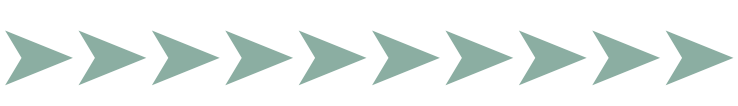
Financial Services Authority

Review of firms' implementation of a risk-based approach to anti-money laundering (AML)

March
2008



Contents

Introduction 1

Executive summary 3

Findings 9

Money laundering risk assessment 9

Senior management responsibility 12

Changes to AML policies and procedures 15

Customer due diligence 17

Enhanced due diligence 19

Correspondent banking 20

Monitoring customer activity 21

Staff awareness and training 23

Introduction

The move to more principles-based regulation is a key part of our strategy and has been endorsed by the Better Regulation Task Force. Where financial crime is concerned, we adopted this approach in August 2006 when we replaced the detailed rules contained in the Money Laundering Sourcebook with high-level rules in the Systems and Controls (SYSC) section of our Handbook, backed up by the industry-written Joint Money Laundering Steering Group Guidance. This Guidance, in effect, fleshes out the requirements of SYSC to give practical help to firms in assessing and mitigating their money laundering risk and putting in place an effective and efficient AML control environment. (Under SYSC, when considering whether a breach of our rules on systems and controls against money laundering has occurred, we will have regard to whether a firm has followed relevant provisions in the guidance for the UK financial sector issued by the Joint Money Laundering Steering Group.)

The broad intention of the Guidance is to encourage firms to adopt a risk-based approach by focusing their financial crime resources on areas of higher risk. That does not detract, however, from the need for firms to do their own analysis of where their risks lie, in order to make a risk-based approach effective. Such an approach will, for example, ensure that lower risk customers do not suffer from unduly burdensome procedures and requirements. And, on the other hand, it will ensure that firms undertake enhanced due diligence whenever that is required, ie, for customers and business lines that pose higher risk.

Accordingly, in line with a public commitment we gave in our FSA Business Plan 2007/8, our newly formed Financial Crime Operations Team launched a major project in June 2007, aimed at establishing the extent to which a wide range of firms across the financial services industry had adapted to the new SYSC rules and the revised JMLSG Guidance that accompanied those rules.

Please note that the period of the review pre-dated the coming into force, on 15 December 2007, of the Money Laundering Regulations 2007, which introduced the risk-based approach into UK AML law by requiring all relevant persons to establish and maintain 'appropriate and risk-sensitive' policies to enable them to comply with the various requirements of the new regulations.

The project entailed visits to 43 firms in total, ranging from major high-street banks, building societies, insurers and asset managers to some very small firms in both the wholesale and retail sectors. We gathered additional information on approximately 90 small firms by means of a survey, posing a limited number of fairly high level questions to the Money Laundering Reporting Officer of each firm and, where appropriate, following up the answers given with a telephone call.

This report sets out our findings under broad headings, which cover the key aspects of a firm's AML systems and controls. For ease of analysis and comparison, we have categorised our findings by size of firm: large, medium and small.

We envisage that firms will find the report useful in enabling them to benchmark their own efforts to manage money laundering risk effectively against those of their peers in the financial services industry. The report should also give firms a clearer idea of our expectations.

This report does not constitute formal guidance from the FSA given under section 157 of the Financial Services and Markets Act. The report is published for information but, if you have comments, please send them to:

John Ellis
Financial Crime & Intelligence Division
The Financial Services Authority
25 The North Colonnade
London E14 5HS
Email: john.c.ellis@fsa.gov.uk
Telephone: 020 7066 0976

Executive Summary

Overview

- The following points, set out under the same headings as we have used in the main body of this report, summarise the key findings of our review. These findings include observations of good practice adopted by firms, as well as some examples of poor practice.
- We were pleased to find many examples of good practice, particularly in the way that large firms had fully embraced the risk-based approach to AML and senior management's accountability for effective AML.
- We recognise that smaller firms, which generally represent lower risk, have fewer resources to devote to money laundering risk assessment and risk mitigation measures. But we found clear room for improvement in some firms. In particular, firms must ensure that staff are adequately trained, and they should not treat reviewing AML policies and procedures as a one-off exercise.
- The Joint Money Laundering Steering Group Guidance, written by the industry and endorsed by the Treasury, is readily available to provide firms with practical help in meeting their legal and regulatory obligations in the areas of both anti-money laundering and terrorist financing.
- Firms must have effective ways of managing their money laundering risks and meeting their obligations. If they do not align their AML processes with those recommended by the JMLSG, they will need to demonstrate that their alternative approach is as effective in achieving those outcomes.

Money laundering risk assessment

- Most **large firms** had undertaken a formal money laundering risk assessment. The Money Laundering Reporting Officers (MLROs) in these firms had also documented the risks posed by their customers and products/business lines. In two cases, the firms had commissioned consultants to carry out a further review of AML policies and procedures and to quality assure the MLRO's money laundering risk assessment and mitigation measures.
- Risk-scoring information was typically fed into a risk matrix that staff were required to use when taking on new clients and would determine what level of Know Your Customer (KYC) information was required for taking on that client.

- Not all large firms had considered how often their risk assessment would be reviewed. Some said that it was a continual process; others said that it would happen as and when new products were launched; some intended to review their money laundering risk profile annually; and others said it would be a one-off exercise or had not considered it at all.
- Most **medium-sized** firms had assessed the money laundering risks in their business, but these assessments varied greatly in scope and sophistication.
- Those medium-sized firms that had not conducted a formal risk review were generally more concerned about fraud risk to their business than money laundering risk, although they recognised the risk of reputational damage if they were found to have been used as a vehicle for money launderers.
- Medium-sized firms that had undertaken extensive risk analysis, and changed their AML policies and procedures as a result, believed that the changes had reduced the burden on clients. Firms themselves expected to derive benefits from gaining a level of assurance that, as resources were now targeted to areas of higher risk, the firm as a whole was at less risk from fraud or reputational damage.
- Most **small firms** had carried out some kind of risk assessment, some with the help of consultants.
- The majority of small firms classified the risk of money laundering across their businesses as low, although some identified certain products or client types as higher risk.
- Small firms gave a number of reasons for low risk classification, including the fact that they were dealing with funds already in the system and that business was introduced by lawyers and accountants.

Senior management responsibility

- **Large firms** had made relatively few changes to senior management accountability for an effective AML control environment. Formal responsibility was already held at a sufficiently senior level.
- The key consideration was that the MLRO had sufficient influence to persuade executive business management to implement, and maintain, adequate AML measures. That influence might derive either from the MLRO's own seniority within the firm or from his direct reporting line to the chief executive or to another member of the firm's senior management with a seat on the Board or a key Board Committee.
- We found a good level of communication and interaction between MLROs and their line managers. The same was broadly true in UK firms with head offices abroad, and a global head of AML based outside the UK.

- Management information (MI) on AML issues was often communicated up to the Board via the Audit Committee or Group Risk Committee.
- Within **medium-sized** firms, AML risk tended to be viewed in the same way as any other risk to the business and chief executives were generally committed to ensuring that AML controls were given adequate attention. Overarching responsibility for AML was seen by some chief executives as their responsibility, although in many firms the day-to-day responsibilities were delegated. Often, the MLRO reported directly to, or had regular meetings with, the chief executive.
- MLROs were generally senior managers with compliance and oversight responsibilities. Where MLROs had multiple roles, with few exceptions, they were able to devote sufficient time to AML.
- MLRO Annual Reports were adequately detailed and described how firms measured the success of their AML policies and procedures.
- Most **small firms** had appointed a senior manager to oversee AML controls, in addition to an MLRO. In most of these firms, AML issues were discussed regularly with senior management, either informally or at Board meetings, or were communicated upwards as regular MI.
- With one exception, small firms produced an annual MLRO Report. MLROs took responsibility for implementing recommendations from the report and, in some cases, this was monitored by the Board or senior executive management. MLROs were generally able to report directly to the Board.

Changes to AML policies and procedures

- **Large firms** were well used to assessing the money laundering risk in their business and responding appropriately. Nevertheless, at least two firms had undertaken a formal gap analysis, in order to see whether their existing AML policies and procedures broadly matched what the JMLSG Guidance recommended.
- As a result, very little had needed to be changed, though one firm commented that a side effect was to formalise the decision making in its main AML committee.
- Only two **medium-sized** firms said that they had not implemented any changes as a result of the 2006 JMLSG Guidance.
- Most of the remaining firms had carried out a gap analysis of existing policies and procedures against those outlined in the JMLSG Guidance. In response, changes had been made in client take-on, client monitoring, AML staff awareness and training and senior management reporting.
- Two **small firms** used external consultants to carry out an AML review. Not all firms said they would carry out further reviews of policies and procedures in the future to ensure they were still suitable for their business.

- We encountered only one small firm which was unaware that the Money Laundering Sourcebook had been removed and revised JMLSG Guidance had been published. All other small firms said they had integrated AML measures into their overall policies and procedures and made appropriate changes.

Customer due diligence

- **Large retail banks**, in particular, had specifically reviewed the risk of moving to a single official document to verify identity, bearing in mind the overall financial crime risk of doing so, but had not all come to the same conclusion.
- In one case, the firm had decided to continue requiring two pieces of identification evidence, partly on anti-fraud grounds and partly to allow for later cross-selling of products and services to customers without having to revert to customers for additional identification evidence.
- Another retail bank, however, had reviewed the fraud risk across its various business lines and decided to move to a single official document, while increasing its risk-based sampling to mitigate the possibility of enhanced fraud risk.
- This bank estimated that the 'opportunity gain' from moving to requiring a single piece of identification evidence from prospective customers amounted to £10mn per annum, enabling the bank to redeploy staff elsewhere, notably, to transaction monitoring in commercial banking.
- For **medium-sized and small firms**, the flexibility to accept one piece of identification evidence was much less of an issue. Generally, such firms continued to seek two pieces of identification from prospective customers.
- We found that the revised JMLSG Guidance had not directly affected the provision of financial services to the 'financially excluded'.
- Typically, providers of 'basic bank accounts' had procedures in place for any prospective customer who had difficulty with producing the most common forms of identification evidence. An exception process was thereby triggered and the account opener would refer to much more extensive lists of documents that were considered acceptable in exceptional circumstances. These lists would normally encompass the vast majority of situations.

Enhanced due diligence

- All the **large firms** carried out enhanced due diligence (EDD) measures on clients which they viewed as posing higher risk. A range of approaches was adopted and numerous triggers for EDD measures were in place, including in relation to Politically Exposed Persons (PEPs).

- For most **medium-sized firms**, EDD was triggered by geographic location of the client or by product type. Some firms had dedicated teams to carry out EDD measures but, for most, it was an integral part of the client take-on process. PEP and sanctions screening tended to be undertaken manually, because the likelihood of taking on a PEP or sanctioned person as a client was considered too low to justify investing in an automated checking system.
- Where **small firms** were concerned, the trigger for EDD measures was predominantly the client's geographic location. Not all the small firms we interviewed carried out regular PEP or sanctions screening across their client base – mainly because, in their view, it was most unlikely that any of their clients would feature.

Correspondent banking

- All the large banks that provided relevant services took the process of risk rating prospective respondents very seriously. Such clients typically first approached the correspondent via a relationship manager.
- The assignment of risk ratings typically had several implications. First, it drove the way the respondent's account was managed for AML purposes, in that higher risk accounts might have to be approved at a higher level. Second, it also determined the frequency of review. Third, the risk rating might also feed into a firm's automated transaction monitoring software, so as to determine the status of an alert. The higher the status of an alert, the more urgently it was reviewed.

Monitoring customer activity

- Most of the **large firms** operated automated transaction monitoring systems, of varying degrees of sophistication, though one firm had not yet fully implemented the system. The software used either rules or profiling methods or a combination of both to identify possible suspicious activity and generate alerts. Firms' experiences with automated systems varied considerably.
- A small number of large firms continued to rely on producing a suite of exceptions reports, typically for transactions exceeding a specified threshold (limits ranged from £3,000 - £9,000), to monitor the activities of their customers.
- Most **medium-sized firms** conducted client monitoring by manually checking database interrogation reports, which were produced using sets of rules deemed appropriate to the business. Only two firms were considering moving towards a fully automated transaction monitoring system.
- None of the **small firms** used automated transaction monitoring systems. Some MLROs relied on weekly or monthly print-outs of client activity, which they manually checked, whereas other MLROs quality assured a percentage of new business taken on by each consultant (usually 10%).

Staff awareness and training

- Most **large firms** used computer based training (CBT) packages to train staff in AML and other financial crime topics, with refresher training having to be undertaken annually.
- In addition to CBT, many firms provided specific training sessions for staff working in certain roles or business areas. These sessions might be face-to-face presentations or video/DVDs which staff were required to watch.
- Most **medium-sized firms** used a CBT package for AML training. However, only two used this as the sole means of training staff.
- Other training methods included:
  - tailored paper-based workbooks, produced by the local training and development team;
  - ad-hoc training sessions, requiring staff to have completed special reading packs and to pass a test;
  - scenario-based training sessions;
  - team exercises included in weekly staff meetings; and
  - training videos.
- Half of the medium-sized firms conducted annual AML refresher training. The rest either conducted biennial refresher training or had no documented procedures for refresher training.
- We found that most **small firms** did not use CBT packages to train their staff on AML, preferring the MLRO to deliver in-house training face to face. Consultants were also used more often in smaller firms, to deliver refresher presentations: however, tests did not commonly form part of this training. We note that, where staff understanding has not been tested, it is hard for firms to judge how well the relevant training has been absorbed.
- Refresher training in small firms was generally conducted every one to two years. Wholesale small firms, however, were an exception, with most having no comprehensive AML training or refresher policies.

Findings

Money laundering risk assessment

1. The high-level requirement in SYSC is that a firm must ensure that it has in place systems and controls that (i) enable it to identify, assess, monitor and manage money laundering risk; and (ii) are comprehensive and proportionate to the nature, scale and complexity of its activities. The JMLSG Guidance makes clear that such risk may arise from customers' behaviour; from the nature of the relationship and the delivery channel; and from the products and services provided by the firm. Necessary controls to manage and mitigate money laundering risk include appropriate customer due diligence procedures and monitoring of customers' activity. The effective operation of these controls should be kept under regular review, which is also a SYSC obligation.

2. We found that most **large firms** had undertaken a formal money laundering risk assessment. The Money Laundering Reporting Officers (MLROs) in these firms had also documented the risks posed by their customers and products/business lines. Two of the large firms visited had commissioned consultants to carry out a further review of their AML policies and procedures and/or to quality assure the money laundering risk assessment and mitigation measures used by the MLRO.

3. Some large firms produced risk matrices or scoring systems for their client profiles, products, delivery channels and the geographical location of their customers, with each profile attracting a similar priority. Other firms weighted their assessments towards one of these risk factors.

4. Risk scoring information was typically fed into a risk matrix that staff were required to use when taking on new clients and would determine what level of Know Your Customer (KYC) information was required for taking on that client. Higher risks were usually mitigated by requesting additional KYC information with emphasis on identification of the source of funds or by conducting additional client monitoring. Some large firms assigned high risk clients to a relationship manager who would oversee all business conducted with that client.

5. We noted that an MLRO working for a large investment bank had recently created a higher risk category. As the bank had 3,500 high-risk clients globally, he created an additional group for the top 100 highest risk clients. Where two or more negative factors applied to a client, he identified that client as potential higher risk and he or his deputy reviewed activities on the client's account every month. In such cases, unless the issue was serious enough to prevent client take-on, the Compliance Team would review any available press information about the client and conduct ongoing transaction monitoring. (This was in addition to the normal automated transaction monitoring.) The

approach to these higher risk cases was seen as an evolving process and the MLRO was mindful that his list of the top 100 riskiest clients must not grow beyond a manageable number.

6. Many firms had not actually considered how often their risk assessment would be reviewed. Some said that it was a continual process; others said that it would happen as and when new products were launched. Some intended to review their money laundering risk profile annually; and others said it would be a one-off exercise or had not considered it at all.

Example of good practice

One large firm's procedures required it to undertake periodic KYC/Customer Due Diligence reviews of existing clients. The depth of the review is determined by the risk ranking assigned to the client. Clients rated A and B are reviewed every three years; Cs every two years; and Ds and Es are reviewed annually. For lower risk (A-C) clients, the review may amount to no more than refreshing the client's file to take account of: significant changes in ownership or capitalisation; changes in the client's line of business; addition of a Politically Exposed Person (PEP) to shareholders or senior management; or any negative news on the client's owners or senior managers. For high risk (D or E) clients, visits to the client are necessary to provide an extra layer of comfort. Such visits would typically cover: review of client's client take-on procedures; sample testing of KYC documentation on underlying clients; and obtaining answers to outstanding queries on, eg, annual AML certification, transaction queries, and potential PEP or sanctions hits.

7. We found that most **medium-sized firms** had assessed the risks in their business. But these assessments varied greatly. In one case, the firm had conducted formal risk assessments of each area of business, considering: client type; product type; delivery channels; and geographical location, leading to the production of a risk matrix and implementation programme, that was constantly reviewed and overseen by a management committee. In other cases, firms had undertaken a simple assessment based on client type, in one case formulated using a standard AML tool produced by a consultancy.

8. Where medium-sized firms had not conducted a formal risk review, they were also generally more concerned about fraud risk to the business than the risk of the firm being used as a vehicle for money launderers, although they recognised that this posed a risk of reputational damage. The most common factor attracting a high-risk rating in medium-sized firms was non-face-to-face business. The factors which most commonly attracted a low risk rating were UK-based clients taking out long-term investment products.

9. We found that, where extensive analysis had taken place in medium-sized firms, this had led to more changes in AML policies and procedures. Firms believed that these changes had reduced the burden on clients but the process had often been expensive. In these cases, firms expected the benefits to derive from gaining a level of assurance that, as

resources were now targeted to areas of higher risk, the firm as a whole was at less risk from fraud or reputational damage.

10. One mortgage broker said the move to the risk-based approach had made their business more difficult as lenders had all conducted individual risk assessments of their business, clients and products, resulting in a wide range of different risk levels, with some lenders even classifying all mortgages as low risk. This broker now required a number of different KYC documents from customers at the outset of the business relationship. The aim was to meet the differing requirements of lenders, as customers sometimes needed to move their business to another lender and, in these cases, the broker believed it would be unreasonable to return to the customer to ask for more documents verifying their identity.

Example of good practice

One building society undertook a comprehensive policy review following the publication of the 2006 JMLSG guidance, in order to identify which parts of the business were affected and what action was needed. It identified eight core business areas, which represented the key operational areas exposed to risk from money laundering. These business areas were ranked in order of risk and formed into work streams. The local managers from each workstream business area were then trained by the Compliance Policy Team, using a series of presentations and individual workshops, to understand the impact of the risk-based approach, their individual responsibilities and the appropriate customer due diligence policies. These managers were then required to apply this awareness and their existing knowledge of their workstreams' business activities to create documented risk profiles covering customers, products, delivery channels and geography. The risk profiles were graded as Red, Amber and Green and customer due diligence and monitoring requirements set at appropriate levels.

11. Most of the **small firms** we interviewed had carried out some kind of risk assessment, following the introduction of the 2006 JMLSG Guidance. Three of the firms used consultants to assist. Some firms said they would re-assess their AML risk review annually; others said this would be done periodically.

12. Risk assessments were generally based on a range of criteria, including: client profiles; geographic location of the client; product profile; delivery channel and one firm also mentioned staff. One firm saw the main risk of money laundering as being at the 'integration' stage because much of the money invested was received from other financial institutions. The firms generally carried out high levels of due diligence to establish clients' source of wealth to help mitigate this risk.

13. The majority of firms we interviewed classified the risk of money laundering across their businesses as low, although some identified certain products or client types as higher risk. Examples quoted to us included trusts, non-UK clients, SIPPS, SAPs and derivatives.

14. Reasons cited by small firms for a low risk classification included: firms were dealing with money that was already in the system; firms offered discretionary services; there was low portfolio turnover; clients were predominantly UK based; business was introduced by lawyers and accountants; and no 'new money' was introduced to the business.

Example of poor practice

Some firms did not have a robust approach to classifying the money laundering risk associated with their clients. For example, one wholesale small firm classified all its clients as low or medium risk, despite the fact that most of them were based in Eastern Europe, North Africa and the Middle East. Another firm's risk-assessment procedures provided that the Compliance Officer or MLRO would determine the risk category for each client and would record the basis of the assessment for each client. However, a file review showed no evidence that risk assessments had actually been carried out.

15. We were told that the risk of traded products (higher risk) being used for money laundering depended on the nature of the client, the market participants, the product involved and whether the products were traded on an exchange or 'over the counter' (OTC). One equity derivatives broker said that audit trails were relatively easy to obscure in derivatives markets, which could make these markets more attractive for money laundering. So when dealing with OTC business, the firm recognised it must carry out a more detailed risk assessment.

Senior management responsibility

16. There are two main provisions in SYSC that relate directly to senior management responsibility. The first is that a firm must allocate to a director or senior manager (who may be the MLRO) overall responsibility within the firm for the establishment and maintenance of effective AML systems and controls. Second, such systems and controls must include appropriate provision of information to the firm's governing body and senior management, including a report at least annually by the firm's MLRO on the operation and effectiveness of those systems and controls.

17. In **large firms**, we found that relatively few changes had been prompted by the new SYSC provisions. Typically, formal senior management responsibility for AML controls was held at a sufficiently senior level already, for example, by the Chief Risk Director, Chief Security Officer, Chief Operating Officer or Director of Compliance. These senior managers sometimes held the title of MLRO as well, but delegated day-to-day responsibility for AML controls to their deputy, who usually acted also as the nominated officer responsible for making disclosures of suspicious activity to SOCA under the Money Laundering Regulations 2003 and the Proceeds of Crime Act 2002. Where the MLRO himself was directly engaged in day-to-day AML issues, we found that it was generally not considered necessary to appoint anyone above him with overarching

responsibility for the AML control environment. The key consideration was that the MLRO had sufficient influence within the firm to persuade executive business management to implement, and maintain, adequate AML measures, as and when necessary. That influence might derive either from the MLRO's own seniority within the firm or from his direct reporting line to the chief executive or to another member of the firm's senior management with a seat on the Board or a key Board Committee.

18. We found a good level of communication and interaction, both formal and informal, between MLROs and their line managers, where money laundering issues had arisen. The same was broadly true in UK firms with head offices abroad, and a global head of AML based outside the UK. Within the UK, a broadly common approach was for the MLRO to produce a monthly report to the Compliance Director, covering, amongst other things, major fraud or money laundering incidents or cases; the status of AML related projects; and the status of action taken in response to recommendations raised in the previous year's MLRO annual report to the Board. The monthly report focused on issues, next steps and achievements. The Compliance Director used this information to provide a summary for the Executive Committee of the firm, on a monthly basis. Externally, the firm's UK Compliance Director provided a copy of the report prepared for the formal Executive Committee to the Compliance Managing Director of the US parent company. In addition, each month, the Compliance Director and CEO of the UK firm held a conference call with their opposite numbers in the US parent company to discuss significant compliance, including AML, issues in the UK firm.

19. Management information (MI) on AML issues was often communicated up to the Board via the Audit Committee or Group Risk Committee. In one case, we were told that the Board received the minutes of all Audit Committee meetings, as well as an oral report from the Chair of the Audit Committee on any issues of which the Board should be made aware. This ensured that the Board was kept up to date with any significant AML issues in between receiving, and discussing, the MLRO's annual report.

Example of good practice

In response to the SYSC changes, one major bank decided to appoint the MLRO's line manager as the designated director with overarching responsibility for AML controls. This director was seen as the obvious choice for the role, given that his portfolio of responsibilities included fraud, risk and money laundering. The bank's decision formally to appoint a Board level senior manager to this position was viewed as reinforcing the importance of having in place a robust AML control framework.

Following his appointment, the director decided that the management information (MI) on AML issues he had hitherto received was too ad hoc and fragmented. So the SYSC/JMLSG changes proved to be a catalyst for the bank establishing more organised MI and a Group-level Financial Risk Committee to consider relevant issues. (In the past, various Risk Committees had considered such issues.) The new Committee's remit covered fraud, money laundering and sanctions issues; however, its primary focus was AML.

20. Within **medium-sized firms**, AML risk tended to be viewed in the same way as any other risk to the business and CEOs were generally committed to ensuring that AML controls were given adequate attention. Overarching responsibility for AML was seen by some CEOs as their responsibility, although in many firms the day-to-day responsibilities were delegated. Often, the MLRO reported directly to, or had regular meetings with, the CEO. Generally, we found that MLROs had the necessary seniority to implement appropriate changes and many had dedicated AML resource available to them if required: for example, some had appointed a deputy MLRO to oversee key controls such as monitoring and staff training.

21. MLROs were generally senior managers with compliance and oversight responsibilities and, in some firms, were also the Nominated Officer. Where MLROs had multiple roles (Management, Company Secretary, Compliance, CEO), with few exceptions, they were able to devote sufficient time to AML.

22. We found that MI was prepared for Board meetings and various committees by most firms to keep senior management informed of AML issues. AML was often a standing item on Board meeting agendas or featured regularly on executive management meeting agendas. MLRO Annual Reports were adequately detailed and described how firms measured the success of their AML policies and procedures.

23. Most of the **small firms** we interviewed had appointed a senior manager to oversee AML controls, in addition to an MLRO. In the majority of firms, AML issues were discussed regularly with senior management, either informally or at Board meetings, or were communicated upwards as regular MI.

Example of poor practice

Some small firms had produced inadequate annual MLRO reports, which failed to demonstrate to their governing body and senior management that the firms' AML systems and controls were operating effectively. In one case, the MLRO stated categorically that there had been no perceived deficiencies in the suspicious activity reporting process. However, he was unable even to describe that process to us, so it was highly unlikely that he had ever reviewed the SAR process for possible deficiencies.

24. All but one of the firms we interviewed produced an annual MLRO Report. MLROs took responsibility for implementing recommendations from the report and, in some cases, this was monitored by the Board or senior executive management. MLROs were generally able to report directly to the Board.

25. We found that all MLROs had some previous financial services experience but not all had specific AML training and experience. Most of the small firms had not appointed a deputy MLRO, because the size and nature of the firm did not justify it.

Example of poor practice

In one small firm, the MLRO was clearly not fully engaged in his role. For example, he was unaware that we had removed the Money Laundering Sourcebook and he was still using an outdated (2003) edition of the JMLSG Guidance. It was not entirely clear whether this arose from a lack of interest in his MLRO function or from inadequate compliance resources at the firm, which left him with insufficient time to keep up to date with AML matters, or a combination of both.

Changes to AML policies and procedures

26. A common response from the **large firms** was that the introduction of high-level SYSC rules had caused them no difficulty, not least because several firms were closely involved in developing the JMLSG Guidance on implementing a risk-based approach to AML controls. These firms argued that they had never applied FSA rules and the JMLSG Guidance slavishly – 'we live and breathe our AML policy', said one MLRO – and were well used to assessing the money laundering risk in the business and responding appropriately. Nevertheless, at least two firms had undertaken a formal gap analysis, in order to see whether their existing AML policies and procedures broadly matched what the JMLSG Guidance recommended. As a result, very little had needed to be changed, though one firm commented that a side effect was to formalise the decision making in its main AML committee. Furthermore, the same firm had also decided that, whereas previously a paper outlining the firm's risk-based approach would have only needed approval at Group MLRO level, it was now considered desirable to obtain the necessary endorsement at executive director level. Another firm said that there had been no step change in its approach, because AML measures – to be effective – must constantly evolve, but the risk-based approach was now better documented. In particular, the client risk assessment was now conducted at an earlier stage and there was a written record of processes followed and decisions made.

27. In contrast, one major firm had introduced a number of changes following the revision of the JMLSG Guidance. These changes included: combining its AML and anti-fraud polices; placing increased reliance on financial advisers to verify the identity of new clients on the firm's behalf; reinforcing the importance of AML as a business risk; implementing a new business escalation procedure; enhanced monitoring of higher risk transactions; and introducing risk-based AML training of staff.

28. In another case, the firm had decided to divide its client procedures manual into three sections to reflect the risk in each business area. Client identification checks were identical for each business but specific risks in each line of business were picked out and appropriate controls introduced. So, for example, in private wealth management, emphasis was placed on checking both source of funds and source of wealth during the early stages of client take-on.

29. More generally, one firm told us that, while it believed it had a well balanced approach to AML, the firm had benefited considerably from discussing AML issues widely, not only within its own organisation but also with others from across the industry. Other firms, with different products and customer bases, would not necessarily follow the same approach to AML. However, it had proved useful to exchange ideas via discussions with the British Bankers Association, Building Societies Association and various MLRO groups.

30. Only two **medium-sized firms** said that they had not implemented any changes as a result of the 2006 JMLSG Guidance. One firm told us it would engage a consultant to review its AML policies and procedures to ensure best practice was embedded in the firm. The other firm stated that its existing policies and procedures were appropriate and that AML procedures were embedded in its existing client take-on questionnaire.

31. Most of the remaining firms had carried out a gap analysis of existing policies and procedures against those outlined in the JMLSG Guidance. In response, changes had been made in client take-on, client monitoring, AML awareness and training and senior management reporting.

32. Those firms that had carried out a formal risk assessment identified a range of factors that would influence KYC and client take-on. These included client type; jurisdiction in which the client or intermediary was based; fund distribution channels and whether or not the business was single-premium only.

33. Three of the **small firms** interviewed said that they made no changes to their AML policies and procedures as a result of the 2006 JMLSG Guidance but they did use the Guidance as a point of reference. Using a risk based approach, they determined that their existing policies and procedures were appropriate to the size and nature of their businesses.

34. Two small firms used external consultants to carry out an AML review. Not all firms said they would carry out further reviews of policies and procedures in the future to ensure they were still suitable for their business.

35. We encountered only one firm which was unaware that the Money Laundering Sourcebook had been removed and that revised JMLSG Guidance had been published. All other small firms said that AML measures had been integrated into their overall policies and procedures and appropriate changes made.

36. Changes implemented by small firms included: the introduction of a more formal approach to assessing client risk, which covered recording source of funds and source of wealth; relaxing client identification requirements, depending on the size of the initial investment; and accepting certified copies of valid identification evidence where previously the firm would only accept original documents.

Customer due diligence

37. While the new high level AML requirements in SYSC did not materially affect firms' customer due diligence (CDD) procedures, the revised JMLSG Guidance introduced some changes to, and amplification of, previous guidance to the industry. The key change concerned a move away from firms needing to check both the name and address of individual customers towards checking one Government-issued document bearing a photograph of the customer and either the customer's address or their date of birth. Furthermore, the Guidance continued to include provisions relating to both simplified and enhanced due diligence. So, on the one hand, firms should still maintain systems for dealing with 'financially excluded' customers or those who could not be expected to produce standard evidence of their identity. On the other hand, where higher risk customers or delivery channels were concerned, firms should have enhanced due diligence processes in place, eg, to cover Politically Exposed Persons (PEPs) and correspondent banking.

38. We found that **large retail banks**, in particular, had specifically reviewed the risk of moving to a single official document to verify identity, bearing in mind the overall financial crime risk of doing so, but had not all come to the same conclusion. In one case, the firm, following lengthy internal debates, had decided to retain its requirement to obtain two pieces of identification evidence. However, at the same time, the firm would make clear to customers in its marketing literature that the second piece of evidence was needed for anti-fraud purposes. Another important consideration was the firm's cross-selling of products and services to existing customers. If the firm took adequate steps to ensure that it had obtained all necessary identification evidence at the outset of the customer relationship, then if the customer later applied for an additional product or service, it would not be necessary to undertake additional identification measures. This decision by the firm had not caused any adverse feedback from prospective customers, who generally still expected to have to produce two pieces of identification evidence.

39. Another retail bank, however, had decided to move to a single official document to verify identity, subject to appropriate fraud and risk mitigation. Research carried out by the bank's money laundering team with their anti-fraud counterparts, across both the retail and wholesale business, indicated that there was unlikely to be increased fraud risk. Accordingly, with the agreement of risk officers in individual business units, the bank had documented what it considered an acceptable list of official documents in most cases (passport, EU identity card and photo driving licence, mainly). However, prospective customers from higher risk jurisdictions would continue to be required to produce two pieces of original identification evidence.

40. At the same time, additional risk-based sampling was introduced to mitigate possibly enhanced fraud risk. This sampling was targeted at areas considered most at risk, eg, high risk jurisdictions, post codes and branches that had proved particularly susceptible to fraud and any areas of business that exhibited lower than expected pass rates for account opening. The bank told us that it had derived a number of benefits from these changes. First, it was easier for customers to do business with the bank, removing identity verification as a potential barrier to business. Second, it helped the bank's 'Treating Customers Fairly' agenda. Third, the account opening process was made both faster and easier. And, fourth, the bank's retail and wholesale processes were better aligned, making it easier to transfer data. Furthermore, there had been no material changes in the number of fraud incidents.

41. This bank estimated that the 'opportunity gain' from moving to requiring a single piece of identification evidence from prospective customers amounted to £10mn a year, enabling the bank to redeploy staff elsewhere, notably, to transaction monitoring in commercial banking.

42. For **medium-sized and small firms**, the flexibility to accept one piece of identification evidence was much less of an issue. Generally, we found that such firms continued to seek two original, or appropriately certified, pieces of identification from prospective customers. In most cases, this comprised a valid passport, photo driving licence or national identity card, together with a recent utility bill or bank statement. Often, these firms accepted business from introducers, including accountants, solicitors and other regulated financial institutions, brokers or independent financial advisers. However, in most cases, medium-sized and small firms did not rely solely on the introducer to carry out CDD measures. Where, for example, higher value investment business was involved, client review meetings were held. In most firms, at least one meeting with a prospective client would be arranged, although for more complex products, three or four meetings might be required.

Example of poor practice

We found some cases of medium-sized and smaller firms documenting their client take-on procedures but not regularly updating those procedures and not always following them. For example, one firm told us that CDD information on clients was refreshed every time clients applied for a new product or service. However, a file review showed no evidence that this had been done.

43. We found that the revised JMLSG Guidance had not directly affected the provision of financial services to the 'financially excluded'. This was probably, so we were told, because the Banking Code Standards Board reviewed the provision of so-called 'basic bank accounts' annually, reporting its findings to the Treasury Select Committee and giving feedback to individual providers. That report included results from mystery shoppers, general industry findings and individual firm findings.

44. Typically, providers of basic bank accounts had procedures in place for any prospective customer who had difficulty with producing the most common forms of identification evidence. An exception process was thereby triggered and the account opener would refer to much more extensive lists of documents that were considered acceptable in exceptional circumstances. These lists would normally encompass the vast majority of situations. If not, however, the providers all allowed the customer to apply for a waiver, under which their case would be reviewed in the light of their particular circumstances. As a result, it was quite rare for a customer to be refused an account, unless they were a bankrupt or had a fraud history.

45. We noted that opinions differed between providers on whether basic bank accounts were higher risk accounts, through being predominantly cash based. One bank told us that it had not experienced a higher level of criminality with such accounts and regarded accounts offering credit as much more likely to be targeted by criminals. Another bank, however, had experienced a high incidence of false passports being used by basic bank account applicants. It had also found these accounts being used to receive fraudulent benefit payments.

Enhanced due diligence

46. All the **large firms** carried out enhanced due diligence (EDD) measures on clients which they viewed as posing higher risk. A range of approaches was adopted and triggers for EDD included: location of client in high risk jurisdiction; PEPs; offshore trusts; special purpose vehicles; international business companies established in locations with lax money laundering legislation, bank secrecy or confidentiality rules; private or public companies with bearer share ownership; money service businesses; gaming entities; and customers with multiple account relationships across a number of jurisdictions. Where such relationships were concerned, firms would typically undertake more rigorous validation of identity, particularly in relation to beneficial ownership, and checking of both source of funds and source of wealth, as well as requiring senior management sign-off at the outset of the business relationship. After that, activity over the accounts of these higher risk customers would be subject to more frequent scrutiny and information held by the firm on the customer would be refreshed at regular intervals.

47. Many of the firms used proprietary automated systems to check whether prospective customers might be PEPs or feature on sanctions lists. These checks would often be made not only on the customer but also on whether the customer was owned or controlled by a PEP or sanctioned person or entity. One international bank told us that it always erred on the side of caution, eg, even in relation to a PEP who was involved with a corporate customer but who had no controlling interest in the company. This could present problems in certain countries in the Far East, for example, where every company of any size had a PEP on its Board.

48. One major retail firm told us that it had decided not to carry out EDD or enhanced monitoring on any of its domestic PEPs, taking the view that it was sufficient to know

who they were. The firm perceived them to be no higher risk customers than any other; nevertheless, it had the ability to 'close monitor' account activity on any individual PEP through its automated transaction monitoring system. The same firm added that it would, in due course, formally document its PEP policy and procedures but, at the time of our visit, the firm was waiting to see the final text of the 2007 Money Laundering Regulations before doing so.

49. For most of the **medium-sized firms**, EDD was triggered by geographic location of the client or by product type. Some firms had dedicated teams to carry out EDD measures but, for most, it was an integral part of the client take-on process. PEP and sanctions screening tended to be undertaken manually, because the risk of taking on a PEP or sanctioned person as a client was considered too low to justify the considerable cost of investing in an automated checking system.

50. Generally, EDD also entailed closer transaction monitoring. Most of these firms were able to say whether or not they had a PEP on their books and one firm even had a fully documented PEP policy. Some firms required management sign-off before taking on any PEP business or opening an account for a client with any link to a PEP.

51. Where **small firms** were concerned, the trigger for EDD measures was predominantly the client's geographic location. Not all the small firms we interviewed carried out regular PEP or sanctions screening across their client base, mainly because, in their view, it was most unlikely that any of their clients would feature. For example, financial planning for families enabled a great deal of information to be gathered over the course of the client take-on process, so there was perceived to be no need for further EDD measures. Other small firms undertook manual checks for PEPs and sanctions 'hits', while other firms only made these checks at the client take-on stage.

Example of poor practice

A number of medium-sized and small firms were unaware that it was illegal for them to deal with individuals or entities named on the Treasury's Financial Sanctions list. As a result, no screening of clients or transactions was being undertaken against that list. One firm said that it did not routinely check the Financial Sanctions list, because it did not deal with the type of client which might appear on the list.

Correspondent banking

52. The JMLSG Guidance states that correspondents should undertake an appropriate degree of customer due diligence on their respondents, using a risk-based approach. Various risk indicators should be taken into account, including the respondent's domicile; ownership and management structures; business and customer base; and the extent to which the respondent itself provides correspondent banking services to other

banks. Where enhanced due diligence measures are considered necessary, the correspondent should review the respondent's ownership and management; PEP involvement; and AML/CTF controls. Monitoring of respondents' activity should be undertaken, as should any change in the respondent's nature and status.

53. We found that all the large banks in our sample that provided relevant services took risk rating prospective respondents very seriously. Such clients typically first approached the correspondent via a relationship manager. This might arise from the correspondent targeting a particular country for new business or it might simply stem from an exchange of SWIFT test keys or a request for a foreign exchange limit. The risk rating process differed slightly between correspondents. In one case, the first step was to assess the respondent from publicly available sources of information and then set a level 1, 2 or 3 rating. That rating then determined the amount of documentation required by the correspondent. In contrast, the approach adopted by another correspondent was to complete a standard series of due diligence checks and then risk rate the respondent at the end of that process, on a case-by-case basis.

54. The assignment of risk ratings typically had a number of implications. First, it drove the way the respondent's account was managed for AML purposes, in that higher risk accounts might have to be approved at a higher level. Second, it also determined the frequency of review. A common approach was to review higher risk client relationships at least annually (a 'trigger event' could prompt an intra-year review), whereas there might be no fixed period for reviewing low risk relationships. Third, the risk rating might also feed into a firm's automated transaction monitoring software, so as to determine the status of an alert. The higher the status of an alert, the more urgently it was reviewed.

55. We found that correspondents attached considerable importance to collecting information on expected volumes and values for any new respondent account, albeit that respondents often had great difficulty in predicting what their activity levels might be. (A sudden one-off payment of $300mn would not be unusual.) Such information was necessary for both AML/CTF and business reasons. Any unexpected spikes in activity needed to be reviewed to decide whether a suspicious activity report was appropriate. At the same time, a lot of unexpected payments by the respondent might provide the correspondent with a marketing opportunity.

Monitoring customer activity

56. The high-level SYSC rules do not specifically cover monitoring of customer activity. However, the revised JMLSG Guidance, while pointing out that there is no legal or regulatory requirement to monitor, states that internal control and Proceeds of Crime Act 2002 requirements on reporting suspicious activity make an appropriate degree of monitoring desirable. There is no presumption in the Guidance about whether such monitoring should be manual or automated. Furthermore, by whatever means monitoring is undertaken, it is no substitute for ongoing staff alertness to possible suspicious activity.

57. Most of the **large firms** we visited had in place automated transaction monitoring systems, of varying degrees of sophistication, though one firm had not yet fully implemented the system. The software used either rules or profiling methods or a combination of both to identify possible suspicious activity and generate alerts. These firms' experiences with automated systems varied considerably. A common view was that the most successful automated systems to date had been developed for retail banking and nothing comparably effective was yet available for investment banking. On the one hand, firms which had operated automated systems for retail banking for a number of years reported the greatest success. But on the other hand, a foreign bank which had operated the same software for less than a year was still suffering teething troubles, with new transaction codes causing the system to crash and foreign exchange amounts being calculated incorrectly. As a result, the bank was having to run rules-based monitoring alongside the new system, when it should have been possible to switch off the rules-based monitoring.

58. A small number of large firms continued to rely on producing a suite of exceptions reports, typically for transactions exceeding a specified threshold (limits ranged from £3,000 - £9,000), to monitor the activities of their customers.

59. Most **medium-sized firms** conducted client monitoring by manually checking database interrogation reports, which were produced using sets of rules appropriate to the business. Only two firms in our sample were considering moving towards a fully automated transaction monitoring system.

60. In most cases, manual checking was conducted by the Compliance team or MLRO once a month. The rules-based reports covered suspicious activity typologies, such as cancellations and early redemptions, change of customer details, such as name and/or address or the transfer of an investment to another beneficiary.

61. Some medium-sized firms also checked payments or claims against previous activity undertaken by the client and some reviewed all client files periodically (twice a year in one case). Most medium-sized firms also had systems in place to freeze or apply restrictions to accounts on which there had been no activity for over one year.

62. Some medium-sized firms outsourced the administration of their products and, in these cases, they relied on the custodians (who were also regulated entities) to conduct client activity monitoring on their behalf.

63. None of the **small firms** in our sample used automated transaction monitoring systems. Some MLROs relied on weekly or monthly print-outs of client activity, which they manually checked, whereas other MLROs quality assured a percentage of new business taken on by each consultant (usually 10%).

64. Firms undertaking discretionary portfolio management usually monitored client activity by ensuring that each client was relationship managed by a single consultant. A number of small firms commented that the client relationship could also be monitored through regular meetings – or home visits – between the consultant and client.

Staff awareness and training

65. The high-level provision in SYSC is simply that a firm's AML systems and controls should include appropriate training for its employees in relation to money laundering. The JMLSG Guidance states that firms should consider providing case studies and examples that are relevant to a firm's business. Firms should also train their employees in how to operate a risk based approach.

66. Most **large firms** used some sort of computer based training (CBT) package to train staff in AML and other financial crime topics, with refresher training having to be undertaken annually. The standard CBT packages included a test which staff were required to pass and the questions or topics covered could also be tailored to suit the business.

67. In addition to this, many firms provided specific training sessions for staff working in certain roles or business areas. These sessions might be face-to-face presentations or video/DVDs which staff were required to watch. Some firms offering specialised or tailored training sessions had organised these by classifying staff roles as high, medium and low risk in terms of potential exposure to financial crime. This was based on factors relating to the level of contact the staff members had with customers or those who handled client data.

68. Some firms had not communicated the introduction of the new JMLSG Guidance to staff, as it had resulted in little change to their procedures. Other large firms regularly produced AML bulletins or newsletters aimed at key members of staff or business units who had a particular interest in anti-financial crime systems and controls.

Example of good practice

One large bank judged that staff AML training and awareness were suitable for the development of a risk-based approach. It saw a need to differentiate between AML requirements in various business units, so that training could be adapted to the needs of the job. So in Retail, training had been re-designed to produce a more balanced package. Accordingly, staff were required to undertake one training module per quarter, with the emphasis on a different area in each module and a test taken every quarter. The aim was to see what impact this constant 'drip feed' of training had on suspicious activity reporting. At the time of our visit, this bank was also in the throes of merging its anti-fraud and AML training. The overall objective was to make it more difficult for criminals to do business with the bank undetected.

69. Most of the **medium-sized firms** visited used a CBT package for AML training. However, only two used this as the sole means of training staff.

70. Where CBT packages were used, staff needed to pass a test at the end of the course, usually requiring a 75-80% pass mark. Some tests also required a pass mark of at least 70% for each section.

71. Other training methods included: tailored paper-based workbooks, produced by the local training and development team; ad-hoc training sessions, requiring staff to have completed special reading packs and to pass a test; scenario-based training sessions; team exercises included in weekly staff meetings; and training videos.

72. Half of the medium-sized firms visited conducted annual AML refresher training. The other firms either conducted biennial refresher training or had no documented procedures for refresher training. Where there were no documented procedures, this was attributed to existing training policies being revised or because refresher training was conducted on an ad-hoc basis.

73. Communication to staff working in medium-sized firms mainly took the form of e-mails. However, some companies communicated changes in AML policy or procedure to business unit managers who were then responsible for disseminating the information to their staff.

74. We found that most **small firms** did not use CBT packages to train their staff on AML, preferring the MLRO to deliver in-house training face to face. Consultants were also used more often in smaller firms, to deliver refresher presentations: however, tests did not commonly form part of this training. We note that, where staff understanding has not been tested, it is hard for firms to judge how well the relevant training has been absorbed.

75. Most small firms had staff manuals covering both compliance and AML procedures. Staff were usually requested to sign a log to confirm they had read and understood the content of the manual.

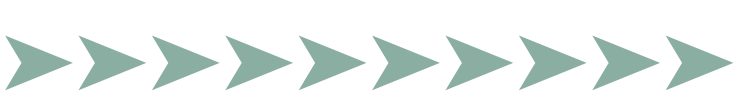
76. Refresher training in small firms was generally conducted every one to two years. Wholesale small firms, however, were an exception; most had no comprehensive AML training or refresher policies.

Example of poor practice

Some medium-sized and small firms admitted that staff AML training was an area where improvement was needed. One firm told us that training was delivered as part of an induction programme but not refreshed at regular intervals throughout the employee's career. Another firm said that it provided AML induction training only if a new joiner specifically requested it and no new employee had actually made such a request. The firm's MLRO took the view that most new employees came from the regulated sector, so should already be aware of their AML obligations. Such employees were merely required to sign a form to confirm that they were aware of the firm's AML procedures, but their understanding was never tested.

77. The MLROs in small firms generally used e-mail as a method of communicating regulatory or compliance related changes to staff. Several MLROs commented that staff communication was easy in a small firm, as all staff tended to be based in the same office.

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



FSA®