYC information; and
- practical issues relating to acquiring and using KYC information.

What is the purpose of KYC?

3.2 KYC serves two main purposes:

i. to help firms to manage effectively their money laundering risks, by reducing the likelihood that they will take on a money launderer as a new customer and increasing the likelihood that they will detect the use of their products and services for money laundering; and

ii. to help firms meet their reporting obligations under the Proceeds of Crime Act 2002 (PoCA) (see **Annex 6**).

3.3 KYC information also helps law enforcement agencies decide whether to initiate and whether to pursue an investigation.

Legal and regulatory requirements

3.4 Although there are no specific legal or regulatory KYC (as opposed to simple identification) requirements, high-level obligations in the Money Laundering Regulations[10] and in our Handbook (see **Annex 3**) require a firm to counter the risk of money laundering. And firms may find that they are exposed to

10 The Money Laundering Regulations 1993 5(1)(iv) states, firms should have "such other procedures of internal control and communication as may be appropriate for the purposes of forestalling and preventing money laundering". This is expected to be carried over in the Money Laundering Regulations 2003.

increased legal risk of failing to meet their reporting obligations under PoCA[11] if they focus on basic identification evidence and do not collect or use wider KYC information.

3.5 The Home Office is to use its powers under PoCA[12] to prescribe the form which firms must use to make Suspicious Activity Reports (SARs) and how firms must make them. Currently, the National Criminal Intelligence Service (NCIS) ask firms to use a form on the NCIS Website (the form is also in an annex in the JMLSG Guidance Notes). In a Consultation Document[13], the Home Office discusses the information that might be included in a prescribed form, and what information fields should be mandatory and what should be discretionary. In the case of SARs about individuals it might include the date of birth, occupation, employer and National Insurance number. And in the case of SARs about companies, the type of business.

Good practice standards

3.6 The FATF Recommendations, the JMLSG Guidance Notes, the Basel Committee, and the Wolfsberg Group[14] all state (see **Annex 4**) that additional information over and above identification information should be obtained and used by firms. This is to help the firm to assess the risk of money laundering at the outset of the relationship and to continue to assess this risk during the course of the relationship. Knowing what is usual for or expected of a customer allows the firm to identify what is unusual, which places the firm in a better position to manage its money laundering risk.

Scope of KYC information

3.7 If firms obtain more information about their customers than just identification information, what information may need to be collected? The information suggested in the various good practice documents referred to in **Annex 4** includes:

- the purpose and reason for opening the account or establishing the relationship;
- the anticipated level and nature of the activity that is to be undertaken;
- the various relationships of signatories and underlying beneficial owners;

11 Section 330 (2)(b) requires a firm to report where they have reasonable grounds for knowing or suspecting that someone is engaged in money laundering.

12 See section 339

13 Home Office Consultation Paper: The Proceeds of Crime Act 2002 Part 7 (Money Laundering) Section 339 Form and Manner of Disclosures. August 2002.

14 The Wolfsberg Group consists of 12 leading international banks that published global anti-money laundering guidelines for international private banks in October 2000 and for correspondent banks in November 2002.

- the expected source and origin of the funds to be used in the relationship;
- details of occupation/employment (for personal bank current accounts);
- sources of wealth or income (particularly within a private banking relationship); and
- net worth.

We recognise that the amount and type of information will vary according to the type of customer (personal or business), product and risk.

Why firms may have existing customer information

3.8 KYC for anti-money laundering purposes should not be considered in isolation. Firms often obtain a significant amount of information for other purposes. The availability of information obtained for other purposes is important in assessing the cost and practical implications of KYC for anti-money laundering purposes. It is also important for anti-money laundering risk management purposes. That is why the Money Laundering Sourcebook (ML) requires a firm to take reasonable steps to give its Money Laundering Reporting Officer (MLRO) access to any 'Know Your Business' information it has. It is also relevant to the PoCA 'objective test', since it may bear on whether a firm has reasonable grounds for suspicion.

3.9 **Conduct of Business requirements.** Many firms are subject to our Know Your Customer and suitability requirements[15] to obtain sufficient personal and financial information about a customer relevant to the services that the firm is providing. This information is expected[16] to be sufficient to provide an analysis of a customer's personal and financial circumstances, leading to a clear identification of the customer's need, so that a suitable investment can be recommended. Our guidance also indicates that, when assessing affordability, regard should be had to the customer's current level of income and expenditure and any likely future changes.

3.10 **Firms' business needs.** Firms obtain customer information when someone becomes a new customer, or applies for a new product or service, to enable them to decide whether to accept the application. Firms also use this information to help them understand the profile of individual customers, or of its customers as a whole, for marketing and product development purposes. So, account and product application forms often include fields for such items as residential status, employment details, income and other sources of income.

15 See Conduct of Business (COB) 5.2.5 R.

16 See Conduct of Business (COB) 5.2.11 G.

3.11 **Credit risk management.** Before lending, a firm will normally obtain enough information to be satisfied that the customer will be able to meet the liability. This will usually include information on income and on expenditure patterns.

3.12 **Customer relationship management.** Increasingly, firms obtain, analyse and use information about their customers for customer relationship management (CRM) purposes. This helps them to personalise products and services and to build customer relationships (particularly in non-face-to-face business), to increase selling opportunities and to improve customer loyalty.

Some practical issues

3.13 The acquisition and use of KYC information raises a number of practical issues.

3.14 **Amount of information and its verification.** Verification is important to effective identification. That is why firms are expected to seek independent corroboration of name and address. So far as KYC information is concerned, practice varies according to the circumstances. For example, firms are likely to verify income and assets before giving a secured loan, but not routinely to verify employment, source of wealth, or reason for business in the case of savings or investment accounts.

3.15 This differentiation will partly reflect a view of what is needed for business purposes. It may also reflect a view about customers' willingness to provide information unless they consider it appropriate and proportionate in the circumstances. For example, customers may be more willing to provide information when they are applying for credit, or seeking a continuing wealth management service, than in opening a basic savings account or a non-discretionary investment service.

3.16 A relevant factor is the increased tendency for individuals to have more than one product and service, and more than one supplier for a main bank account, savings accounts, unit trusts, life policies, securities broking, discretionary or non-discretionary fund management, credit etc. In the case of banking relationships, how much a bank knows about its customer will depend on whether the customer uses the bank for principal income payments and regular debits, or whether it is a secondary banking relationship.

3.17 In practice, under a risk-based approach, it will not be appropriate for every service supplier to know their customers equally well, regardless of the purpose, use, value etc. of the product or service provided. Firms' information demands need to be proportionate, appropriate and discriminating, and capable of being justified to customers.

3.18 **Maintenance and updating.** Even where a firm obtains KYC information at the outset of a relationship, it may not be easy for the firm to maintain it - for example, when the customer experiences a job change, a new source of

income (e.g. property rental), or a change of wealth (e.g. inheritance, bonus). The JMLSG Guidance Notes suggest that firms should take reasonable steps to keep the information up-to-date as appropriate, and as new opportunities arise – for example, when an existing customer opens a new account. They also suggest that updated information obtained through any meetings, discussions or other communication with the customer should be kept.

3.19 Opportunities for updating information may arise when a customer takes out a new product. Customers may volunteer new information on their own initiative. Customers with a credit or insurance relationship with their firm may be under a contractual obligation to inform the firm of a material negative change of circumstances (e.g. loss of income or a critical illness). It would not seem practical, however, to expect firms to oblige customers generally to update the information that the firm has when a material change of circumstances occurs.

3.20 **Cost.** Acquiring, storing and maintaining personal information creates costs for firms. They require systems, capacity, data protection and data integrity processes. They can significantly increase the cost of moving from legacy to new systems or of combining databases (for example, after a merger or take-over).

3.21 **Customer privacy and data protection.** In considering what KYC information to obtain and maintain, firms need also to meet their obligations under the Data Protection Act 1998 (DPA). Firms must ensure that personal information held by them is accurate, up-to-date, relevant, adequate but not excessive for its purpose, securely held and not kept longer than is necessary. There are also constraints on using customer data unless given the customer's express, informed consent.

3.22 Firms should also be alert to the provisions under the Human Rights Act 1998 that everyone has the right to respect for his or her private and family life, his or her home and his or her correspondence.

3.23 These requirements will have implications for the cost of data maintenance. They will also impact on the ability of firms to use information obtained for the purposes of anti-money laundering for commercial purposes such as marketing. However, we do not consider that data protection considerations constrain the effective use by firms of KYC information to meet legal or regulatory requirements.

4 Anti-money laundering monitoring

4.1 In this chapter we focus on anti-money laundering monitoring, covering:

- current legal and regulatory obligations and industry good practice standards;
- current industry practice and the reasons for increasing interest;
- good monitoring processes, and the need to tailor them to suit different kinds of business; and
- automated monitoring systems.

4.2 By anti-money laundering monitoring, we mean a firm's use of systems and controls to be actively alert to indications of unusual use by a customer of its products and services. And through this to seek to detect and address circumstances that suggest that their products and services may be being used to launder money. Those systems and controls may, but need not, include an automated element. So this chapter is about both automated and non-automated monitoring.

Current legal and regulatory requirements

4.3 Although neither the law nor our Handbook impose specific requirements to monitor, there are relevant legal and regulatory obligations including those applying to the MLRO (see **Annexes 2 and 3**).

4.4 So a firm that does not attempt to pick up what may be unusual for its business may be exposing itself to a higher risk of money laundering (and falling short of these obligations) than a firm taking an active approach.

Good practice standards

4.5 The new FATF Recommendations in 2003 have stronger statements about monitoring (whether manual or automated) than the previous version (see **Annex 5**). Both the JMLSG Guidance Notes and the Basel Committee (see

Annex 5) treat monitoring as an essential component of anti-money laundering control, particularly in the case of higher risk accounts. In general these sources give two main reasons for monitoring as good practice:

i. it helps the firm to be alert to signs of money laundering by highlighting what is unusual for a customer or different to their peers; and

ii. using adequate KYC information in conjunction with monitoring allows firms to make a judgement about whether an activity or transaction is suspicious – helping the firm to comply with their reporting obligations.

Industry practice

4.6 Our knowledge of industry practice has grown progressively through our:

- Money Laundering Theme project[17];
- subsequent reviews of practice in different sectors (see Summary reports on our Website[18]);
- visits (over a hundred) since N2 by our Risk Review Team[19]; and
- informal discussions with firms, specialist consultants and providers of automated systems.

4.7 We found that the large deposit-taking firms have invested heavily in automated systems, but most firms continue to rely on staff vigilance, which in some cases is complemented by systems of exception reporting.

Reasons for increased industry interest in monitoring

4.8 A number of developments have increased the industry's focus on anti-money laundering monitoring. In particular:

i. **changing business methods.** The increase in non-face-to-face business, the decline in the relationship manager and the greater propensity of customers to change service providers and to have multiple service providers have made relationships between firms and their customers much more remote. This means that detecting unusual activity can be more difficult.

ii. **increased industry risk awareness.** The new regulatory dimension, the increased focus on terrorist finance, and the introduction of PoCA have made the industry more sensitive to reputational and regulatory risks.

17 The Money Laundering Theme. Tackling our new responsibilities. July 2001.

18 www.fsa.gov.uk/what/ml_thematic. Domestic banking – August 2002, on-line broking and spread-betting – October 2002, IFAs taking customer money – February 2003, international banking – June 2003.

19 This team includes money laundering experts that assist FSA supervisors to conduct money laundering visits.

iii. **terrorist finance.** Firms find it difficult to meet their obligations in relation to sanctions[20] without some continuing monitoring and capacity to interrogate their customer data.

iv. **scale.** Firms with millions of customers and high volumes of transactions see automation as essential to the effective management of their risks.

v. **technological development.** Suppliers and firms themselves have developed automated monitoring systems, often out of other systems used for other purposes (e.g. credit risk management).

Monitoring processes

4.9 The authoritative standards, and industry practice, suggest that effective monitoring (automated or otherwise) is likely to involve several elements.

4.10 **Risk assessment.** Monitoring is active, not passive. It must be based on a considered identification of characteristics that justify further scrutiny, for example:

- the unusualness of a transaction (e.g. abnormal size or frequency for that customer);
- the nature of a transaction (e.g. the early surrender, or the assignment to a third party, of an insurance policy);
- the nature of a series of transactions (e.g. a number of cash credits);
- the geographic destination or origin of a payment (e.g. to or from a high-risk country); or
- the parties concerned (e.g. a payment to or from a person on a sanctions list).

4.11 It is the individual firm that is best placed to identify what is unusual, given its particular business and customer profile, and to have regard to publicly available money laundering typologies and other sources of experience and expertise.

4.12 The unusual is not the same as the suspicious. Even customers with a stable and predictable transactions profile (for example, routine direct debits, routine salary payments) will have periodic unusual transactions – a house purchase, an investment realisation, a gift etc. And many customers will, for perfectly good reasons, have a persistently erratic pattern of transactions. Identifying what is unusual, therefore, is only the starting point – firms must assess whether what is unusual gives rise to suspicion.

20 United Nations Security Council resolutions require the imposition of sanctions on named individuals or entities. The UK implements these resolutions by directions under the Terrorism (United Nations Measures) Order 2001. The Bank of England acts as the Treasury's agent in this matter.

4.13 **Detection.** Arrangements to enable the firm to spot specific unusual transactions. These could be automated. They could involve the training of staff to spot and deal specially (e.g. by upward referral) with situations that suggest increased money laundering risk. Or, they could involve exception reporting by reference to objective triggers (e.g. transaction amount).

4.14 **Internal reporting and review.** Arrangements for the internal reporting, via line management or directly to the MLRO, of unusual transactions so that they may be reviewed by staff with enough experience and judgement to be able to assess whether the unusual is suspicious, and a decision made about any further action.

4.15 **External reporting to NCIS.** Arrangements under which the MLRO and the MLRO's staff review unusual transactions and, where appropriate, make suspicious activity reports to, and/or seek the consent of, NCIS. Firms need to meet their legal obligations, increased by PoCA. The reports they make to NCIS need also to be of adequate quality, in terms of the information which they include.

4.16 **Review and feedback.** Arrangements for continuing review of the firm's experience (with alerts, internal reports and SARs), and of any new external information about threats and typologies, so that it may learn from experience and revise its systems and risk profiling as necessary.

Some practical issues

4.17 An active approach along these lines raises several issues.

4.18 **Cost.** The industry is concerned about the increased costs of anti-money laundering. The specific cost implications of automated monitoring are discussed below. Both automated and other systems of active monitoring require more systematic money laundering risk assessment, staff training, processes for making and reviewing alerts and management time. Firms may be able to build on monitoring arrangements they have for other purposes – for example, credit risk management, combating fraud, market integrity or market settlement. Although this investment may benefit the firm in reducing its financial crime (including fraud), reputational and regulatory risks, the overall benefits significantly depend on SARs making a material contribution in practice to the fight against crime and terrorism.

4.19 **Customer privacy.** Increasing customer awareness of firms' responsibilities to make SARs to NCIS will require the government, law enforcement agencies and the industry to promote adequate customer understanding of, and support for, the purpose and value of this surveillance[21]. So far as industry is concerned, this may mean increased transparency with their customers about their anti-

21 The Treasury, NCIS and the FSA launched a public information campaign on money laundering on 24 June 2003.

money laundering responsibilities and sensitive application of anti-money laundering controls in practice.

4.20 **Relationship with identification.** Some argue that effective monitoring should enable the industry to reduce the effort put into identification. It is not open to us to vary the identification requirements of the law, and there are no current proposals to change those requirements. So, effective monitoring is unlikely to replace or modify the need for basic identification.

What might monitoring involve for different kinds of firm?

4.21 The financial services industry is very diverse. Monitoring arrangements should be appropriate in nature, scale and sophistication to the size, nature and scale of the business.

4.22 Some financial services business typically involves infrequent transactions with customers about whom the business has a good deal of information, acquired for both business and regulatory reasons. Life insurance and pensions business, advisory (including IFA) investment business, discretionary fund management and private banking business may fall into this category. In these cases, the main needs will be for:

- high standards of initial risk identification and assessment when new customers are taken on;
- continuing staff training and alertness, so that transactions that justify review are picked up;
- awareness of money laundering risk in the relationship management context, so that events that should trigger further enquiry can be identified for review; and
- robust internal and external reporting practices.

4.23 Other types of financial business involve frequent transactions with customers about whom the business may need to have only limited information for regulatory or their own business purposes. Deposit-taking, broking and on-line business may fall into this category. In these cases, over and above robust customer take-on procedures and staff alertness, firms may have a greater need for ongoing monitoring. The greater the volume of transactions, the less easy it will be for a firm to do that without the aid of automation.

Automated monitoring systems

4.24 For many firms, the question of automated monitoring may not be relevant. However, for some firms, it will need to be considered. Systems available include anti-fraud systems that many firms, particularly those that offer credit, use to monitor fraud. These use rules-based systems to look for patterns in

transactions or account behaviour which may indicate that fraud is taking place. Although not specifically designed for anti-money laundering, these types of monitoring can give rise to knowledge, suspicion or reasonable grounds to suspect that someone is engaged in money laundering. Automated systems raise a number of issues.

4.25 **Cost.** Automated monitoring can be, but does not have to be, expensive. The costs will vary according to firms' needs and circumstances. There are a range of options, and not all are sophisticated or costly. The costs range from several thousand pounds (for example, for exception reporting systems used by some on-line brokers) to millions of pounds. The initial cost will depend on such factors as:

- the capacity required;
- the volume of transactions to be processed;
- the complexity of the business – e.g. the number of branches;
- whether the system is developed in-house or bought, and, if bought, whether more or less 'off the shelf' or significantly customised;
- the sophistication of the functionality required;
- the compatibility with a firm's existing, legacy systems;
- the ease or otherwise of installation; and
- the IT systems required – hardware, software or internet.

4.26 After the initial investment, there will be additional and ongoing costs, such as ongoing support and upgrades; licensing; staff training to recognise suspicious activity; staff costs in operating the system; and any costs of dealing with additional internal reports and SARs.

4.27 **Effectiveness.** The effectiveness of a system, automated or manual, in identifying unusual activity will depend on the quality of the parameters which determine what alerts it makes, and the ability of staff to assess and act as appropriate on these outputs. So, the needs of each firm will be different, and each system will vary in its capabilities according to the scale, nature and complexity of the business. Examples of risk indicators drawn from bodies such as the JMLSG and FATF include:

- customer activity not consistent with their known personal or business profile;
- customers issuing unusual instructions;
- dealing with customers not normally expected in that part of the business;
- customers from high-risk jurisdictions;

- transfers to and from high-risk jurisdictions;
- unexplained changes in customer requirements or level of transaction/account activity;
- accounts involving offshore banks; and
- unexplained deposits of large cash amounts.

4.28 The system supplier and the user firm set the parameters and rules. Some risk indicators can be addressed straightforwardly – for example, the application of a list of high-risk countries. Many require judgement and understanding.

4.29 Users of automated systems see them playing a key role in the future. They assert that, realistically, only automated systems can efficiently scan and mine the volumes of transaction data experienced by, for example, the major retail deposit-takers. The purpose is to identify individual customers and transactions that might be problematic and patterns and relationships that require review (e.g. possible undetected organised threats, or indicators of vulnerability in the way in which the institution does its business). That is why substantial investments have been made to buy or develop automated systems and ongoing costs incurred on staff to review alerts generated by the systems.

4.30 However, users also recognise that they need to increase the precision and efficiency of their systems. The unusual is by no means the same as the suspicious. At present, the 'conversion rate' (the proportion of alerts that are 'converted' into SARs) for automated alerts tends to be much lower than in the case of alerts generated by staff. So users are investing considerable effort to learn from experience, refine the parameters for alerts, factor in feedback etc. Significant expert resource is being applied by providers and users to develop and evolve the parameters used to generate automatic alerts. As with any automated systems, it seems likely that the functionality and capacity of systems will increase, and their costs reduce, over time.

4.31 Users recognise that no automated system can meet all the firm's needs. Nor can a system eliminate the need for human review of alerts before reports are made to NCIS. So, it is essential to continue to attach importance to human alertness. Such factors as staff intuition, direct exposure to a customer face-to-face or on the telephone, and the ability, through practical experience, to recognise transactions that do not seem to make sense for that customer cannot be replaced.

Firms' understanding of their automated monitoring systems

4.32 So, in considering their own monitoring needs, firms need to be able to assess the value that an automated system may add to manual systems and controls. They also need to be confident that the parameters determining the outputs of the system they use are appropriate. Firms need to understand how their

systems work and how they generate alerts. They must not simply equate alerts generated as grounds for suspicion and for making SARs to NCIS.

4.33 In assessing an external system, or developing a system internally, a firm – and that means in particular the senior management responsible, including the MLRO – must know, and be comfortable with, in the circumstances of the firm:

- the data being monitored;
- the parameters being applied for monitoring – from simple exception reports to complex multiple relationships;
- why the system generates alerts; and
- how the firm is going to evaluate alerts critically.

5 Options and questions

5.1 In Chapters 3 and 4 we sought to identify the main issues relating to KYC and anti-money laundering monitoring. On both, the question is whether, without an active approach, a firm would be sufficiently confident that it can:

- effectively manage its substantive money laundering risks and associated reputational risks; and
- meet its high-level legal and regulatory obligations.

5.2 There is considerable diversity of practice amongst firms. This partly reflects differences of risk profile and in risk management techniques. But it also reflects differences in firms' attitudes – for example, to the systematic use of customer information for anti-money laundering purposes. It also reflects differences of quality – for example, in the professionalism of firms' anti-money laundering risk management techniques. Too many firms do not take the basic steps of identifying and assessing their own specific money laundering risks and developing a policy and putting in place arrangements to manage them.

5.3 Against that background, should we include new provisions in our Handbook on these matters? Since this is a DP we do not set out firm proposals or conclusions. Our aim at this stage is to prompt debate and to obtain the views of interested stakeholders.

Options

5.4 In our view, our main options (not mutually exclusive) are as follows.

5.5 **Option 1 – include in the Handbook specific rules and/or guidance on KYC and/or monitoring**, as we have on such topics as identification, internal and external reporting, and the role of the MLRO. This gives us several broad possibilities.

(a) *New **specific rules***

5.6 The first possibility would be provisions that include specific **rules** (that is, enforceable requirements) requiring firms to take reasonable steps (in countering the risk that their firm may be used for money laundering) to obtain KYC information over and above identification information. These rules could also require firms to monitor the use that their customers make of their products and services.

5.7 The 'reasonable steps' qualification would make the obligation risk-based. What would be reasonable would depend on the money laundering risk profile of the firm (a judgement in the first instance for the firm itself). It would be in keeping with the roles of ML and the JMLSG Guidance Notes for any such rules to be complemented by guidance in the Guidance Notes to firms about what steps might be reasonable in different circumstances.

(b) *New **specific guidance***

5.8 We could include **guidance** in the Handbook. This would say that we expect firms, in developing effective systems and controls, to counter financial crime (SYSC 3.2.6 G), to have appropriate, considered policies and practices for obtaining and using KYC information, and/or for monitoring their customers' accounts (again, for the reasons referred to in paragraph 5.1 above).

5.9 We understand that some interpret SYSC 3.2.7 (3) G ('The FSA's detailed requirements for systems and controls with respect to money laundering are set out in the Money Laundering Sourcebook.') to mean that ML is an exhaustive statement of what SYSC 3.2.6 R requires in practice, so far as anti-money laundering systems and controls are concerned. We did not intend, and do not agree with, this interpretation. So we will consult on proposals to make it clearer that SYSC 3.2.7 (3) G is a signpost to the existence of ML, not a limitation on the scope of SYSC 3.2.6 G.

(c) *Extend the specific link between ML and the Guidance Notes beyond identification to cover (at least) KYC and monitoring.*

5.10 At present, ML commits us expressly to have regard to a firm's compliance with the JMLSG Guidance Notes only in relation to our identification requirements (see ML 3.1.4 G). This does not mean that in identification matters we treat the Guidance Notes as if they were our rules. They are industry guidance, not obligations. So, 'have regard to' means that we take what the Guidance Notes say into account in the particular context, not that we require rigid application of the Guidance Notes. Nor does the absence of an explicit reference mean that we totally disregard what the Guidance Notes say

on other matters relevant to compliance with ML[22]. The Guidance Notes may well be relevant in, for example, assessing a firm's anti-money laundering systems and controls in the context of SYSC 3.2[23].

5.11 However, the reference to the Guidance Notes in ML 3.1.4 G does give them a somewhat stronger status in the context of identification. A reference to the Guidance Notes in relation to other matters would need to relate to some specific requirement in our Handbook – in other words, we need a context in which we will 'have regard to' the Guidance Notes. This could be the general provisions in SYSC, or new general or specific provisions in ML, as referred to above. We propose to consult on broadening the link with the Guidance Notes.

Option 2 – include new high-level rules or guidance, or both, on money laundering risk management

5.12 We could include in ML more general rules or guidance, or both, requiring firms to assess and address their money laundering risks. This would be along the lines of the guidance under development for various prudential risks in the context of the Integrated Prudential Sourcebook. A relevant example is the proposed chapter on Operational Risk Systems and Controls[24], which envisages – draft 6.1.11 G – that firms should document their policy for managing operational risk. The guidance would state explicitly that firms should take reasonable steps to document their policy for managing their money laundering risk. That is how they identify, assess, monitor and control their money laundering risks, including an overview of the people, processes and systems that they use.

Option 3 – leave ML unchanged; rely on the JMLSG Guidance Notes

5.13 As set out in Annexes 4 and 5, the current Guidance Notes contain some relevant material on these topics. The JMLSG has embarked on a fundamental review of its Guidance Notes. This will cover the existing material on KYC and on monitoring. The JMLSG will no doubt reflect developments in practice and in industry needs for guidance in the context of the overall risk-based approach with which they are approaching the task. Our decisions, in the light of responses to this DP, will also need to take account of the likely future content of the Guidance Notes.

5.14 Consistent with the complementary roles of ML and the Guidance Notes, we could decide to include no specific material in ML and leave it to the Guidance Notes to meet industry's need for guidance on good practice in meeting their various legal, regulatory and risk management requirements.

22 See Enforcement Manual (11.9.1G)

23 SYSC Chapter 3.2, areas covered by systems and controls.

24 Operational risk systems and controls. CP 142. July 2002. See also feedback Policy Statement of March 2003.

Option 4 – make no settled decision now and review the position again in, say, two years time.

5.15 Under this option, our Handbook would remain unchanged for the present, so far as KYC and monitoring are concerned. We would review the position again in, say, 2005. This would not only enable us to take into account the revision of the Guidance Notes. We would also have the benefit of longer experience of the impact of PoCA and of the decisions made on the SAR process in the light of the KPMG review[25]. Developments in monitoring systems and practices would also be relevant.

Criteria for our decision

5.16 Our decision will take into consideration the following factors:

i. Risk to our financial crime objective

Is there sufficient risk to our financial crime objective as to need further action by us? If so, should that action include further Handbook material?

FSMA requires us to have particular regard to the desirability of firms being aware of the risk of their business being used in connection with money laundering, and to their taking appropriate measures (and devoting adequate resources) to prevent money laundering, facilitate its detection and monitor its incidence. **It would be particularly useful to receive responses on how firms currently match up to these risk management considerations.**

ii. Our risk mitigation tools

Developing the Handbook is only one of the tools available to us. Other relevant tools would be:

- to make it clear – not just through speeches but through our supervisory and enforcement action – that we believe that firms are already under sufficient obligations on KYC and monitoring;
- greater use of our industry training services; and
- reliance on the Guidance Notes (with no specific Handbook support) as adequate to achieve acceptable industry standards.

iii. Costs, benefits, and the principles of good regulation

We will accompany any proposals for specific changes to our Handbook with a cost benefit analysis. We would need to be satisfied that the benefits of change were consistent with the costs, and that changes met the tests in the principles of good regulation. This includes issues such as proportionality,

25 The Home Office Commissioned a report on behalf of NCIS to assess the UK's SAR regime. The report is available at www.homeoffice.gov.uk

responsibilities of senior management and competitiveness. **We would particularly welcome any comments on the actual or potential costs of an active, but risk-based, approach by firms to KYC and to monitoring. We would also welcome comments from law enforcement agencies on the benefits of such an approach.**

The government, in giving us the reduction of financial crime objective, brings financial firms into the fight against crime generally. Our role is to make sure firms have good controls – like identification, monitoring and reporting. These controls benefit firms by ensuring they are prudent in how, and with whom, they do business, and link with our other objectives. They also have wider benefits. They make a positive contribution to the work of law enforcement agencies in investigating and fighting crime. Our role is also to make sure that firms' efforts are focused in the most efficient and effective ways to help law enforcement agencies to fight crime and terrorism.

iv. Transparency

It is important that firms should know what their regulatory obligations are. This requires adequate clarity and completeness in our Handbook. **We would particularly welcome comments on whether firms are confident that they understand our regulatory requirements and what we expect of them.**

Questions

5.17 Over and above any general responses, we would welcome responses on the following questions.

Q1: How necessary is the collection of KYC information and an active approach to monitoring in reducing money laundering risk and in meeting legal and regulatory obligations, in particular reporting?

Q2: How should firms pursue a risk-based approach to anti-money laundering?

Q3: What type of monitoring (and reports) would be most useful to law enforcement agencies?

Q4: What are, or may be, the costs and benefits of KYC and monitoring?

Q5: Which options presented do you prefer and why?

The reduction of financial crime objective – section 6 Financial Services and Markets Act 2000

(1) The reduction of financial crime objective is: reducing the extent to which it is possible for a business carried on –

(a) by a regulated person, or

(b) in contravention of the general prohibition,

to be used for a purpose connected with financial crime.

(2) In considering that objective the Authority must, in particular, have regard to the desirability of –

(a) regulated persons being aware of the risk of their business being used in connection with the commission of financial crime;

b) regulated persons taking appropriate measures (in relation to their administration and employment practices, the conduct of transactions by them and otherwise) to prevent financial crime, facilitate its detection and monitor its incidence;

(c) regulated persons devoting adequate resources to the matters mentioned in paragraph (b).

(3) "Financial crime" includes any offence involving –

(a) fraud or dishonesty;

(b) misconduct in, or misuse of information relating to, a financial market;

(c) handling the proceeds of crime.

(4) "Offence" includes an act or omission which would be an offence if it had taken place in the United Kingdom.

(5) "Regulated person" means an authorised person, a recognised exchange or a recognised clearing house.

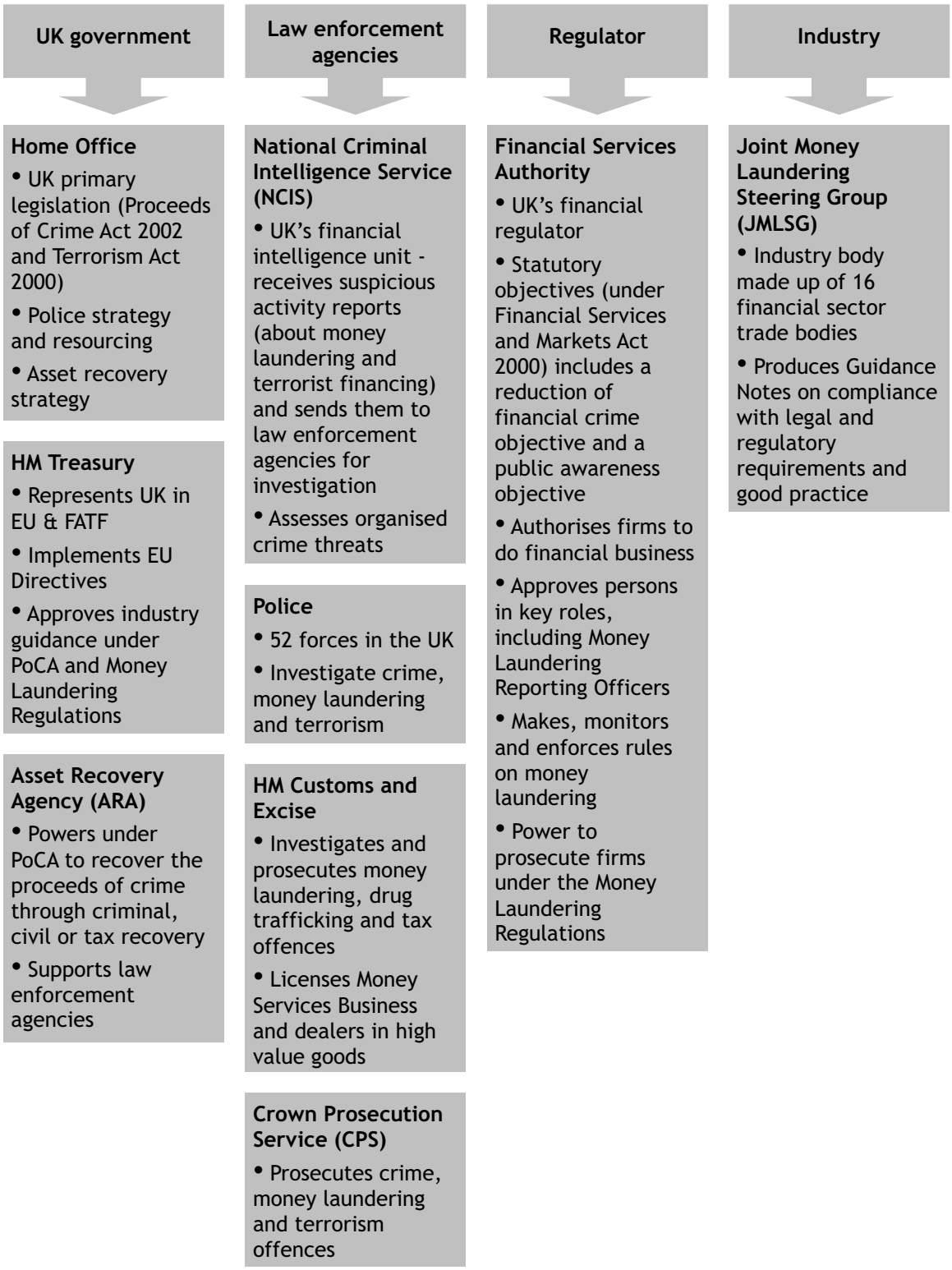
The International and UK Anti-Money Laundering Legal and Regulatory Framework

This diagram summarises the current UK and international legal and regulatory standards that determine or influence the UK's approach to money laundering.

International governmental standards	**The Financial Action Task Force (FATF)** - intergovernmental body, with 29 member countries, set up to combat money laundering. It issued 40 Recommendations in 1990, which were revised in 1996 and 2003. It issued 8 Special Recommendations on terrorist finance in 2001.
EU Money Laundering Directives	**1st Directive (1991)** - requires Member States to impose identification, reporting and other systems and controls requirements on credit and financial firms. **2nd Directive (2001) -** extends anti-money laundering controls to non-financial businesses (e.g. lawyers, accountants and dealers in high value goods).
UK primary legislation	**Proceeds of Crime Act 2002** - creates new money laundering offences and strengthens obligations on regulated firms to report money laundering. **Terrorism Act 2000** - consolidates law on terrorism and mirrors reporting obligations in the Proceeds of Crime Act.
UK secondary legislation	**Money Laundering Regulations 2003** - implements the EU 2nd Directive and consolidates and clarifies provisions of the Money Laundering Regulations 1993 (as subsequently amended).
International regulatory standards	**Basel Committee on Banking Supervision** (Customer due diligence for banks, October 2001) and **International Association of Insurance Supervisors** (Anti-money laundering guidance notes for insurance supervisors and insurance entities January 2002).
Regulation	**FSA's Handbook of rules and guidance (2001) -** imposes high-level obligations on firms to counter the risk of financial crime **(SYSC)**, mirrors specific requirements of the Regulations **(ML Sourcebook)**, places obligations on firms' senior management and makes the role of MLRO an approved person **(APER)**.
Industry guidance	**Joint Money Laundering Steering Group (JMLSG) -** industry body that issues Guidance Notes on legal and regulatory requirements and on good practice.

The UK Anti-Money Laundering Institutional Framework

This diagram summarises the institutional framework for anti-money laundering in the UK.



FSA Handbook of rules and guidance

This annex summarises the main provisions relating to anti-money laundering in our Handbook of rules and guidance (available at www.fsa.gov.uk).

Threshold conditions

A firm must satisfy the Threshold Conditions in order to obtain Part IV Permission – in particular, for anti-money laundering purposes, threshold condition 5 (suitability).

COND 2.5.7G 'In determining whether a firm will satisfy and continue to satisfy threshold condition 5 in respect of having competent and prudent management and exercising due skill, care and diligence, relevant matters, as referred to in COND 2.5.4G(2), may include, but are not limited to whether:

(10) the firm has in place the appropriate money laundering prevention systems and training, including identification, record keeping and internal reporting procedures (see ML)…'

Senior Management Arrangements, Systems and Controls (SYSC)

General high-level obligations are set out in the Senior Management Arrangements, Systems and Controls module.

SYSC 3.1.1 R states that 'a firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business'.

SYSC 3.1.2 G amplifies this rule by stating that the nature and the extent of the systems and controls which a firm will need to maintain will depend upon a variety of factors, including:

- the nature, scale and complexity of its business;
- the diversity of its operations, including geographical diversity;

- the volume and size of its transactions; and
- the degree of risk associated with each area of its operations.

SYSC 3.1.2 G also states that a firm should carry out a regular review of its systems and controls to enable it to comply with the obligation in the rule.

SYSC 3.2.6 R. requires firms to 'take reasonable care to establish and maintain effective systems and controls for…. countering the risk that the firm might be used to further financial crime'.

Money Laundering Sourcebook (ML)

The Money Laundering Sourcebook is the main source of our detailed anti-money laundering systems and controls rules and guidance. These cover in particular:

- identification;
- internal reporting;
- MLRO access to Know Your Business information;
- external reporting;
- making use of government and FATF findings;
- awareness and training;
- the role of the MLRO;
- compliance monitoring; and
- record keeping.

ML 3.1.4 G states that, in assessing a relevant firm's compliance with its duty to identify a client in accordance with ML 3.1.3 R, the FSA will have regard to the relevant firm's compliance with the Joint Money Laundering Steering Group's Guidance Notes for the Financial Sector.

ENF 11.9.1 G states that, the FSA's money laundering rules are set out in ML 1 to ML 8. The FSA, when considering whether to take disciplinary action in respect of a breach of those rules, will have regard to whether a firm has followed relevant provisions in the Joint Money Laundering Steering Group's Guidance Notes for the Financial Sector.

The Supervision Manual (SUP)

SUP 10.7.13 R makes the position of MLRO a controlled function, so the holder of the post must be approved by us.

The Code of Practice for Approved Persons (APER)

APER 4.7.9 E states that, in the case of the MLRO, failure to discharge his responsibilities under chapter 7 of ML is conduct that does not comply with Statement of Principle 7 for Approved Persons, namely that 'an approved person performing a significant influence function must take reasonable steps to ensure that the business of the firm for which he is responsible in his controlled function capacity complies with the relevant requirements and standards of the regulatory system'.

Know Your Customer – statements of good practice

This annex contains extracts from key authoritative international and UK statements of good practice regarding Know Your Customer.

Financial Action Task Force – The Forty Recommendations (June 2003)

(available at www.1.oecd.org/fatf)

Customer Due Diligence and Record-keeping (extract)

Recommendation 5

The customer due diligence measures (CDD) to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship; and

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The

measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

The Joint Money Laundering Steering Group Guidance Notes (December 2001)

(information on how to obtain the Guidance Notes is available at www.jmlsg.org.uk)

Basic Principles and Objectives of Money Laundering Prevention and Compliance

1.13

e) Satisfactory "Know Your Customer" procedures must be established to identify the users of financial services, the principal beneficial owners and the origin of the funds being deposited or invested. Other than for one-off transactions, it also includes knowing the nature of the business that the customer normally expects to conduct; and being alert to transactions that are abnormal within the relationship.…

The Nature and Level of the Business to be Conducted

4.9. The second requirement of knowing the customer is to ensure that sufficient information is obtained on the nature of the business that the customer expects to undertake, and any expected, or predictable, pattern of transactions. **A risk based approach will be needed in respect of the extent of the additional information that might be required or validated for this purpose.**

4.10. Information collected at the outset for this purpose might include:

a) the purpose and reason for opening the account or establishing the relationship;

b) the anticipated level and nature of the activity that is to be undertaken;

[Note: for many products, a) and b) above may be implicit or self evident e.g. credit cards, retail credit sales, loan accounts, single premium or term investments, and savings accounts. However, for other more complex products they may not be, e.g. corporate accounts, private banking accounts, investment banking and fund management arrangements].

c) the expected origin of the funds to be used within the relationship.

[Note: in many cases, this will be covered by funds being drawn from an account in the customer's name at another bank or building society or from salary payments paid directly into the account].

d) details of occupation/employment might be sought for bank current accounts and sources of wealth or income will be required for some banking relationships, particularly within a private banking relationship.

4.11. Following the start of the relationship, reasonable steps should be taken to keep the information up to date as appropriate and as opportunities arise e.g. when an existing customer opens a new account. Any updated information obtained through any meetings, discussions or other communication with the customer should be recorded and kept with the customer's records to ensure, as far as practicable, that current customer information is readily accessible to the MLRO or, for FSA regulated firms, the supervisor under the FSA's "Know Your Business" requirements.

Basel Committee on Banking Supervision

Customer due diligence for banks (October 2001) (extract)
(available at www.bis.org)

4. … KYC safeguards go beyond simple account-opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts…

6. … enhanced diligence is required in the case of higher-risk accounts or for banks that specifically aim to attract high net-worth customers.

27. Banks need to obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate etc.) and the expected size of the account.

Wolfsberg AML Principles

(available at www.wolfsberg-principles.com)

Global Anti-Money-Laundering Guidelines for Private Banking (May 2002)

1. Client acceptance: general guidelines

1.3 *Due diligence*

It is essential to collect and record information covering the following categories:

- Purpose and reasons for opening the account

- Anticipated account activity
- Source of wealth (description of the economic activity which has generated the net worth)
- Estimated net worth
- Source of funds (description of the origin and the means of transfer for monies that are accepted for the account opening)
- References or other sources to corroborate reputation information where available.

Unless other measures reasonably suffice to do the due diligence on a customer (e.g. favourable and reliable references), a customer will be met prior to account opening.

Client acceptance: situations requiring additional diligence/attention

2.1 General

In its internal policies, the bank must define categories of persons whose circumstances warrant additional diligence. This will typically be the case where circumstances are likely to pose a higher than average risk to a bank.

2.2 Indicators

The circumstances of the following categories of persons are indicators for defining them as requiring additional diligence:

- Persons residing in and/or having funds sourced from countries identified by credible sources as having inadequate anti-money laundering standards or representing high risk for crime and corruption.
- Persons engaged in types of business activities or sectors known to be susceptible to money laundering.
- "Politically Exposed Persons" (frequently abbreviated as "PEPs"), referring to individuals holding or having held positions of public trust, such as government officials, senior executives of government corporations, politicians, important political party officials, etc., as well as their families and close associates.

Global Anti-Money Laundering Principles for Correspondent Banking (5 November 2002)

4 Risk-Based Due Diligence

These Principles advocate a risk-based approach. Correspondent Banking Clients presenting greater risk should be subjected to a higher level of due diligence. These Principles outline the type of risk indicators that an institution shall consider in initiating the relationship, and on a continuing

basis, to ascertain what reasonable due diligence or enhanced due diligence it will undertake. In particular, the institution will consider these risk indicators:

- The Correspondent Banking Client's Domicile…..
- The Correspondent Banking Client's Ownership and Management Structures...
- The Correspondent Banking Client's Business and Customer Base….

5 Due Diligence Standards

All Correspondent Banking Clients shall be subjected to appropriate due diligence that will seek to assure that an institution is comfortable conducting business with a particular client given the client's risk profile….

6 Enhanced Due Diligence

In addition to due diligence, each institution will also subject those Correspondent Banking Clients that present greater risks to enhanced due diligence…

11 Updating Client Files

The institution's policies and procedures shall require that the Correspondent Banking Client information is reviewed and updated on a periodic basis or when a material change in the risk profile of the Correspondent Banking Client occurs. Periodic review of the Correspondent Banking Clients will occur on a risk-assessed basis.

Monitoring – statements of good practice

This annex contains extracts from key authoritative international and UK statements of good practice regarding monitoring.

Financial Action Task Force – The Forty Recommendations (June 2003)

(available at www.1.oecd.org/fatf)

Recommendation 5

The customer due diligence (CDD) measures to be taken are as follows:

d) conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the customer due diligence measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

Recommendation 11

Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

Recommendation 21

Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

Joint Money Laundering Steering Group Guidance Notes (December 2001)

(information on how to obtain the Guidance Notes is available at www.jmlsg.org.uk)

Know your customer – the basis for recognising suspicions

5.7 Sufficient guidance must be given to staff to enable them to recognise potentially suspicious transactions. However, the type of situations giving rise to suspicions will depend on a firm's customer base and range of services and products. As some products and services are more vulnerable to money laundering than others, a risk-based approach might be appropriate.

5.8 Satisfactory "know your customer" procedures provide the foundation for recognising unusual and suspicious transactions. **Where there is a business relationship, a suspicious transaction will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account.** Therefore, the first key to recognition is knowing enough about the customer and the customer's normal expected activities to recognise when a transaction, or series of transactions, is abnormal.

5.9 Questions that staff might be encouraged to consider when determining whether an established customer's transaction might be suspicious are:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer's business or personal activities?
- Has the pattern of transactions conducted by the customer changed?
- Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

5.10 Firms might also consider monitoring the types of transactions and circumstances that have given rise to suspicious transaction reports by staff, with a view to updating internal instructions and guidelines from time to time.

5.11 Additional vigilance and monitoring procedures should be applied to relationships involving senior political figures, their immediate families and close associates…

Joint Money Laundering Steering Group Guidance Notes (Draft 20 June 2003)

(N.B. This text is subject to change and to approval by HM Treasury.)

Monitoring procedures to assist KYC

5.12 Ongoing monitoring of customer activity, either through manual procedures or computerised systems, is one of the most important aspects of effective KYC procedures. The type of monitoring procedures introduced will depend on a number of factors, including the size and nature of the business and the complexity and volume of the transactions or activity. Financial sector firms can only determine when they might have reasonable grounds to suspect money laundering if they have the means of assessing when a transaction or instruction falls outside their expectations or when it falls within one of the circumstances that should normally give rise to further enquiry, such as those illustrated in 5.11 above.

5.13 The extent of KYC information necessary both at the outset and ongoing, and the transaction monitoring that is required, will need to be assessed taking a risk-based approach. However, as stated in Section 4 paragraphs 4.9 and 4.10, the information requested and updated must be reasonable in the circumstances and regard must be had to a customer's right to privacy.

5.14 Higher risk accounts and customer relationships will generally require more frequent or intensive monitoring. For higher risk situations, e.g. private bank accounts and wealth management relationships, the following should be considered:

- Firms should assess whether they have adequate procedures or management information systems in place to provide relationship managers and MLROs with timely information. The type of information that may be needed includes transactions made through a customer's account that are unusual, the nature of a customer's relationship with the firm, and any readily identifiable connected accounts and relationships.
- The personal circumstances and sources of wealth and income for higher risk customers should be recorded, reviewed on a regular basis annually and, wherever possible, verified to check their legitimacy.

- Firms should seek to develop a clear policy, procedures and controls in respect of business relationships with customers who are known, suspected, or advised, to be politically exposed persons (PEPs) or with persons and companies that are clearly related or associated with them (see Section 2 paragraphs 2.28 – 2.33). As all PEPs may not be identified initially, and because existing customers may subsequently acquire PEP status, regular reviews for identifying PEP customers should be undertaken.
- Firms should consider reviewing the KYC information held on file and the activity for higher risk customers at least annually. Firms should consider the centralisation of their data in order to streamline the audit of higher risk customers.

Basel Committee on Banking Supervision

Customer due diligence for banks (October 2001)
(available at www.bis.org)

3. *Ongoing monitoring of accounts and transactions*

53. Ongoing monitoring is an essential aspect of effective KYC procedures. Banks can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The extent of the monitoring needs to be risk-sensitive. For all accounts, banks should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert banks to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account. Examples of suspicious activities can be very helpful to banks and should be included as part of a jurisdiction's anti-money-laundering procedures and/or guidance.

54. There should be intensified monitoring for higher risk accounts. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, they type of transactions involved, and other risk factors. For higher risk accounts:

- Banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. The types of reports that may be needed include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank.
- Senior management in charge of private banking business should know the personal circumstances of the bank's high risk customers and be alert to sources of third party information. Significant transactions by these customers should be approved by a senior manager.
- Banks should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them.[16] As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

Wolfsberg AML Principles

(available at www.wolfsberg-principles.com)

Global Anti-Money Laundering Guidelines for Private Banking (May 2002)

5 Monitoring

5.1 Monitoring Program

A sufficient monitoring program must be in place. The primary responsibility for monitoring account activities lies with the private banker. The private banker will be familiar with significant transactions and increased activity in the account and will be especially aware of unusual or suspicious activities (see 4.1). The bank will decide to what extent fulfilment of these responsibilities will need to be supported through the use of automated systems or other means.

5.2 Ongoing Monitoring

With respect to clients classified under any category of persons mentioned in 2, the bank's internal policies will indicate how the account activities will be subject to monitoring.

16 (Footnote taken as part of an extract from the Basel Committee on Banking Supervision). It is unrealistic to expect the bank to know or investigate every distant family, political or business connection of a foreign customer. The need to pursue suspicions will depend on the size of the assets or turnover, pattern of transactions, economic background, reputation of the country, plausibility of the customer's explanations etc. It should however be noted that PEPs (or rather their family members and friends) would not necessarily present themselves in that capacity, but rather as ordinary (albeit wealthy) business people, making the fact they owe their high position in a legitimate business corporation only to their privileged relation with the holder of the public office.

Global Anti-Money Laundering principles for correspondent Banking (5 November 2002)

12 Monitoring and Reporting of Suspicious Activities

The institution shall implement bank-wide policies and procedures to detect and investigate unusual or suspicious activity and report as required by applicable law. These will include guidance on what is considered to be unusual or suspicious and give examples thereof. The policies and procedures shall include appropriate monitoring of the Correspondent Banking activity.

The Proceeds of Crime Act 2002

This annex summarises the main changes made by the Proceeds of Crime Act 2002 (PoCA) to the UK's money laundering offences, investigation powers and asset recovery powers. In particular, PoCA:

- extends the obligation to report to NCIS (by replacing the offence of failing to report when a person had *knowledge or suspicion* of drug money laundering) to report any kind of money laundering when a person within the regulated sector[26] *knows or suspects or has reasonable grounds to know or suspect* that somebody is engaged in money laundering;
- creates a single set of money laundering offences (by bringing into line the law on laundering the proceeds of drug and non-drug offences) that are applicable throughout the UK to the proceeds of any property obtained through criminal conduct;
- makes NCIS the single recipient of Suspicious Activity Reports (SARs);
- provides for the Home Secretary to prescribe the form in which reports must be made and the manner in which they are sent to NCIS;
- creates the concept of the 'nominated officer' to receive internal reports – this will normally be the Money Laundering Reporting Officer (MLRO) – who is under a duty to make reports to NCIS in appropriate cases;
- makes it clear that if a firm has knowledge, suspicion or reasonable grounds to know or suspect that somebody is engaged in money laundering before a transaction is carried out they must seek consent from NCIS to qualify for a defence against a charge of money laundering;
- contains new investigation powers for use in tracing the proceeds of crime and investigating money laundering – a *customer information* order requires a firm to identify any account held by a person under investigation

26 A person within the regulated sector will be defined in the Proceeds of Crime Act 2002 (Business in the Regulated Sector and Supervisory Authorities) Order 2003 when it comes into force.

and an *account monitoring* order requires a firm to provide transaction information on a suspect account for a specified period of time; and

- establishes an Asset Recovery Agency (ARA) to investigate and secure criminal assets – the Director of the ARA has the powers to use the civil recovery scheme to recover the proceeds of crime where a prosecution is not available or recover any outstanding tax on gains suspected from crime.

Failure to comply with the PoCA reporting obligations is punishable on conviction of 5 years imprisonment.

The money laundering and asset recovery provisions came into force on 24 February 2003.

Glossary

ARA	Asset Recovery Agency
Basel Committee	The Basel Committee on Banking Supervision was established by the central bank Governors of the Group of Ten countries, which includes the UK. The Committee formulates broad supervisory standards and guidelines and recommends statements of best practice for banking supervisory authorities to implement in ways best suited to their own national systems
Customer	In this paper we use the term 'customer' to refer to both customers and clients (client is a term used in wholesale business)
FATF	The Financial Action Task Force is an intergovernmental body. Its Secretariat is based at the Organisation for Economic Co-operation and Development (OECD). Its purpose is to develop and promote policies to combat money laundering and terrorist financing. It has 29 member countries, including the UK
First EU Money Laundering Directive	The Council Directive of 10 June 1991 on prevention of the use of the financial system for the purposes of money laundering (No. 91/308/EEC)
Forty Recommendations	International good practice standards issued by the Financial Action Task Force
FSA	Financial Services Authority
FSMA	Financial Services and Markets Act 2000

Handbook	FSA Handbook of rules and guidance
Identification	In this paper refers to the collection of basic information (name and address) to meet the identification obligations in the Money Laundering Regulations 1993 and FSA Money Laundering Sourcebook
JMLSG	Joint Money Laundering Steering Group
KYC	In this paper Know Your Customer refers to the additional information (e.g. occupation) that a firm may obtain for anti-money laundering risk management purposes over and above the basic identification information
ML	FSA Money Laundering Sourcebook
Money laundering	Money laundering is defined in section 340(11) of the Proceeds of Crime Act and section 18 of the Terrorism Act 2000
Money Laundering Regulations 1993	Money Laundering Regulations 1993 (SI 1993/1933) implement the First European Money Laundering Directive
Money Laundering Regulations 2003	The Money Laundering Regulations 2003 (when they come into force) implement the requirements of the Second European Money Laundering Directive and consolidate, clarify and update the existing provisions of the Money Laundering Regulations 1993
Monitoring	In this paper monitoring means being alert to how a customer is using a firm's products and services and therefore to signs of money laundering
MLRO	Money Laundering Reporting Officer
NCIS	National Criminal Intelligence Service
N2	1 December 2001 – the date the FSA's powers came into force
PoCA	Proceeds of Crime Act 2002
SARs	Suspicious Activity Reports (sometimes known as Suspicious Transaction Reports (STRs))

Second EU Money Laundering Directive	The Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purposes of money laundering
SYSC	Senior Management Arrangements, Systems and Controls module of the FSA Handbook
Wolfsberg	The Wolfsberg Group consists of 12 leading international banks that published global anti-money laundering guidelines for international private banks in October 2000 and correspondent banks in November 2002

ISBN: 0117045446

The Financial Services Authority
25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000 Fax: +44 (0)20 7066 1099
Website: http://www.fsa.gov.uk