Financial Services Authority

Review of private banks' anti-money laundering systems and controls

July
2007

Contents

Introduction

1. This report is a summary of our review of anti-money laundering (AML) systems and controls at several FSA-regulated private banks during December and January 2007. The review covered these firms' relationships with all their customers, wherever they were located. It did not cover the private banking activities of overseas entities within the same groups. The review was commissioned by our Financial Crime Sector team in response to a report by our Intelligence team, which highlighted the money laundering risk within private banking and the need for us to enhance our understanding of the adequacy of AML controls in this sector.

2. As previous visits to private banks had been to follow-up on firm specific issues or as part of wider programmes of work, there was also a general recognition amongst those with financial crime responsibilities that a more focused thematic review would be the best way to assess risk and controls in this area.

3. Our work involved full or half day visits to interview Money Laundering Reporting Officers (MLROs) and other staff involved in AML, together with desk-based reviews of AML policies, procedures, management information, training material and recent Suspicious Activity Reports (SARs).

4. These firms were selected from a wider population of FSA-regulated private banks, through discussion with the individual firms' supervisors and taking into account any relevant supervisory or business issues. The sample of firms selected met our objective of covering a cross section of firms in terms of size, client base, products and services, corporate structure and risk profile. Our findings also reflect information obtained from a third party on AML systems and controls at another private bank.

5. The review focused on firms' policies and procedures for identifying, assessing, monitoring and managing money laundering risk. We looked, in particular, at the control environment relating to Politically Exposed Persons (PEPs) and high-risk clients in general, including customer due diligence and the identification of beneficial ownership. All of these are important features not only of the current AML statutory and regulatory regimes but also of the forthcoming EU Third Money Laundering Directive (3MLD) and the Financial Action Task Force's Forty Recommendations on Money Laundering.

6. In this report the term 'private banking' describes the provision of banking and investment services in a closely managed relationship to high net worth clients. Such services will include bespoke product features tailored to a client's particular needs and may be provided from a wide range of facilities available to the client. These include current account banking, high-value transactions, use of sophisticated products, non-

standard investment solutions, business conducted across different jurisdictions and offshore and overseas companies, trusts or personal investment vehicles.

7. Due to these characteristics, private banking, particularly international private banking, is vulnerable to money laundering. We recognise, however, that the private banking 'label' applies to a range of businesses with varying money laundering risk profiles. For example, the risk inherent in a private bank which operates a consistent business model serving UK resident clients, who have largely gained their wealth through inheritance, will be very different from one that operates in jurisdictions with weak money laundering controls where the origins of clients' wealth are difficult to verify.

8. The close relationship that private banks aim to have with their clients, and the bespoke requirements that many private banking clients have, should allow private banks to develop a very good understanding of their clients and the reasons for their clients' transaction activity. With this knowledge and given the risks inherent in the sector, we would expect AML systems and controls within private banks to be of a high standard and calibrated to reflect the specific money laundering risks that the business is exposed to.

9. 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 should you wish to provide us with comments please address them to:

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

Executive Summary

Money Laundering Risk

10. Firms are attracted to the private banking business because it offers potentially high returns through the provision of value added services. While these services are attractive to legitimate customers with substantial assets and relatively complex financial affairs, they often have characteristics that are attractive to criminals with significant funds to launder. The facilitation of cross-border transactions, expertise in offshore investment and associated services and a tradition of high quality, discrete customer service are examples of some aspects private banking which can lead to an inherently high level of money laundering risk within this business.

11. Within the sample of firms covered by our review, we in fact found that money laundering risk varied significantly. We consider this variation to be a reasonable reflection of the risk profile of the sector as a whole. Some firms operating at the lower end of the risk 'spectrum' had relatively enhanced AML systems and controls, which benefited like other private banks from their relationship managers' (RMs) knowledge of their clients, but the risk inherent in the business conducted by these firms was closer to that seen in a standard retail and investment businesses environment.

12. At the higher end of the risk spectrum, firms provided services to a more internationally diverse client base – some of whom were located in high-risk jurisdictions – through RMs based both in the UK and overseas. Clients of these firms were more likely to have non-standard financial requirements and manage their affairs through complex structures. The ratio of relationship managers to clients was another measure of risk, which ranged from 200 clients per relationship manager to less than 50.

13. We consider that the following factors, in particular, are likely to increase the risk of money laundering within private banking businesses:

    i. An international customer base which includes people or organisations from jurisdictions with:

        a. relatively weak legal structures and/or economies, from which residents are likely to 'shelter' funds overseas;

        b. a reputation for providing secretive or discrete company and trust formation and administration services; and

        c. a poor record on the implementation of measures to prevent and enforce against financial crime, including corruption.

ii. A failure by private banks' senior management to communicate and enforce high ethical standards, particularly in relation to financial crime, within the business.

iii. A failure to obtain sufficiently detailed, accurate or up-to-date customer information, or review this at an appropriately senior and independent (from relationship managers) level within the organisation.

iv. Inexperienced and/or relatively autonomous RMs operating in locations or markets with which the firm is unfamiliar, which may increase the risk of customers misleading, exerting undue influence over or colluding with RMs.

v. A lack of a means of monitoring customer transactions, including a robust independent process for querying and investigating unusual activity on accounts.

Overall Assessment

14. Overall, we found that the private banks covered by our review acknowledged the relatively high inherent money laundering risk within many of their business activities and recognised the need to develop and implement strong AML systems and controls to address areas of their business activities which were relatively vulnerable to money laundering.

15. However, we have some specific issues to raise on aspects of AML within the firms we visited. These are covered below under the following headings: reputational risk, changes to private banks' risk profiles, risk-based approach to AML, senior management oversight and control, relationship managers, customer due diligence, reliance on others, approval of customer relationships including high-risk customers, monitoring, and suspicion reporting.

16. As London's, and the UK's, position as an international financial centre continues to grow, private banks operating out of the UK should be more vigilant about the risk of money laundering. Customers, inevitably including some criminals, see London as a convenient and increasingly important centre for conducting financial transactions.

17. The ability to differentiate legitimate from suspicious activity will become more of a challenge as global financial markets expand and both the markets and criminals become increasingly sophisticated. Private banks must continue to develop high AML standards and operate robust controls based on reliable and up-to-date due diligence, close links between Know Your Customer (KYC) information and transaction monitoring and a robust ethical stance and oversight of controls by senior management.

Reputational Risk

18. When deciding whether to enter into or continue with a customer relationship, private banks link financial crime and reputational risk considerations. We acknowledge that there is an overlap between these two categories of risk and that, to an extent, they are

interchangeable. But we would be concerned if a firm's assessment of reputational risk resulted in a lowering of its standards in relation to financial crime.

Changes to Private Banks' Risk Profiles

19. Some private banks with lower money laundering risk profiles had put in place AML systems and controls which were of a similar level to those at firms operating in 'standard' retail banking or investment business environments. We did not have any significant concerns with these firms' assessments of their current risk profiles, but we believe firms should be more proactive in anticipating the risks which may arise from changes to their business models. We expect firms to be ready to respond with appropriate changes to their systems and controls as their risks change.

20. Private banks with relatively small numbers of customers and staff are likely to develop particularly close, personal relationships with their clients. In this environment, it is more difficult to implement independent checks and balances over account take-on, the adequacy of due diligence and transaction monitoring. However, we expect small private banks to think carefully about whether there are reasonable steps they can take to formalise or tighten their AML control environment. In particular, there are increased risks at these firms that established ways of working may not be sufficient to manage changes to their risk profiles resulting from new higher risk customers or the development of products and services that are more vulnerable to money laundering.

21. Should firms risk profiles change in this way, we would expect firms to have enhanced their systems and controls ahead of this change. The ability to do this relies on MLROs and others with AML control responsibilities being sufficiently aware of business developments and ensuring that improvements to the control environment are made in a timely manner and supported with adequate resources.

Risk-Based Approach to AML

22. As with all firms, we expect private banks to meet their AML legal and regulatory obligations by operating systems and controls that are appropriate to the risks faced by their business activities. Private banks should be in a good position to implement an effective risk-based approach to AML due to their close relationship with clients and relatively comprehensive view of customers' financial activity.

23. We found that the emphasis placed in the 2006 JMLSG Guidance Notes (the Guidance Notes) on the importance of firms adopting a risk-based approach to AML had not resulted in significant changes to the approach adopted by the private banks we visited. We were not specifically concerned by this, as AML practice at private banks appears to having been evolving in a risk-based way for some time.

24. We observed some risk-based simplification of basic identification requirements, for example the development of a formal process for determining whether exceptions to

standard requirements could be made. However, in general the Guidance Notes appear to have given private banks more confidence to continue to develop alternative judgement-based verification and due diligence procedures rather than lower their standards.

Senior Management Oversight and Control

25. The firms benefited from having AML control structures that were common to their different business units and relatively well established policies, procedures and controls.

26. We observed that strong oversight of AML risk management and the adoption of a robust ethical stance by senior management are fundamental to the operation of effective AML systems and controls in private banking. Given the potentially high-risk client base and private banking's attractions to money launderers, the level of senior management's risk appetite for taking on new business, and support for an effective AML control framework, ultimately determine the level of money-laundering risk a firm is exposed to.

27. At one large firm the ethical stance adopted by group senior management could be seen to have a direct effect on the risk appetite and approach to risk management followed 'on the ground'. One aspect of this approach was the way in which RMs were remunerated, which was driven by a variety of business and control considerations rather than being directly linked to revenue generation. As another example, the business was prepared to invest in ongoing initiatives to improve the quality of customer due diligence information which went beyond the current recommendations of the Guidance Notes.

28. In general, senior management were sufficiently involved in and exercised adequate oversight of AML controls. Firms overall had procedures in place to ensure that there was a clear allocation of AML responsibilities and appropriate senior management approval of new client relationships, in particular for those accounts (including PEPs) which were assessed as high risk from a money laundering perspective.

29. However, we saw examples within large, internationally active groups of some AML responsibilities not being clearly attributed, including an historic failure to ensure that accounts which were (partly) relationship managed from the UK but booked overseas were treated for control purposes as UK accounts, and a failure by management to allocate responsibility for the effectiveness of an automated monitoring system.

30. The level of involvement in, and influence over, day-to-day AML controls by MLROs was good. In comparison with other sectors within the financial services industry, MLROs had relatively higher levels of experience, involvement in the businesses and influence over senior management. This reflected the importance attached to effective controls but also the 'manageable' scale of the businesses and the fact that MLROs often occupied other roles such as head of compliance. MLROs were closely involved in approving new clients and were proactive in raising initial and ongoing standards of client due diligence.

Relationship Managers

31. Despite the implementation of mechanisms to oversee and control RMs, the inherent risks associated with RMs having close relationships with customers will always exist in private banking. These strong relationships serve to both enhance the AML control environment, but also potentially increase the risks of conflicts of interest, collusion or RMs being subject to undue influence by the client.

32. We were pleased to see that the private banks covered by our review clearly relied on their relationship managers as their 'front line defence' against money laundering and in general had independent levels of control over the RMs. Such controls were as much to guard against fraud as money laundering. There was one notable exception to this, where the failure of an RM to report suspicious activity was not identified through other monitoring procedures. However, firms would benefit from the improvements to customer due diligence recommended below, which would improve the transparency of customer information within firms and prevent potentially suspicious information being hidden by RMs. Given the key controlling role performed by RMs, it would also be appropriate for firms to provide RMs with more 'valued added' specialist AML training than is currently delivered.

Customer Due Diligence

33. Private banks should obtain and keep up-to-date detailed KYC information on their clients. Private banks normally have access to a good level of customer information, which should allow them to conduct a level of diligence that is appropriate for the risk posed by a particular client. As a result, firms emphasised to us that the level of due diligence conducted inevitably varies from client to client, depending on the judgement of relationship managers and those responsible for approving new accounts.

34. We acknowledge that customer due diligence at private banks cannot be a formulaic process and that it is an inherently judgemental process. However, firms must have mechanisms to ensure that these judgements are applied consistently and are guided by clear standards, sufficiently detailed guidelines and effective training.

35. Without such a framework, there is a risk that standards of due diligence will be applied inconsistently and with too much subjectivity. In addition, it may subsequently be difficult to understand and assess the risks associated with a customer relationship on an ongoing basis and take or justify decisions about whether to continue dealing with a client. Firms also need this framework to guard against changing their standards and financial crime risk appetite over time.

36. Risk-based KYC and enhanced due diligence procedures were in place and being applied at all the firms we visited. However, some firms did not have sufficiently detailed standards and guidelines to ensure that relationship managers and others, with responsibilities for gathering, assessing and documenting customer due diligence information, did so consistently.

37. We believe that firms can do even more to gather, verify and record client KYC and due diligence information and to monitor the adequacy of this on an ongoing basis. We do not advocate an increase in procedural form filling, but firms should perform more analysis of the 'story' behind each client and document this in a systematic way. Firms' recognition of the need to make these improvements was implicit in the steps some had taken to improve their quality control over periodic KYC reviews, and in measures taken by other firms to improve due diligence, for example by taking steps to verify (as will be required by 3MLD) as well as document clients' beneficial ownership.

38. Firms that used standard pro-forma documents to collate KYC information were in a better position to ensure that information was recorded consistently. And it was easier for them to satisfy their required standard of due diligence, without compromising relationship managers' flexibility to record and verify information to a standard that was appropriate for the client concerned. Any exceptions or overrides could be more easily identified.

Reliance on others

39. Some of the firms we visited gained significant new business from clients who were introduced to the firms by professional advisors. Firms emphasised the benefits of these types of introductions from an AML perspective. Despite the fact that in many cases assurance can be gained from the introduction role performed by professional advisers, firms should be careful to ensure that each case is assessed on its merits and, if appropriate, further independent enquiries are made. We did not see any examples of firms systematically reviewing introduced business to ensure it was reasonable to rely on introductions, but this could be appropriate in some circumstances to avoid complacency.

40. The firms covered by our review were generally unwilling to rely on introduction certificates, from other UK regulated firms or overseas firms within their own group, as forms of client identification. This reflected a desire to retain full control of the AML risk management process. This stance is unlikely to be changed by 3MLD, despite the opportunities the Directive provides for reliance to be placed on third parties.

Approval of Customer Relationships, including High Risk Customers

41. We observed some examples of differences in firms' risk appetite for dealing with potentially high risk overseas clients, in particular from Russia. These differences were driven as much by variations in firms' appetites for reputational risk as by their assessments of financial crime risk. While we recognise that, within certain boundaries, firms are free to determine the amount of risk they are exposed to, they should ensure that these decisions are subject to thorough reviews at appropriate senior levels within firms.

42. Many firms conducted periodic reviews of customer relationships. These were performed either annually for all clients or less frequently depending on customers' risk profiles. It was good practice for these reviews to:

- consider KYC information to establish if it remains current and whether the existing risk classification of the customer remains appropriate;
- establish whether the conduct of the account constitutes suspicious activity;
- be conducted by the RMs responsible for the customer but subject to a process of independent review, possibly on a sample basis;
- require senior business line and control function management approval and in the case of high risk customers, including PEPs; and
- be governed by documented standards and guidelines.

Monitoring

43. Because of the depth of customer information private banks hold, these firms should be well placed to monitor customer transactions in order to identify potentially suspicious activity. In general, private banks are in an inherently stronger position than other financial services firms to determine whether customer activity is legitimate and consistent with an expected pattern of behaviour.

44. We expect private banks to have clearly defined policies and procedures to show how and when monitoring should be carried out by RMs or other team members and to whom issues should be escalated. In some cases, we observed that the criteria for deciding whether to exit a customer relationship were not sufficiently clear in firms' policies and procedures. This could potentially lead to inconsistent decision making.

45. The involvement of RMs in the monitoring of activity on accounts contributes to the achievement of a high AML control standard. Conversely, the effectiveness of monitoring, including the follow-up and investigation of unusual or potentially suspicious activity, will be reduced if there is high turnover amongst RMs or the ratio of customers to RMs is high.

Suspicion Reporting

46. Given the relatively low volumes of suspicious activity reports made by private banks, we believe MLROs should be closely involved in the suspicion reporting process. This includes being responsible for reviewing all or a selection of internal suspicion reports which the firm decides to send – or not – to the Serious Organised Crime Agency (SOCA). This was generally the case at the firms we visited, although the MLRO of one major firm had not been sufficiently involved in this process.

47. We do not consider the low volumes of SARs necessarily to be an indicator that firms are failing to identify suspicious activity. Low volumes could reflect robust due diligence during the account opening process, although at larger more diverse firms, where RMs are less familiar with their customers, low volumes of SARs could potentially be more of a concern.

48. Because of the low volumes of SARs and the variety of sizes and business models of the firms we visited, we did not attempt to analyse the variances in reporting between different firms in detail. Such analysis may be possible with a larger sample of firms, in order to gain a better understanding of the reasons for variances between firms – for example, whether these arise from particular monitoring or other AML procedures, or business models.

Findings

Business Overview

49. The private banks covered by our review offered a broad mix of banking and investment services to high net worth individuals and legal entities, such as trusts or personal investment companies, through which these individuals conducted their financial transactions.

50. The largest firms we visited offered cross-border services to an internationally diverse customer base. Some of the smaller firms within our sample focused more on providing investment management rather than banking services. Others served primarily UK resident customers with a less sophisticated product offering that could be described as 'enhanced' retail banking and investment management.

Money Laundering Risk

51. The money laundering risks inherent in private banking are set out for UK-regulated firms in the Guidance Notes (www.jmlsg.org) and, in an international context, in the industry developed Wolfsberg AML Principles on private banking (www.wolfsberg-principles.com).

52. The Guidance Notes state that money launderers are attracted to private banking by 'the availability of complex products and services that operate internationally within a reputable and secure wealth management environment that is familiar with high value transactions'. The following are examples the Guidance Notes quote as factors contributing to the increased vulnerability of wealth management:

    a. Wealthy and powerful clients – they may be reluctant or unwilling to provide adequate documents, details and explanations.

    b. Multiple and complex accounts – within the same firm or group, or with different firms.

    c. Cultures of confidentiality.

    d. Concealment – for example of beneficial ownership through offshore trusts.

    e. Countries with statutory banking secrecy in certain jurisdictions.

    f. Movement of funds – often high value and rapid transfers.

    g. Credit – the extension of credit to clients who use their assets as collateral also poses a money laundering risk unless the lender is satisfied that the origin and source of the underlying asset is legitimate.

53. The Wolfsberg Principles also emphasise the link between money laundering risk and corruption in private banks by stating that 'transactions involving the proceeds of corruption often follow patterns of behaviour common to money laundering associated with other criminal activities…..In most cases a financial institution will not necessarily be aware that corruption is involved in a particular transaction'.

54. Specific examples of risk quoted by Wolfsberg include dealing with higher risk industries such as arms dealing or with PEPs who either are in a position to exert undue influence on decisions regarding the conduct of business by private sector parties, or have access to state accounts and funds.

55. The highest risk business activities conducted by the firms we visited had characteristics that were consistent with the risk factors highlighted by the Guidance Notes. Examples of these were the provision of offshore accounts where there was little face-to-face contact with clients, fiduciary services for trusts and other corporate structures, and a wide range of services provided to clients from various emerging markets, notably including Eastern Europe and Africa. Several firms had both opened accounts and turned down applications from Russian oligarchs, who were frequently cited during our visits as an example of a group of very high-risk customers on whom firms had conducted extensive due diligence.

Senior Management Oversight

56. Most of the MLROs at the firms we visited were also heads of compliance. Although this was partly a reflection of the size of the firms, it meant that MLROs had regular and direct access to senior management and in many cases reported directly to the CEOs. As heads of compliance, MLROs were in a strong position to be able to direct compliance resources towards AML and often exercised direct control over the account opening process.

57. There were some exceptions to this. At one firm the Money Laundering Compliance Officer reported to the head of compliance and worked closely with other areas with key AML responsibilities, notably an overseas transaction monitoring team and a central account opening team within operations. At another firm the MLRO operated in more of an advisory role and, with the exception of suspicion reporting, the front office had full responsibility for day-to-day AML. These arrangements reflected the organisational structures and business models of these two firms and relied to a greater extent than elsewhere on good collaboration between different areas of the business.

58. Overall, we were satisfied that senior management were sufficiently involved in and exercised adequate oversight of AML controls. Firms had procedures in place to ensure that there was appropriate senior management approval of new client relationships, in particular for those accounts (including PEPs) which were assessed as high risk from a money laundering perspective.

59. We expect firms to have regular management reporting on money laundering issues (e.g. number of reports to authorities, monitoring tools, changes in applicable laws and regulations, the number and scope of training sessions provided to employees). It appeared that Boards and other committees with responsibilities for AML were in a position to receive sufficient information about issues and the effectiveness of controls on a regular and ad hoc basis. This was usually because MLROs provided regular reports (often covering regulatory compliance as a whole) to, and were represented on, these bodies.

Role of Relationship Managers

60. The role of the RMs is particularly important to private banks in managing and controlling money laundering risks. RMs develop strong personal relationships with their clients, which facilitate the collection of the necessary information to know the client's business, including knowledge of the source(s) of the client's wealth.

61. RMs must, however, at all times be alert to the risk of becoming too close to the client and to guard against the risks which can arise from a false sense of security or conflicts of interest, including the temptation to put the client's interests above that of the firm, or from being subject to undue influence by the client.

62. The private banks covered by our review clearly relied on their relationship managers as their 'front line defence' against money laundering. RMs were responsible for conducting most of the KYC processes and reviewing transactions in order to identify potentially suspicious activity.

63. Although these were more limited at the smaller firms, all the firms had review and approval processes in place to balance and control the role of the RMs. These included second and third levels of new client approval and reviews of KYC information by independent units within the business. We were also informed that full due diligence would be conducted on any clients brought by an RM from another firm.

64. Despite the implementation of mechanisms to oversee and control RMs, the inherent risks noted above in relation to RMs will always exist in private banking. In particular, this risk is higher when one part of a group relies on assurances and due diligence information provided by RMs working for the same group in a different jurisdiction. Some firms recognised this and were reluctant to rely on information provided from overseas parts of their group unless it could be verified by the UK business (see 'Reliance on Others' below).

Client Identification and Due Diligence

65. Client acceptance procedures are at the core of effective AML risk management in private banks. These should include the verification of identity and due diligence on account holders and underlying beneficial owners, including establishing the origin of wealth and source of funds deposited. These procedures should take into account key risk indicators such as whether the customer is located in a high-risk country or categorized as a PEP. Because of the risks associated with private banking, the level of client due diligence will usually be higher than for other retail financial services. A key consideration should always be whether there is clear justification for clients conducting business in a certain way.

Know Your Customer (KYC)

66. It is therefore important for private banks to always collect and record information covering the purpose and reasons for opening an account, anticipated account activity, source of wealth, estimated net worth, source of funds (the origin and the means of transfer for funds that are accepted for the account opening), clients' business and business structures and references or other sources to corroborate KYC information where available.

67. In addition, RMs should meet clients – ideally before account opening. The Guidance Notes state that relationship managers should record visits to clients' businesses or homes and gather information including changes in client profiles, expectations of product usage, volumes and turnover going forward, together with any international dimension to the client's activities and the risk status of the jurisdictions involved.

68. All firms had policies and procedures for obtaining KYC information about potential and existing clients. These required RMs at least to obtain information on the source of clients' wealth, their business and occupation and the purpose of the account. It was the policy of all firms to exercise a greater degree of diligence at the inception of a client relationship, but also in varying degrees to maintain up-to-date KYC information on an ongoing basis.

69. The extent of verification undertaken on KYC details provided by clients was determined by firms on a judgemental basis. As a result, this varied from case to case, depending on the clients' circumstances, availability of information and assessment of risk by the firms. Although this information was inherently 'bespoke', firms that used standard pro-forma documents to collate KYC information were in a better position to ensure that information was recorded consistently, satisfied the firms' required standard of due diligence and, if information was not available, they noted the reasons for this.

70. Most clients were visited by relationship managers at their homes or business premises at the start of a relationship and also on an ongoing basis. In some cases this was a mandatory account opening requirement. Firms recognised that this was an important

part of the KYC process, which allowed relationship managers to substantiate clients' personal and business circumstances and cross refer these to patterns of activity on clients' accounts.

71. Quality KYC information is the key to a wider AML control environment, as it is a prerequisite for effective risk assessment, transaction monitoring and suspicion reporting. One MLRO stated that client take-on still involved too much procedural form filling and not enough analysis of the 'story' behind each client. Others had taken steps to improve their quality control over periodic KYC reviews and the quality of due diligence.

72. We agree with several firms who emphasised to us that due diligence cannot be a formulaic process. They said they have to rely on the judgement of relationship managers, MLROs and others to determine whether a sufficient level of client due diligence has been conducted. But we believe that firms can do even more to ensure that KYC information is gathered, verified and recorded on a consistent, sufficiently reliable and detailed basis.

73. RMs and others responsible for deciding whether to enter into customer relationships need to be able to refer to clear standards and guidance from senior management and MLROs when assessing how much information to obtain and verify. Without these, the level of KYC held by a firm is more likely to be inconsistent, out of date and insufficient for the risk posed by the customer.

Beneficial ownership

74. Where the client is a company, such as a private investment company, it is important to be able to follow the chain of title to know who the beneficial owners are and conduct due diligence on the principal beneficial owners, as defined by the Third Money Laundering Directive and under firms' risk-based policies. The structure of the company also needs to be sufficiently understood to determine all the providers of funds and those who have control over the funds, e.g. the directors and those with the power to give direction to the directors of the company. A reasonable judgement must be made, by RMs and those responsible for approving new accounts, as to the need for further due diligence on other shareholders.

75. The same principles apply where the client is a trust, where the structure of the trust must be sufficiently understood to determine the provider of funds (e.g. settlor), those who have control over the funds (e.g. trustees) and any persons or entities who have the power to remove the trustees.

76. Private banks must establish whether the client is acting on his/her own behalf. This assessment inevitably relies heavily on the judgement and instinct of RMs. Firms that served overseas clients informed us that it could be difficult in some jurisdictions to determine whether the party they were dealing with was the real underlying client. In these situations, it was vital to have good local contacts and experience in order to

pick up reliable information from informal channels. Two firms benefited in this way from being able to leverage off the knowledge of their local retail branch network in jurisdictions where reliable official information was difficult to obtain, such as Russia and parts of Africa.

77. We found that the private banks we visited had policies and procedures to ensure that the ultimate beneficial owners and controllers were adequately identified and that sufficient due diligence was conducted on them.

78. The firms covered by our review did not set formal fixed thresholds for the level of beneficial interest above which owners would be identified and subject to wider due diligence, although we were informed that those holding underlying stakes of 25% or more would always be subject to this process. Some firms set a guide of between 20% and 25% as the threshold, but this was in some cases as low as 10%. Firms explained that they wished to retain the flexibility to conduct due diligence on any beneficial owner or party with controlling influence if they considered it necessary in the circumstances. Although these standards met the requirements of 3MLD, it was clear that they were set using risk-based judgements rather than being driven directly by this Directive.

79. While all firms conducted identification and due diligence on beneficial owners, verification of the links between different levels of ownership has traditionally not been done by firms in general. However, there were signs that private banks were beginning to try to verify these links as part of their standard due diligence procedures. One MLRO informed us that, in his opinion, the Guidance Notes (which reflect the future 3MLD requirement to conduct due diligence on beneficial owners with stakes over 25%) were 'too soft'; if he could not verify ownership to a level that he was satisfied with he would not proceed with the relationship.

80. Currently, this verification process relies to a large extent on the willingness of clients to volunteer information; for example, one firm imposed a formal requirement on all clients to inform the bank of any changes to beneficial ownership and another did the same for holders of bearer shares through an annual certificate of ownership, which required the approval of a managing director. This process of certification is standard practice in Switzerland, where there are legal penalties for providing false declarations. This firm was also in the process of encouraging owners of bearer shares to register their interests and was running a major long-term project to verify the chain of ownership for all its clients. In general, it is too early to say if firms will encounter widespread resistance from clients when they seek to verify beneficial ownership. However this should become clearer once firms are forced to do this following implementation of 3MLD.

Reliance on others

81. Some of the firms we visited gained significant new business from clients who were introduced to the firms by professional advisers (predominantly accountants or solicitors rather than financial advisors). In many cases, referrals from existing clients

were also a valuable source of new business. Firms emphasised the benefits of these types of introductions from an AML perspective. While standards of due diligence would generally not be lowered for business sourced in these ways, additional assurance was gained from the fact that clients had been introduced by reputable parties who in many cases would have conducted their own due diligence and were likely to have a detailed knowledge of the clients' affairs.

82. Despite the fact that in many cases assurance can be gained from the introduction role performed by professional advisers, firms should be careful to ensure that each case is assessed on its merits and, if appropriate, further independent enquiries are made.

83. The firms covered by our review were generally unwilling to rely on introduction certificates, from other UK-regulated firms or overseas firms within their own group, as forms of client identification. Even one firm that was part of a major international group had a policy of not issuing or accepting group introduction certificates. One firm was an exception to this, but still adopted a cautious approach to all other parts of its group. Another accepted introductions from other firms but these were usually for one-off deals for which the transaction due diligence process was inherently very thorough.

84. Where clients were already dealt with by others parts of the same group, firms typically obtained copies of the original identification evidence from the other part of the group but conducted their own due diligence in the client. This was driven by various factors such as a very low appetite for reputational risk and a view that the firms may discover previously unknown information about a client.

85. Firms received a limited number of requests from 'walk-in' clients to open accounts, which were always more likely to be treated with caution than introduced business. We were informed that new clients who were brought to the firms by relationship managers who had previously served these clients at another firm would be subject to the same standards of due diligence as any other prospective client.

New account approval

86. All the firms we visited recognised the importance of conducting thorough due diligence on potential new clients. In most cases this was seen as a response to the relatively high inherent money laundering risk, although in some cases firms could justifiably argue that the products and services they offered and their client base were no more risky that standard retail banking and investment business.

87. RMs were typically responsible for collating identification and KYC information on potential clients. The relatively small size of many private banks covered by our review allowed RMs to communicate closely with the MLROs if necessary during the account opening process. We found that MLROs were keen to be accessible to the front office during this process and strongly encouraged RMs to bring issues and queries to them as early in the account opening process as possible.

88. Along with the relevant RM and a senior manager from the front office, MLROs at most of the smaller firms formally approved all new accounts. At the larger firms, while RM and senior manager approval was also required, approval by a member of a specialised central account opening team – within an operations area or within compliance under the direct control of the MLRO – was also required. New high risk clients (see below), including PEPs but otherwise defined under firms' own criteria, always required the sign off of the MLRO and the CEO of the private banking business or someone in a very senior controlling role within the business.

89. Reviews by specialised central account opening teams consisted of checks to ensure that the information obtained by RMs was complete and met the firm's detailed policy standards. They were also responsible for screening new clients against third party data sources, for general KYC information gathering purposes and also for identifying any negative information. Some firms used in-house databases to screen clients, which contained a variety of group-wide information such as details of previous suspicion reports, issues and investigations. Common external data sources such as Worldcheck, Factiva and Lexis Nexis were also used.

High-risk clients

90. In its internal policies, firms should define categories of persons whose circumstances warrant additional diligence and senior management approval. This will typically be the case where the circumstances are likely to pose a higher than average risk to a bank. These could include 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 and persons engaged in types of business activities or sectors known to be susceptible to money laundering.

91. The Guidance Notes recommends that clients connected with such businesses as gambling, armaments or money service businesses should be considered for treatment as high risk, and relationships with PEPs (see below) should only be entered into with the approval of senior management.

92. Firms often used specialist investigation agencies to conduct research on the backgrounds of potential clients who were considered to be high-risk The most frequently quoted examples of this type of due diligence related to clients from the former Soviet Union. However, information obtained by specialist investigators was often from unattributable sources. In these cases, firms questioned how much reliance could be placed on this information and whether the final decision about whether to conduct a relationship would be almost as subjective as it would have been without this type of information.

93. When deciding whether to take on high-risk clients, firms' concerns about financial crime risk were invariably interlinked with reputational risk considerations. Several firms explained to us that it could be difficult to find adverse information relating to high-risk potential clients. This was likely to lead to the decision to take-on a client being driven by the firm's appetite for the customer's business.

94. From our review work and evidence obtained from other firms, it is clear that private banks have varying levels of risk appetite for dealing with high-risk clients. We believe that these differing risk appetites usually reflect different appetites for reputational and legal risk, together with non-specific financial crime concerns. There was evidence that firms were prepared to turn away high-risk business. Some firms had a formal policy of not opening accounts for clients involved in certain business activities such as arms dealing.

95. Most firms had well developed policies for categorising clients by risk and had put in place procedures for regular reviews of the highest risk clients by senior management. As an example, one firm classified its highest risk clients using the following factors:

- have active financial links with countries included in the bank's 'hot-list';
- are engaged in schemes that are 'tax aggressive';
- are engaged in the manufacture or sale of armaments;
- are engaged in businesses involving dangerous, radioactive or toxic substances and/or significant human or environmental risk;
- are deemed high risk because, as yet, the bank has insufficient information about their activities;
- have been the subject of a suspicious activity report; and
- the account officer considers the account needs transaction level monitoring.

Sanctions & Politically Exposed Persons

96. The Wolfsberg guidelines state that when PEPs are private banking clients, they should be subjected to greater scrutiny. Examples cited of high-risk indicators in relation to PEPs are if the customer has a family member in a government position, has failed to disclose owners, partners or principals, uses shell or holding companies or equivalent structures that obscure ownership without credible explanation and has little or no expertise in the industry or the country in connection with which he acts as an intermediary.

97. PEPs are defined by 3MLD as 'natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons'. This definition only applies to those outside the UK. Because of their position and associations, PEP status may lead to a client being considered high-risk.

98. The Directive will require firms, on a risk sensitive basis, to:

a. have appropriate risk-based procedures to determine whether a customer is a PEP;

b. obtain appropriate senior management approval for establishing or maintaining business relationships with such customers;

c. take reasonable measures to establish the source of wealth and source of funds of such customers; and

d. conduct enhanced ongoing monitoring of the business relationship.

99. All the firms we visited had systems in place to screen potential and existing clients to identify whether they were PEPs or listed on the Bank of England and other international financial sanctions lists. Worldcheck was by far the most commonly used database service for screening clients in this way, as well as against a range of publicly available background information. Complicheck and Factiva were also used for these purposes. Some firms used Lexis Nexis to search media publications for references to particular clients.

100. We observed some good practice at one firm in relation to screening and following-up alerts. The firm used 'Pinpoint' software which provided an interface between the firm's client database and the 300,000 names contained in Worldcheck, whose data was downloaded daily. The Pinpoint software ensured that, where there is at least an 85% fuzzy match between Worldcheck data and the firm's client database, Pinpoint raised an alert.

101. RMs logged on to Pinpoint every morning, to review the alerts that had been flagged. The system allowed the RMs to click directly onto the relevant Worldcheck entry, in order to see exactly what it said – including the date the information was first entered and when it was last updated, and what external sources provided the information. The relevant RM, having reviewed the data, then attached his recommendation to the alert and forwarded it to Compliance for a second opinion. No front-office staff member was able to park, bury or hide such an alert.

102. Annual reviews of lists of existing PEP customers and other firm-defined categories of high-risk accounts were a standard procedure for some firms. These typically involved circulating existing lists of PEPs to RMs so they could recommend additions to or deletions from the list. In one case this involved direct discussion between relationship managers and compliance to confirm the status of accounts and agree any actions or information needs.

103. Firms should have formal escalation and decision-making procedures for resolving any issues relating to the approval and ongoing conduct of PEP or high-risk accounts. These procedures existed at most firms we reviewed. At one firm this involved a review by the MLRO and a senior business line manager followed by an escalation of unresolved issues to the CEO. At another, senior business, legal and compliance approval was required annually for all high-risk relationships, including PEPs.

104. At some firms, enhanced monitoring was conducted on PEP and other high-risk accounts. Where this was not the case, firms justified their approach on the basis that all clients were subject to a common high level of monitoring and review.

Updating KYC

105. Private banks should exercise a greater degree of ongoing due diligence on their clients than would normally be expected in a retail banking environment. This includes understanding whether the pattern of client's activities is consistent with the expected legitimate activity, based on the KYC information already obtained for the client.

106. To be in line with the JMLSG Guidance Notes, firms should review and update client information periodically, or when a material change occurs in the risk profile of the client. Periodic reviews should be set on a risk basis and be performed at least annually for higher risk clients.

107. Overall, we found that firms conducted periodic reviews of KYC information. At one large firm a dedicated central client services team was responsible for both processing new accounts and ensuring that RMs carried out annual reviews, which were diarised and monitored by the team. This allowed senior management to track the progress of relationship managers in conducting these reviews.

108. Periodic KYC reviews were designed to identify changes to clients' risk profiles due to new products or transaction behaviour. However, firms did not in general perform additional due diligence when they provided addition products or services to existing clients that were higher risk than those previously provided to the clients. Instead, firms preferred to conduct due diligence at the account opening stage that was sufficient for the highest risk products in order to avoid inconvenience to clients at a later stage.

Transaction Monitoring

109. In view of the risk associated with private banking activities, it is appropriate that there should be a heightened ongoing review of clients' account activity.

110. The primary responsibility for monitoring account activity lies with the RM, who should be familiar with significant transactions and increased activity on the account, and will be best placed to identify unusual or suspicious activities. At the large firms, best practice would be for these responsibilities to be supported by the use of automated systems.

Manual monitoring

111. The firms we reviewed relied primarily on RMs to identify unusual and potentially suspicious transaction activity on clients' accounts. RMs were expected to be aware of their clients' transaction activity, but the frequency and thoroughness with which this was done was determined to a large extent by the RMs.

112. There were examples of firms taking a relatively formal approach to this, such as categorising accounts between high, medium and low risk to determine the nature of

transaction activity reviews, with the following result at one firm: high risk – reviewed on a monthly basis, using a rolling three months of previous transaction data; medium risk – reviewed on a three monthly basis, using six months of transaction data; and low risk – reviewed as and when deemed necessary.

113. At one firm the MLRO or his deputy reviewed all transactions for accounts categorised as high risk and, in the case of payments, before transactions were processed.

114. Transactions into and out of investment management portfolios were relatively easy for small and medium sized firms to monitor. Although third party payments could be made, as these were infrequent and often for known reasons such as tax, relationship managers usually had a good understanding of the normal expected pattern of payments and, if necessary, would expect clients to explain the purpose of payments.

115. In summary, manual monitoring must reflect the circumstances and risk associated with a firm and its customers. The frequency and structure of this monitoring will inevitably vary from firm to firm. However, where the ratio of customers to RMs is high, we would expect MLROs to assess more carefully whether RMs have sufficiently detailed knowledge of their customers and conduct transaction reviews on a sufficiently regular basis.

Automated monitoring

116. Alongside manual monitoring, the private banking units within the major groups we visited used automated systems to monitor their customers' transaction activity. We conducted a focused review of systems such as these during 2006, which included group-level visits to two of these groups. The systems used either 'profiling' or 'rules-based' methods. Both techniques were designed to identify unusual transactions (alerts) which were then investigated manually to determine whether they should be reported to SOCA as suspicious.

117. Profiling methodologies used statistical techniques to compare recent patterns of transaction activity (by volume and value) on accounts to historic patterns of activity for the same transaction type on the same account, or on a 'peer group' of accounts, in order to determine whether recent activity was 'unusual' (i.e. over a defined threshold or standard deviation from the norm).

118. Rules-based monitoring methods involved assessing whether transactions with particular characteristics (e.g. customer, product, jurisdiction) exceeded certain absolute thresholds or were within certain fixed ranges (e.g. volume, value, frequency), or whether the transactions met relative measures (e.g. large volume in comparison to recent account or peer group activity). While these 'relative measures' or 'relational rules' were a form of profiling, they were based on simple arithmetic comparisons, not the statistical profiling techniques described above.

119. Overall, the findings from this earlier work indicated that firms needed to devote more resources to analysing and assessing the performance of their systems, in particular defining more clearly how success is measured and producing more robust objective data to analyse performance against these measures. We do, however, support firms' implementation of these systems which should at the least act as a 'safety net' to flag activity which members of staff have failed to identify.

120. From additional information gained for this review, some issues emerged which are more specific to private banking businesses. These included a lack of clarity over responsibility for the effectiveness of the automated monitoring system. At one group, we believed that measures could be taken (such as reviews of transactions not flagged by the system) to assess whether the system was identifying the most unusual and potentially suspicion transactions.

121. One MLRO expressed concern about the volumes of alerts and insufficient calibration of the alert parameters, although the existing system was due to be replaced. Despite having some reservations about the existing system, this MLRO's view was that systems-based monitoring was useful because it encouraged dialogue with RMs, prompting them to keep their customer and compliance knowledge up to date.

122. Other smaller private banks used simple 'rules based' techniques to identify and review unusual transactions. This typically involved transactions being flagged if they breached or met one or a number of pre-set thresholds or patterns of activity. Examples of these rules are: cash transactions above a certain value, transactions into and out of an account within a set timeframe and total value of account turnover in a given period.

123. These rule settings were typically based on the judgement of those with compliance and AML responsibilities. To be effective, the reviewing of alerts required close liaison between a central team with responsibility for processing the alerts and RMs with detailed knowledge of the clients concerned, who would be asked to explain and document the legitimate reason for a transaction or other reasons for it not being considered suspicious. Our overall impression was that these processes were sensibly designed.

Suspicious Activity Reporting

124. Unusual or suspicious activities can be identified through monitoring of transactions, customer contacts (meetings, discussions, in-country visits etc.), third party information (e.g. newspapers, internet, vendor databases), RMs' or corporate knowledge of a customer's environment (e.g. political situation in their home country).

125. Overall, our reviews of samples of suspicious activity reports indicated that these reports were well documented and based on reasonable assessments of the customer activity in question.

126. Given the size of the private banks we reviewed and the relatively small number of SARs generated by the businesses, at most firms staff were able to communicate closely with MLROs when reporting internal suspicions and could rely on the MLROs or members of their team to coordinate any investigation work relating to the reports.

127. There was one exception to the above, where there was a lack of management information regarding trends in suspicion reports and multiple reports made with regard to individual relationships. This resulted in a lack of appropriate AML oversight and a risk that the MLRO may be unaware of patterns or trends. The above problem is more likely to occur at larger private banks where responsibilities for suspicion reported are more delegated and dispersed.

128. Because of the emphasis placed by private banks or protecting their reputation or managing so called 'franchise risk', we saw some evidence that firms are likely to report 'defensively', for example by reporting negative media reports about clients to SOCA. We consider that, to an extent, this is an unavoidable consequence of firms' risk aversion, but MLROs should guard against this tendency as much as possible and ensure, through feedback and training, that staff focus on 'genuine' suspicions.

Controls Monitoring & Assessment

129. Internal audit (IA) departments typically reviewed AML controls on a periodic basis. This work by IA provided a useful means of engaging senior management and influential high level committees in AML issues. But more frequent reviews for compliance monitoring or other quality assurance (QA) purposes, by compliance, risk or operations areas, appeared to be a more targeted and effective means of assessing the adequacy of controls and raising standards.

130. One large firm had taken steps over the last year to enhance its monitoring and QA over the annual KYC review process. As part of this, RMs' performance ratings could be affected by a failure to conduct KYC reviews on a timely basis. Another firm was engaged in an extensive exercise to improve the information held in relation to beneficial ownership and had specific monitoring in place to ensure the completeness of bearer share ownership certification, the correct categorisation of high-risk customers, and of suspicion reports in order to decide whether to exit customer relationships.

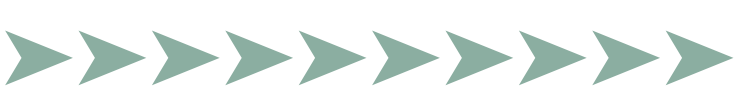
Training

131. In line with best practice, private banks should establish a training program covering the identification and prevention of money laundering for employees who have client contact and for other staff involved in AML. Regular training should also include how to identify and follow-up on unusual or suspicious activities. In addition, employees should be kept informed about any major changes in AML laws and regulations. It is common practice for all new employees to be provided with guidelines on the AML procedures.

132. As with most UK-based financial services firms, the private banks delivered AML training through a combination of general training (often computer based and including a test) for new joiners, and periodically for existing staff, and more targeted face to face delivery for specific parts of the business such as on KYC for client facing staff and on sanctions for settlements teams. In general, firms had continued to train all staff at least every two years, although this time limit is no longer an FSA requirement.

133. Given the particular risks faced by private banks, on balance we believe these firms can do more 'value added' training and awareness-raising in relation to AML. Given the onus placed on RMs and others to ensure adequate customer due diligence and to take well informed judgements on the legitimacy of customers' activity, it is appropriate for private banks to deliver more in-depth and technical training, for example on the UK's Proceeds of Crime Act or country specific risks, than is usually appropriate at other financial services firms. At one firm, for example, improvements in AML training to more closely match job responsibilities would have been welcomed by many staff involved in monitoring and suspicion reporting.

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®