DP22: Reducing money laundering risk – Know Your Customer and anti-money laundering monitoring

In August 2003 we published Discussion Paper DP22. That paper sought to stimulate debate on two important topics seen as crucial to anti-money laundering but which raise difficult practical issues and important questions about proportionality and risk management:

- Know Your Customer (KYC); and
- anti-money laundering monitoring.

We put forward four options to help us decide whether to make changes to our Handbook, rely on JMLSG Guidance Notes or defer action for a period to see how practice develops.

We are very grateful to all those who responded. On 21 April we announced (Speech to a City & Financial Conference by Philip Robinson *Anti-money laundering regulation – next generation developments*, available on www.fsa.gov.uk/pubs/speeches) a programme of work on a number of anti-money laundering topics very relevant to the subjects covered by DP22. We have therefore decided to defer decisions until this work has progressed. This will also enable us to take into account the work of the JMLSG on revised Guidance Notes. We nevertheless consider that it would be helpful to make the responses to DP22 publicly accessible now.

Daniel Shonfeld
Financial Crime Policy Unit
The Financial Services Authority
25 The North Colonnade
Canary Wharf
LONDON E14 5HS

3 February, 2004

Dear Mr Shonfeld

Discussion Paper 22 (Reducing Money Laundering Risk – Know Your Customer and anti-money laundering monitoring): response from Abbey

Abbey welcomes the opportunity to contribute to the FSA's ongoing consideration of the appropriate range and scope of the regulatory requirements for anti-money laundering activity by regulated firms within the UK.

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

KYC information

The collection of KYC information is important for financial services firms to be able to meet their legal and regulatory obligations, in that it provides a wider picture of the customer's circumstances and the likely parameters within which the customer will use the financial services firm's products and services. Information such as occupation, salary or income, date of birth, and the nature of a customer's business allows firms to conduct a more effective and accurate risk assessment of their customer base and thereby ensure that their monitoring activities remain appropriately focussed and targeted on the right groups of customers.

That said, the nature of a firm's products and business, and the relative risk that each bears, should then determine the extent and nature of the KYC information that is sought from the customer. In the absence of any other factors, the extent of KYC information required for low risk products such as term assurance should be less than that for a high risk money transmission account such as a bank account. Similarly, customers from higher risk countries such as NCCTs may require a higher degree of KYC information than those from the UK.

Taking this risk based approach is only appropriate, however, if a firm can identify that an existing customer has entered into a relationship based on a lower level of KYC, and is then able to capture the appropriate level of KYC if the customer returns to buy a higher risk product. For some firms this may mean a choice between investment in enhancing the sophistication of their customer systems or the perceived competitive disadvantage inherent in an intrusive customer proposition.

KYC information is also crucially important in relation to the assessment and potential reporting of suspicious activities. Where a transaction or customer relationship is initially assessed as being potentially suspicious, the additional information obtained through the KYC process allows investigators within the firm to make a significantly better informed decision on whether or not to make a report to NCIS, as knowledge of the customer's occupation or business might either explain a series of transactions or confirm the initial suspicion if it did not match the customer's behaviour. The absence of such information may therefore either lead to a failure to report because of lack of evidence or defensive over-reporting. Conversely, if such information is held, this would allow the firm to make a better quality SAR to the authorities.

On the question of the frequency with which KYC information should be updated, our view is that this should be at a minimum when there is a significant trigger event in relation to that customer, such as a change of address or change of name, although this should not require a full revaluation of all KYC data held on a customer as this could be unduly intrusive. Firms should be able to determine the extent of such a review based on their own assessment of the relative risks. Firms should, however, keep full records both of the date of any change in KYC information, the nature of the change, and the previous records, in order to be able to provide a full audit trail either in the event of contact by law enforcement or to support any internal investigations by, for example, Group Fraud. There may, however, be other customer relationship management reasons for collecting information with a greater frequency than this, but that is unrelated to AML requirements.

<u>Monitoring</u>

We would agree that some form of monitoring beyond ongoing reliance on the alertness of individual members of staff is necessary. Although customer identification at the outset of a new relationship will help in deterring potential money launderers, the availability and extent of forged documents and fake identities mean that this is not enough to mitigate the risk of a firm being used to launder money.

The nature and extent of monitoring, and whether this occurs on a manual basis or through using automated transaction monitoring systems, will again depend on the relative risk and characteristics of the products concerned and the distribution channel used. The volume of transactions within a retail banking environment would mean that reliance on staff manual identification may be of limited effectiveness and an automated monitoring system can provide an effective tool for reviewing patterns of behaviour. In a life assurance business, however, where the major risk for money laundering would arise from specific unusual events such as early withdrawals or significant increases in one-off contributions, an automated system may not provide sufficient cost-effective additional information beyond that available through the usual business process for managing such events.

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

A risk-based approach will require an assessment of the range of factors which will affect the potential for money laundering to take place within the firm. It will therefore need to address *inter alia* the following considerations:

- the inherent potential risks in the products the firm offers;
- the different risks posed by the variety of delivery channels that are utilised;
- whether the customer is taken on and conducts their business on a face to face basis or remotely;
- whether the customer is introduced by a third party, and the extent to which reliance has been placed on the third party in identifying and providing KYC information on the customer;
- the geographic location of the customer, including whether they are resident in an NCCT or non-FATF jurisdiction;
- the relative transaction and turnover size for the customer compared to the expected values for other customers with the same product and customer characteristics;
- evidence of typologies and methods of money laundering provided by the law enforcement community; and
- the efficiency of the firm's systems to treat different categories of customers differently.

Individual firms can then conduct their own assessment of the risks within their own operations against the risk factors that they have identified, and then determine what is appropriate to mitigate those risks. In doing so, we expect that firms will make as much use of external sources of information as possible, including their peer group, evidence from the FSA and law enforcement, industry groups and trade associations.

We do not believe that the FSA should prescribe the nature and extent of the monitoring that firms should conduct, as this will depend on firm-specific factors. That said, there is an argument for some sort of common standards or approach for a base-line level of KYC information, determined in relation to broad product groups, to ensure that there is no competitive pressure to reduce requirements. This is particularly important for those firms which rely on intermediaries, as one benefit of the existing approach to anti-money laundering is that it is not seen as a competitive matter in relation to dealing with customers; by allowing an entirely free-form risk-based approach to dealing with customers, this standard approach will come under pressure.

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

We do not believe this question is for us to answer.

We would, however, encourage law enforcement to provide as much information on this topic to the industry as possible to assist us in providing the right SARs with the right level of information and detail where we have suspicions. In addition, we would strongly support the recommendation for a greatly increased volume and degree of feedback from law enforcement and NCIS (both on individual cases and in respect of typologies) advocated by KPMG report in 2003.

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

We believe that the costs that firms should incur in relation to both obtaining KYC information and implementing monitoring systems should reflect the level and degree of risk that has been identified. The potential costs will therefore vary significantly between different firms depending on their product profile and their customer base.

Increased costs for KYC activities will include the processing costs for the capture and retention of additional information on customers, including links to existing legacy systems or the implementation of new customer relationship management systems. There will be staff costs relating to increased training for any new requirements and the potential additional time spent in taking on new customers, or refreshing data in existing customers.

The benefits of obtaining additional KYC information will be that firms have a greater degree of information on their customers which should allow opportunities for more targeted marketing and a greater understanding of the customer base. It may also provide additional information to combat actual or potential fraud on the organisation.

The implementation of automated transaction monitoring systems will significantly increase the costs for a firm. Not only is there the cost of the relevant IT hardware and software and the attendant systems support and infrastructure, but most systems currently generate a significant number of false positive suspicious transactions which then have to be reviewed and filtered on a manual basis, thereby increasing the number of staff required to manage the process. New manual transaction monitoring systems will incur primarily staff costs, but there will also be systems costs both to change systems to facilitate monitoring and to record the information obtained.

The benefits from automated systems should be that there will be a higher number of good quality SARs produced which can be used by law enforcement to prosecute potential offenders and, where appropriate, seize their assets under the provisions of the Proceeds of Crime Act. They will also provide a greater degree of management information on trends and customer activity on different classes of account, thereby assisting greater customer segmentation and marketing analysis.

Q5: Which options presented do you prefer and why?

On balance, Abbey is in favour of option 2 ("to make new high-level rules and/or guidance, to better money laundering risk management by firms"), although we recognise the strong arguments in favour of option 4 ("to make no decision now and review the position again in, say, two years time"). This is both because of the factors set out below and in recognition of the FSA's proposals to review its financial crime rules; wider guidance on risk management within SYSC would fit within the rationale that the FSA has given for removing Chapter ML and placing a greater focus on SYSC 3.2.6R.

SYSC 3.2.6R requires that firms should consider, assess and manage the money laundering risks that they have identified in relation to their business though the application of appropriate systems and controls. This leaves the onus on firms to identify their own standards through a risk-based approach, whereas in our experience the FSA already has expectations of what different firms in different sectors and with different business profiles should be doing. High-level generic guidance on risk management approaches and articulation of these expectations would provide a minimum standard and allow the FSA to assist in the implementation of industry-wide better practice (if not best practice). This could then cover both KYC issues, either with specific FSA expectations or in relation to the KYC standards set out in the Guidance Notes, and monitoring.

In doing so, any guidance should include an appropriate acknowledgement of the role of individual firms in implementing this guidance within their own circumstances.

There will always remain the risk that, in implementing a risk-based approach to anti-money laundering systems and controls, firms are nonetheless used for either money laundering or terrorist financing. Our view is that the FSA should formally recognise the potential constraints and limitations inherent in a risk-based approach; in doing so it should also formally recognise some form of safe harbour for firms which had established a reasonable risk-based approach based on a sensible view of its business and risk profile but which were then subject to money laundering.

If you would like to discuss any of the issues we have identified, please do not hesitate to contact me.

Yours sincerely

Amanda Hughes

Group Money Laundering Reporting Officer

American Life Insurance Company
Alico House
22 Addiscombe Road
Croydon
CR9 5AZ
Tel: 020 8680 6000
Fax: 020 8680 7217

Mr Daniel Shonfield
Financial Crime Policy Unit
Prudential Standards Division
Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

9 September, 2003

Dear Daniel

re: Discussion Paper 22 - Reducing Money Laundering Risk

I refer to the recently issued Discussion Paper, addressing the issues of 'Know Your Customer' and 'Anti-Money Laundering Monitoring'.

I have reviewed the Discussion Paper with interest and felt that it may be helpful to make some observations.

Just to clarify the position from which we are considering this matter, in terms of the marketing of regulated investment products, we exclusively market our products via Independent Financial Advisers and do not currently operate a Direct Sales Force or, indeed, market products direct to the general public.

In this respect, we are not necessarily in a position to know our customer, albeit the general requirement to maintain vigilance in terms of suspicious transactions is, of course, highly relevant.

In terms of the subject of Money Laundering, our concerns relate more to how companies are expected to respond to both the Rules and Regulations published by the FSA and the contents of the Guidance Notes for the financial sector provided by the Joint Money Laundering Steering Group.

To give you a specific example, FSA Rule 3.2.2 seems to make clear that the duty to identify a client does not apply if a client is introduced to a relevant firm by a person who has given the relevant firm a written assurance that in all such cases he obtains and records identification evidence, provided that person is subject to

Cont'd./...

9 September, 2003

Regulatory oversight. Clearly, this indicates that where business is received direct from an Independent Financial Adviser who confirms that the necessary identity checks have been made, there is no requirement for a company to act further, unless there is any cause for suspicion.

The Guidance Notes issued by the Joint Money Laundering Steering Group, suggest that companies such as ours should request Independent Financial Advisers to provide additional detail such as reference numbers of copy documentation to prove that the IFA has correctly verified the identification and address of the client.

If, as a result of the Discussion Paper, there is a decision reached to take a more active approach to 'Know Your Customer' information, how would this impact on product providers?

It would seem to us to be illogical for a Regulated entity such as a product provider to, effectively, police another directly Regulated entity such as an Independent Financial Adviser.

The other area which does cause some concern in any enhanced programme, would be the question of execution only and direct mail business, which, in an area of enhanced 'Know Your Customer' focus, would by default almost become a suspicious transaction?

Turning back to the questions raised by the Discussion Paper, our observations probably relate specifically to question 4 and question 5.

With regard to question 4, it does appear to us from a product provider point of view that there would certainly be increased costs, with little real benefit, should additional requirement be placed on product providers for business submitted by Independent Financial Advisers. These costs would naturally have to be passed on to our policyholders, with no obvious benefit being derived. We recently carried out a cost benefit analysis relating to the collection of verification documentation from IFAs, as suggested in the Joint Money Laundering Steering Group notes and this did suggest to us an increase in administrative costs of some 5%, with no apparent or obvious benefit.

On the question of the options presented, we would general favour option 1 or option 4, which do at least make clear exactly what is required.

Option 2, would probably lead to unanswered questions, whereas option 3 would continue to create the problem referred to above relating to the difference between

Cont'd./...

9 September, 2003

the FSA Rules and Regulations and the Joint Money Laundering Steering Group's Guidance Notes, which, of course, are derived without any direct consultation or debate.

As stated in your documentation, it is important that firms should know what their Regulatory obligations are and that this requires adequate clarity and completeness in your handbook. It is our feeling that this objective is not currently being met and any forthcoming additional regulation should, in our view, address this issue.

I do hope these comments and observations prove to be of some assistance and await, with interest, the result of your investigations.

Yours sincerely

Chris Woolmer
Compliance Officer

FSA Money Laundering Rules extract:-

When the duty to identify does not apply

3.2.2 **R** The duty in ■ ML 3.1.3 R (1) (Identification of the client: the duty) does not apply if:

(1) the *client* is also a *credit institution* or financial institution covered by the *Money Laundering Directive;* or

(2) the *transaction* is:

(a) a one-off *transaction* with a value of less than euro 15,000; or

(b) is one of a number of *transactions* which are related and, when taken together, have a value of less than euro 15,000; or

(3) with a view to carrying out a one-off *transaction,* the *client* is introduced to the *relevant firm* by a *person* who has given the *relevant firm* a written assurance that in all such cases he obtains and records identification evidence, and:

(a) the *person* who has given the written assurance is covered by the *Money Laundering Directive;* or

(b) The *person* is subject to regulatory oversight exercised by a relevant overseas regulatory authority (see ■ ML 3.2.7 R), and to legislation at least equivalent to that required by the *Money Laundering Directive*; or

(4) the proceeds of a one-off *transaction;*

(a) are to be payable to the *client* but are then to be invested on his behalf;

(b) are to be the subject of a record; and

(c) can thereafter only be reinvested on his behalf or paid directly to him; or

(5) when the *transaction* concerns a *long-term insurance contract:*

(a) taken out in connection with a *pension scheme* relating to the *client's* employment or occupation, if the *policy* contains no surrender clause and cannot be used as security for a loan; or

(b) where the *premium* is a single payment of no more than euro 2,500; or

(c) where the *premium* payments do not exceed euro 1,000 in any calendar year.

Extract from December 2001 Joint Money Laundering Steering Group Guidance Notes

Dealing with agents and introducers regulated in the UK and EU

9. All regulated firms in the UK are bound both by the Regulations and the FSA rules. Regulated firms in other EU Member States will be subject to equivalent requirements under the Money Laundering Directive. As such, they are all required to verify the identity of their customers.

10. Where an investment is to be registered in the name of a regulated firm (e.g. a life assurance company), subject to ensuring that the firm itself is regulated as a financial institution, there is no further requirement to verify either the firm or any underlying customer on whose behalf they are holding the investment.

11. Where the investment is to be held in a nominee name, it is reasonable to apply the same approach, even though nominee companies are not normally regulated entities, provided it can be established that the nominee is a subsidiary of, and therefore controlled by, a financial institution regulated in the UK or EU.

12. Where the customer is introduced by another regulated firm (normally a stockbroker or independent financial adviser) and the investment is to be registered in the customer's own name, there are two ways in which a fund manager may reply (to differing degrees) on the verification that must be carried out by an intermediary regulated in the UK or EU:

    - exemption under Regulation 10(1)(c) and FSA Rule 3.2.2(3) (see paragraphs 13-15 below); or
    - by obtaining a certificate from the IFA that they have verified the identity of an individual customer (see paragraphs 16-18 below).

<u>Exemption under Regulation 10(1)(c)/FSA Rule 3.2.2.(3)</u>

13. As described in paragraphs 4.244 - 4.246, a written undertaking from the introducer (e.g. through signed terms of business with the fund manager) that they will always have verified the identity of the customers they introduce is sufficient to provide an exemption to the fund manager from taking further steps to identify the customer in relation to an individual transaction.

14. The exemption will only apply to the individual "one-off" transactions placed through that IFA.

15. The exemption will <u>not</u> apply to an application for regular savings or regular withdrawal arrangements, which would constitute a business relationship.

Individual certification

16. Except where the exemption described above applies, the fund manager is under an obligation, independent to that of the IFA, to verify the identity of the customer. It has been accepted that, subject to certain conditions, the fund manager is permitted to delegate the verification function to the IFA in order to avoid duplication of the process.

17. The first of those conditions is that the IFA must provide a verification certificate in the form prescribed in Appendix E2(A) to the effect that they have verified identity to the standards required under these Guidance Notes.

18. The second condition is that the verification certificate must be accompanied by certified copies of the documentary evidence obtained by the IFA [or, where the IFA has relied upon the ability to record reference numbers etc in accordance with paragraph 4.58, details of those reference numbers]. This is because the customer's relationship with the manager may continue longer than it does with the IFA and, hence, so will the fund manager's requirements to retain the records of the evidence obtained.

Use of exemptions for one-off transactions

19. Fund managers who intend to take advantage of the exemption for one-off transactions through intermediaries (see paragraphs 13-15 above) or for less than Euro 15,000 (see Appendix F) should first consider the features of their product and service.

20. The exemptions are not available in respect of applications involving regular savings or for regular withdrawal products as these involve establishing "business relationships" within the meaning of the Regulations.

21. Equally important to consider is that using an exemption in no way puts the fund manager in the position of having verified the identity of the customer. Any subsequent transaction will potentially give rise to a need to verify unless a further exemption or concession is available at that time.

22. For example, whether or not the customer will subsequently sell their investment through an intermediary who has provided a general written undertaking of the transaction will fall below the Euro 15,000 threshold will not be within the fund manager's control. It is, therefore, recommended that if a fund manager chooses to make use of one of these exemptions when first dealing with a customer, they do so only where they intend to restrict redemption payments so that they may only be paid direct to the investor in accordance with the provisions detailed under paragraph 4.27.

Alliance Leicester

Alliance & Leicester plc
Customer Services Centre
Narborough Leicester LE19 0AL
Telephone 0116 201 1000 Fax 0116 200 4040
DX 11000 Leicester 14
www.alliance-leicester.co.uk

Mr. Daniel Schonfeld,
Financial Crime Policy,
Prudential Standards Division,
Financial Services Authority,
25 The North Colonnade,
Canary Wharf, London. E14 5HS

Date:	23RD December 03
Our Ref.:	Comp/3500/MJR
Your Ref:	
Direct Dial:	**0116 200 3500**
Direct Fax:	**0116 200 4776**

Dear Mr. Schonfeld,

RESPONSE TO FSA DISCUSSION PAPER 22.

Alliance & Leicester fully supports the FSA's statutory financial crime objective and recognises the need to work in collaboration with a number of public agencies in the fight against financial crime.

We are grateful for the opportunity to respond to the FSA's discussion paper. Our general comments are set out below but in summary, we believe the FSA should pursue the 3rd Option that it outlines in the discussion paper, as we are concerned that unless clear guidance is given on this topic, Know Your Business requirements could be implemented with varying degrees of effectiveness.

In response to the emboldened comments under " Criteria for our decision" and in particular, the following comments:

1) " It would be particularly useful to receive responses on how firms currently match up to these risk management considerations"

We comment:

In 2002 Alliance & Leicester established an Executive governance structure. This has recently been refreshed. We now have three business level steering groups that respectively champion and direct our efforts towards money laundering and fraud prevention. There are two steering groups for our Retail and Wholesale Banking divisions and a Fraud Steering Group. The Retail and Wholesale groups are each chaired by the respective banks' Managing Director's (both of whom are main Group Board directors) and the Fraud Steering Group is chaired by our Director of Credit & Risk. All three groups report to a Financial Crime Steering Group, which includes all four executive directors of our Group Board and which is chaired by

1990006 (3/03)

our Group Chief Executive. All these groups meet monthly and their membership includes the MLRO.

In addition, we have invested heavily in MLRO staffing, staff training and monitoring systems, in addition to the increased executive oversight. Finally, we are about to implement an external software solution to improve checks on PEPs and related individuals on world watch lists.

2) " We would particularly welcome any comments on the actual or potential costs of an active, but risk-based approach to KYC and monitoring."

We comment:

Our automated monitoring solution has cost a capital sum approaching £5 million.

3) " We would particularly welcome comments on whether firms are confident that they understand our regulatory requirements and what we expect of them."

We comment:

We believe that whilst FSA has made its regulatory requirements clear. The current customer review highlighted the challenges of making specific rules, which has strengthened our belief that option 3 is the most appropriate option. Alliance & Leicester believes it would have been unreasonable for the FSA to seek to take enforcement action against a firm's individual progress with the current customer review, but it might be reasonable to enforce against firms who failed subsequently to respond to "Dear Chief Executive letters" which accompany the publication of themed findings.

In response to the specific questions raised by the paper, we comment:

Question 1: "How necessary is the collection of KYC information and an active approach to monitoring in reducing money laundering risk and in meeting legal and regulatory requirements".

An active approach to monitoring is consistent with a risk based approach, which in our view should look to the risks inherent in product lines and distribution channels.

However, the collection of KYC information (in the sense used in this discussion paper) does not necessarily add value to the process. If KYC information had to be an active ingredient in monitoring, it is likely that that would drive firms to invest heavily in neural based monitoring systems. For those firms that have made that investment, the incremental increase in NCIS referrals still remains relatively marginal.

Smaller firms cannot necessarily be expected to invest in such technology and therefore it would appear prudent to communicate expectations of compliance with SYSC rules through the ARROW process, unique to each firm. For smaller firms, this could be evident in industry sector thematic responses published by FSA.

If KYC became "Know Your Customers Business", we are extremely concerned that this requirement could become a "black hole" in terms of cost. "KYB" would require rather more than just the collection of customer data about wealth, source of funds, anticipated account usage and so on (and this could well be intrusive and be misunderstood by customers in the context of some products, such as retail savings); once collected, that data would have to be held on legacy systems, be updated, and be capable of interaction with, or being extracted by, automated monitoring systems. It is doubtful that many firms would have a pre-existing capability to deliver these requirements.

We would not wish our position to be misunderstood: we have shown our commitment to invest in the fight against financial crime and we continue to invest more on training than mere compliance would otherwise require. However, the case for KYB needs to fully be understood before the FSA requires larger banks to invest capital sums in changes to business processes. Questions which we think may assist this debate are set out below:

- Do customers actually provide profile information requested of them?
- Is it accurate?
- How is that verified if a non-credit product is involved?
- How is it used?
- How is it kept up to date?
- Does it lead to an incremental increase in NCIS disclosures?
- Is the quality of such disclosures improved by the collection of KYB, if so, how?
- Do criminals generally provide KYB or not?

The collection of KYB and the sophisticated use of profiling in automated monitoring could be extraordinarily complex, expensive and may not actually lead to significant benefit in the fight against financial crime. This is a clear case for a cost/benefit analysis.

Question 2: How should firms pursue a risk–based approach?

We believe it would be valuable for a definitive position to be agreed on what a "risk based" approach is. The expression is overused and does not appear to have any common touch stone to assess the appropriateness of any particular approach.

Our own narrative approach, presented to our Group Board's Audit & Risk Committee is two dimensional; first an objective analysis by business area/product risk/customer risk; and secondly a subjective analysis by subject i.e. training, monitoring, reporting and so on. This has lead to us exiting or restricting some business lines on the basis of money laundering risk alone.

Question 3: What type of monitoring and reports would be most useful to law enforcement agencies?

Not answered.

Question 4: What are, or maybe, the costs and benefits of KYC and monitoring?

Please see answer 1. If KYC is collected at an individual account level, and that information leads to an NCIS disclosure, which prevented a terrorist outrage or led to the conviction of international drugs traffickers, the benefit is clearly enormous. However, in reality the biggest single output of monitoring is additional NCIS disclosures. Given the large sums that would need to be spent on systems this may mean the unit cost per NCIS disclosure could be disproportionately high.

Question 5: Which option presented do you prefer and why?

For the reasons which we have set out in this letter option 3 is the option we believe should be pursued.

Should you wish to discuss any aspect of this letter we shall be very pleased to do so.

Yours sincerely,

P.P. **Joe Garbutt,**

Head of Group Compliance & MLRO

(signed by Martin Rice, Deputy MLRO, in Mr Garbutt's absence)

472668

11 [illegible] 2003

Arnott Guy & Company

INDEPENDENT INVESTMENT & PENSION CONSULTANTS

Cornerstone House, 4/6 Brassey Avenue, Eastbourne, East Sussex BN22 9QD
Telephone (01323) 520000. Fax (01323) 503306

10 September 2003 BA/HG

Financial Services Authority
25 The North Colonnade
Canary Wharf
London
E14 5HS

Dear Sirs

Re: Discussion Paper 22 Newsletter – Reducing Money Laundering Risk

Being a small practice on the South Coast employing less than 10 people the Money Laundering regulations that have been introduced in recent years have become very onerous on us. I have concluded that generally speaking IFAs are now regarded by the media as people who do not tell the truth and because of this no one is able to use any commonsense.

We have been faced with numerous problems with people living in nursing homes in their 80's and 90's proving ID, ie; they have no passports or driving licences and the only proof of ID that seems to be acceptable within the institutions is to obtain a letter from the nursing home or appropriate solicitor, which is unreasonable. Surely if we have taken sufficient precautions regarding the client's ID then that should be sufficient. Whatever rules and regulations you bring, it in will not deter determined criminals and I would plead that you allow us to use our discretion, especially where the elderly are concerned and are immobile. Indeed, my own staff are being encouraged by Banks and Building Societies to "bend the rules' to prove ID as bank personnel are not willing or able to visit clients' homes/nursing homes to prove identity for their records. I hope these observations are of use to you.

Yours sincerely

Brian Arnott

Partners: Brian R. Arnott Carl R. Guy MSFA

Regulated by The Financial Services Authority

23 February 2004

Mr. Daniel Shonfeld
Financial Crime Policy Unit
Prudential Standards Unit
Financial Services Authority (FSA)
25 The North Colonnade
Canary Wharf
London
E14 5HS

Dear Mr. Shonfeld,

AFB RESPONSE TO FSA DISCUSSION PAPER 22

The Association of Foreign Banks represents over 155 overseas banks doing business in London. AFB provides a forum for the sharing of information on industry issues for the mutual benefit of foreign banks operating in and out of the United Kingdom and makes representation to industry, government, regulatory bodies and other peer group associations to ensure the attainment of good international practice.

AFB is pleased to submit the following response to FSA Discussion Paper 22. We hope that the delay in responding will not prevent these views being taken into account.

Risk Based Approach

We note with interest the considerable emphasis FSA appears to be placing on a risk-based approach to anti-money laundering. AFB fully supports this approach.

We agree that a risk-based approach is not a soft option and in many respects it places additional responsibilities and burdens on the firms themselves. As a result we believe it is equally imperative that FSA at the high level policy echelon as well as within staff levels within surveillance and enforcement fully embraces the approach. By definition, a risk-based approach will vary from one firm to another because firms have different risk profiles. There is no one set approach.

Firms will be hesitant to fully implement a risk-based approach if appropriate assurance is not forthcoming from FSA that they will at all levels accept the firm's risk-based approach. We recognize that firms will have to demonstrate that their management of money laundering prevention is appropriate and they have fully implemented their programme, but if this can be clearly demonstrated there needs to be comfort that FSA will recognize the firm's initiative.

It must also be recognized that a risk-based approach to anti-money laundering is not synonymous to a zero tolerance approach. The critical issue is whether the firm's anti-money laundering systems and procedures are appropriate under the circumstances and are diligently implemented. To retrospectively second guess firms (with the benefit of 20/20 hindsight)

ASSOCIATION OF FOREIGN BANKS
1 Bengal Court, London EC3V 9DD
Telephone: 020 7283 8300 Facsimile: 020 7283 8302 Email: secretariat@foreignbanks.org.uk
www.foreignbanks.org.uk

even where the firm's conduct was reasonable and responsible under the circumstances would clearly undermine firm's willingness to fully embrace the risk-based approach.

Options

You have set out four possible options regarding new provisions in the handbook.

Option 1 We do not think it would be appropriate to make significant changes to the handbook at this time. AFB has not received any significant comments from its members as to deficiencies in the ML sourcebook and we have not noted that FSA has itself signaled there are any significant deficiencies that required attention.

We should note that we have received comments from our members that they would welcome greater certainty about FSA's approach to their rulebook. While some banks would seek to have more detailed rule requirements - to achieve the desired certainty - we believe the broader view from among our members would be to stay with the risk-based approach but to obtain certainty about what the risk-based approach means. This does not mean more detailed rules, just a detailed clarification of FSA's thinking.

Option 2 We equally do not believe there should be new high-level rules on money laundering risk management but there may be something to be said for further guidance on anti-money laundering management.

At the present time there is no 'generally accepted' industry standard for a risk-based approach by banks and/or investment banks. Many commentators have addressed this issue in secondary material, and FSA has itself issued a number of papers that commented on parts of this subject. FSA has also discussed the subject in the context of other regulatory initiatives such as the Arrow programme.

Since there have been various but often inconsistent pronouncements, large and small, it may be appropriate for FSA to initiate a focused discussion on just what it means by a risk-based approach. This would afford an opportunity not only for FSA to bring into a single rationalized discussion paper the various policies and statements it has issued but would give FSA a chance to set out specifics which regulated firms could rely upon. It would also give the industry an opportunity to comment in detail regarding the practical difficulties firms have experienced with such an approach as well as reflecting the areas in which firms are able to effectively implement this approach.

Accordingly, we believe any suggestion that there may be new high-level rules is certainly not warranted at this time but further guidance could be helpful so long as it draws on practical and not just theoretical matters.

Option 3 It would be possible to simply leave the ML sourcebook unchanged and rely on JMLSG Guidance Notes but if FSA were to adopt this approach we strongly urge FSA to unambiguously endorse the Guidance Notes as accepted good practice.

The problem with the present situation is practitioners can not be clear about FSA's position. Firms are not clear what it means when FSA says it will 'have regard' to whether a firm has followed relevant provisions of the Notes when FSA considers whether to initiate disciplinary action in respect of a breach of its rules. We have received many comments from our members that they simply are unable to assess what FSA means by this statement.

Option 4 There is much to be said for this option - to make no settled decision and review the position again in say two years. On balance, we believe this is the position which would be most acceptable to our members.

The UK Money Laundering Regulations have just been promulgated and it will take some time to determine just what regulatory response, if any, will be required. A revised version of the JMLSG Guidance Notes has also just been published and firms will similarly require some time to become accustomed to the revised notes. And above all, the 3rd Money Laundering Directive is slowly yet inexorably proceeding through the Brussels legislative process. It would be entirely inappropriate to embark on a major initiative here in the UK until the final shape of the directive has been agreed.

As a result we certainly support a 'wait and see' approach.

We would be pleased to discuss the foregoing with you in further detail if you wish.

Yours sincerely,

James Tree
Director & Secretary

The Association of Friendly Societies

10/13 Lovat Lane London EC3R 8DT
phone: 0207 397 9550 fax: 0207 397 9551 e-mail: info@afs.org.uk
Doug Thow Secretary

Mr D Shonfeld
Financial Crime Policy Unit
Prudential Standards Division
The Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

20 January 2004

Dear Mr Shonfeld

DP 22: Reducing money laundering risk

I refer to the above discussion paper and have pleasure in submitting the response of the AFS.

The Association of Friendly Societies (AFS) is the representative body for Friendly Societies. The societies for which it speaks exemplify the huge diversity of the Friendly Society movement, covering numerous different types of society which offer their members a wide range of insurance, savings and other products. They have over 6 million members and total funds under management are around £15 billion. Friendly Society members come from all walks of life, including those of modest means not otherwise reached by financial services providers as well as substantial investors.

We have given serious consideration to the discussion paper over the past months taking into account not only its contents but also recent various legal and regulatory developments elsewhere affecting the general operation of money laundering controls in the financial services industry. In this context, the form that controls should take in the future is of relevance to all sectors of the industry and of equal application, at least in principle, to all regulated firms. Thus the options set out in your paper have helped to focus this debate.

On balance, and after having weighed up the pros and cons carefully, we believe that the fourth option of not taking any decision now but to review the position of laying down suitable rules and guidance in say two years time represents the most pragmatic industry-wide solution. We take this view largely because of the recent and on-going events elsewhere and in particular the Proceeds of Crime Act 2002 (POCA), the delayed issue of the Joint Money Laundering Steering Group's (JMLSG) Guidance Notes for 2003 and their scheduled radical revision in 2004. We share the views expressed in the discussion paper that longer experience in respect of POCA is desirable and believe further that the prospective revision of the Guidance Notes in 2004 should help to focus more clearly on the need for flexible controls and standards having regard both to the type of customer and type of firm.

Such a deferment would also allow any other relevant issues that may arise to be properly assessed and avoid having to make hasty or ad hoc changes to specific or high level rules were they to be introduced at this time if either the first or second option was to be adopted. On the other hand sole reliance on Guidance Notes at this stage, as envisaged under the third option, would also be inappropriate because of the fundamental revision exercise being carried out this year.

We hope therefore that the FSA will recognise the merit in delaying action on a universal basis whilst these current and on-going events are given sufficient time to reach a natural conclusion. In this context, the AFS is playing an active part in the production of revised guidance notes and in defining the operational practices and procedures suited to friendly societies.

We also have the following general but brief comments to make on the individual questions posed in the paper:-

1. How necessary is the collection of KYC information and an active approach to monitoring in reducing money laundering risk and in meeting legal and regulatory obligations?

Detailed know your customer information that can be independently verified can be an effective tool against money laundering although there would be additional costs to obtaining, storing and verifying this information.

However, should a firm be required to obtain information that cannot be verified, this information would always appear to justify the nature of the relationship.

Depending upon the nature of the relationship, there will be varying degrees of ease in obtaining any such information required. Obviously there are Data Protection Act issues concerning the amount and nature of the information that we may be required to obtain. A requirement to obtain specific information about a customer before establishing a business relationship may turn off a significant proportion of potential customers

2. *How should firms pursue a risk based approach to anti money laundering ?*

A firm needs to review the products and services it offers and assess the risk of these products and services being used by money launderers and put into place appropriate controls. The risk assessment and controls put in place need to be reviewed on a regular basis to ensure that they are still fit for purpose with specific reviews being triggers by certain events such as

- changes in the legislation, guidance notes and/or FSA Rules
- changes in operating procedures

The risk based approach and the review process should be documented.

3. *What type of monitoring (and reports) would be most useful to law enforcement agencies ?*

This question is best left to the law enforcement agencies.

4. *What are, or may be, the costs and benefits of KYC and monitoring ?*

It is difficult at this stage to evaluate the costs and benefits because they will inevitably vary between different types of firms and indeed different types of friendly societies. This wide fluctuation was a critical factor in the FSA's decision not to proceed with an industry-wide review of customer re-verification last year.

On a general basis, the benefits of having an efficient and effective KYC process and appropriate monitoring systems should be that the opportunities for money launderers to use the UK financial services industry are significantly reduced. However we need to ensure that the additional controls put in place to make these reductions are proportionate in both operational and cost terms and not to the detriment of the honest customers.

We hope that our views and comments are useful to you.

Yours sincerely

D A R Thow

ASSOCIATION OF SOLICITOR INVESTMENT MANAGERS
RIVERSIDE HOUSE, RIVER LAWN ROAD, TONBRIDGE, KENT TN9 1EP
TEL: (01732) 783549 FAX: (01732) 362626 EMAIL: admin@asim.org.uk

Mr Daniel Shonfield,
Financial Crime Policy Unit,
Prudential Standards Division
The Financial Services Authority
25 The North Colonnade
Canary Wharf
LONDON E14 5HS

By e-mail to DP22@sa.gov.uk

31January 2004

Dear Mr Shonfield,

DP22 –Reducing money laundering risk – Know Your Customer and anti money laundering monitoring

ASIM, the Association of Solicitor Investment Managers, is a trade association representing more than 30 solicitors' firms throughout England and Scotland, which provide integrated legal and investment management services to an estimated 40,000 private clients and trustees. We estimate that funds under management by ASIM firms now total over £2 billion. While discretionary portfolio management is the principal investment service which ASIM firms provide to their clients, most will also carry out a broad range of other regulated activities including acting as an ISA manager, providing overall financial advice including advice on pensions and the safekeeping and administration of investments.

We have already commented, in recent responses, that we are overwhelmed by the volume of consultation papers. We would urge the FSA to consider reducing the number of consultations or at least ensuring that we do not have to respond to several consultation papers within a matter of days. The cost and burden of compliance and keeping up to date with changes to the FSA's rules is significant, onerous and seems to be increasing. A period of consolidation would be welcome.

We welcome the opportunity to respond to this discussion paper because some firms of solicitors conduct mainstream investment business and are subject to the Money Laundering Sourcebook. For those firms, any changes in the FSA's rules will be directly relevant. Secondly, we are interested in contributing to the debate on Know your Client issues from the broader perspective, both for the legal profession and for society as a whole.

It may be helpful to explain that, in addition to my being an ASIM Director, I am also a member of the Law Society's Money Laundering Taskforce. The Taskforce has been heavily involved in commenting on the Regulations during the main consultation and subsequently have been involved in detailed discussions with the Treasury.

General comments

1. We are concerned that the burdens being placed on solicitors and others are being seen to be excessive and out of proportion with the potential benefit. Solicitors and other regulated firms are concerned that the UK regime is the most onerous in Europe and goes far further than was required by the Second Money Laundering Directive. This raises important competition concerns which could damage the standing of the City of London.

2. Regulated firms already face significant new requirements in the field of money laundering. The introduction of part 7 of the Proceeds of Crime Act 2002 in February 2003 is having an enormous impact on regulated firms, in relation to training, understanding the new legislation and in particular the new "objective" test. In addition, firms will have to consider the new Money Laundering Regulations 2003 very carefully to ensure that they implement any necessary changes to their systems, controls and procedures. Firms will have to ensure compliance with any changes in the FSA's rules as well.

3. In the Law Society’s response to CP46, concern was expressed that the introduction of the FSA’s Sourcebook would create a separate but parallel regime for firms to contend with. Problems will arise if there are any inconsistencies between the two regimes. The result would be that firms comply with the Money Laundering Regulations and Law Society Guidance but could still be disciplined by the FSA for breaching the Money Laundering Sourcebook. This danger was particularly acute if the FSA's proposed Rules for client verification had been implemented. Similar concern were raised by others. This led to the FSA concluding:

   > "..the overriding message of the concerns was that, by including in our Rules the proposed amount and nature of the detail about identification methods, we were creating confusion and risk as to the respective roles of our Rules and the JMLSG Guidance Notes which was contrary to a stated aim of CP46. "

4. The FSA decided not to proceed with detailed verification rules and commented that the JMLSG Guidance Notes were a key factor in this decision. We believe that the same logic applies equally to the proposals in relation to KYC.

5. The Law Society has now published its own detailed Guidance, a copy of which I understand has been forwarded by the Law Society. This includes detailed guidance on client verification and a risk based approach. We are concerned that this guidance will be undermined by the introduction of any FSA Rules on KYC. We are also concerned that a risk based approach should be taken and that too prescriptive a requirement will be over burdensome and disproportionate for the potential benefit. It is important that firms make a proper assessment of a case rather than relying on a tick box or check list approach which may result in their overlooking a vital piece of information.

6. We are concerned at the "one size fits all approach" and believe the money laundering risks facing solicitors are quite different from, say, a bank. Solicitors often have longstanding relationships with their clients and pride themselves in giving commercial advice and thus understanding their clients’ business. In most cases, solicitors meet with their clients on a regular basis during the course of their relationship. Moreover, professional conduct obligations and duties in contract and tort require solicitors to be familiar with their client's affairs in order to provide services competently and professionally.

7. The problems cannot be overcome by limiting the scope of any KYC requirement. A firm of solicitors offering investment management services will often attract clients from the private client department. That private client department will have substantial information about the client from acting on the case, for example, the trust lawyer will know why the trust was set up, who the trustees are, where the money has come from etc. The level of information available to the trust lawyer will be completely different to the information available to a stockbroker meeting a client for the first time.

8. We feel that the issues raised in the discussion paper are very useful as they are likely to help firms to assess the risks within their own business.

We hope that our comments will be helpful to the FSA and are, of course, happy to discuss the DP22 paper with you further.

Yours sincerely

Alison Matthews
Director
Association of Solicitor Investment Managers

Detailed response

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

9. In our view, the existing regulatory requirements would appear to be sufficient. Firms who are subject to the FSA's rules and the Money Laundering Regulations will have to satisfy the requirement to identify their clients.

10. Over and above the identification requirements, firms should be able to make the assessment themselves as to what types of KYC may be required in what circumstances. We do not believe that rules on KYC are necessary for the reasons set out in paragraph 6 above.

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

11. Firstly, we welcome the idea of a risk based approach, as this seems far more sensible than the current position where, for example, verification is sought in all circumstances, regardless of whether there is an actual requirement or whether there is any risk of money laundering. As to how firms should pursue a risk based approach, this will depend on the individual sector and guidance on the issues to consider would no doubt be helpful. Firms will need to assess the impact and costs of monitoring for their firm.

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

12. The section in the discussion paper considers more what types of monitoring are available to firms and it is quite difficult to answer this question as we are not clear as to the FSA's thinking behind the question. The issues about usefulness of reports etc to law enforcement are perhaps issues to be considered in terms of the overall UK strategy to combat money laundering. The KPMG review, of course, considered the issues in relation to the SAR process and the Government Taskforce is now taking those issues forward. It is important that the relevant bodies are clear as to their role in the regulatory regime.

13. In any event, this question is more one for law enforcement, although it is important for the credibility of the whole regime that firms are not obliged to over report. If a firm is concerned about a particular transaction, a report will be made to NCIS, who will then pass the information to the law enforcement agencies.

14. It is important that a balanced and proportionate view is taken so that the system is not entirely driven by one area's needs or desires but instead that the system is driven by the overall benefit to society, acknowledging the reasonable rights of the individual in accordance with the Human Rights Act 1998.

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

15. It is difficult to answer this question as the costs and benefits will vary according to firms and according to sectors. A prescriptive approach in relation to KYC and monitoring is likely to result in unnecessary costs for the financial sector. There will then be a knock on impact to customers and this may not have any real benefit. We agree with the FSA that firms' information demands need to be proportionate, appropriate and discriminating, and capable of being justified to customers. We are concerned that a prescriptive approach would have a detrimental effect on the UK's competitive position in providing financial services.

Q5. Which options presented to do you prefer and why?

16. Option 4 – We believe that to impose further requirements on the financial sector at the moment would be unreasonable and could result in the imposition of requirements that needed to be changed in the light of experience.

17. The Proceeds of Crime Act should be given time to bed in. There are many legal issues and questions arising from the new legislation. In addition, firms will have to implement any changes required by the Money Laundering Regulations 2003. As the FSA comments, there may also be changes to the SAR process in the light of the KPMG review. We feel that firms should be given the time to consolidate and absorb the recent and prospective changes.

Response from Aviva plc to Discussion Paper 22

Reducing Money Laundering Risk -
Know Your Customer and anti money laundering monitoring.

Introduction.

Aviva welcomes the opportunity to respond and enter the debate on KYC and anti money laundering monitoring. Aviva, through this response, other activities and representation (e.g. on the ABI money laundering committee) is extremely keen to be active in all initiatives that will assist in the ultimate aim of reducing financial crime.

This response is given in the context of the wider considerations and other current activity in the area of 'reducing money laundering risk' in the UK. These include what the UK plc 'perceived' strategies may be, the 3rd EU Directive, 2003 and 2004 JMLSG guidance notes and the KPMG review of the SAR regime.

Additionally the response is mindful, as set out in the paper, of the current laws, regulations and other material (Wolfsberg, Basel, FATF etc) that a company such as Aviva does and/or may take into account when considering its global approach to anti money laundering.

This response is an Aviva response and takes account of the very complex and diverse nature of the Group that now operates in some 28 different jurisdictions. The Group is complex also in that it operates Life business, general insurance and fund management (retail and institutional)

This response (and we hope FSA subsequent considerations) also takes note of the fact that the insurance sector is perceived as a low risk area for money laundering. This particular point highlights the potential difficulty of a 'one rule fits all' type of approach to KYC and monitoring along with the historic view that Guidance Notes have been strongly influenced by the banking sector (possibly correctly given the increased level of risk).

The response is structured by answering the questions posed in the paper and then setting out the preferred option and the reasons why.

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

The answer will be different for different sectors in the financial services industry. For example in Aviva (insurance) given the type of products available, how they are 'distributed', and the source of how the products are funded, for the vast majority of customers a fully enhanced KYC would not, necessarily, in itself reduce the money laundering risk or enhance reporting of 'suspicious activity'. This is because the vast majority of products sold are of low value, with regular premiums paid, where the business is introduced via regulated firms (IFAs) and the funds are received through 'high street' banks (again regulated).

Indeed it could be argued that the above meets most of the generally perceived requirements of KYC as regards source of funds. In respect of understanding the reason behind the opening of a relationship with a customer this is 'implicit' in the product itself (e.g. term assurance, pension plans, long term savings).

Aviva accepts that there are higher risk products (and work continues with the ABI in attempting to categorise these in the insurance sector) where some form of enhanced KYC might be beneficial. However, experience suggests that these are exactly the same types of cases where there are Conduct of Business (COB) requirements. The real issue is therefore who should be responsible for the collection, retention and subsequent disclosure of such information when there are possible reporting requirements.

There is potential for real customer dissatisfaction if they continuously have to provide the same detailed information to different service providers. (As an aside I found this particularly frustrating as a 'customer' when I returned to the UK recently after 10 years overseas where, despite being the same institution with whom I had been with for 25 years, I was required to provide detailed ID evidence to numerous providers who were receiving funds from the one bank account who already held all the relevant data).

The final difficulty in the insurance sector, given the 'non regular' contact with customers (albeit ironically regular transaction behaviour) is ensuring any KYC data is kept 'up to date'. This would have to be as reasonable as practicable and based on actual contact or unusual event occurrence rather than on a periodic basis.

An added argument to a reduced focus on this area of ML control (other than where the risk would necessitate enhanced KYC) is the increase in identity theft and the fact that the truly dedicated launderer/criminal will be aware of the controls on ID./KYC and seek methods to circumvent them.

It must also be recognised that the vast majority of insurance products that would be of benefit to a criminal/launderer require a 'pay out' at the end of the term (or earlier) this provides another opportunity (and is much used) to obtain information.

Our current experience from law enforcement suggests that KYC/ID information is not a critical element in their judgement as to whether to adopt a SAR for investigation as they are in a position to obtain this through their normal investigative methods. What they do find useful is information that will enable them to track/audit trail funds.

Question 1, as it stands, combines KYC and monitoring. It is our belief these are distinct issues and can be separated (given the KYC arguments above) as we fully accept that a crucial element to good reporting, and hopefully a reduction in financial crime, is an efficient monitoring regime that, in turn, results in quality SARs for NCIS.

Again these have to be industry specific and even company specific and, in our case, business unit specific. As it correctly pointed out this does not necessarily mean that they have to be automated either.

Aviva, in meeting the high level requirements to assess ML risk, requires all its businesses, through Group Standards, to apply enhanced KYC requirements on high risk business (guidance given), to consider systems of monitoring (including automated) and to have an efficient reporting regime as a result.

The issue is the type of monitoring. Our submission is that a rule would be difficult to enforce. Firms should consider what monitoring may be required (e.g. rule based, terrorist lists only, automated, etc.) as part of their overall AML risk assessment and then implement accordingly. This does mean an element of subjectivity, as does the whole area of financial crime, and the danger with having too many rules is that it creates an increased ‘tick box’ approach rather than clearly thought out and justified reasoning for applicable and proportionate approaches to mitigate money laundering risk.

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

The approach is to consider the range of issues/risks/threats that manifest themselves into an overall risk matrix. Aviva’s approach at the centre has been to assimilate these perceived risks into a set of high level anti money laundering principles that pertain to each significant ML issue/risk and provide a minimum set of standards for each of those principles to be used to mitigate the risks. These principles in Aviva are:-

The need for documented procedures at local level;
Responsibility and accountability;
ID and KYC;
Reporting Internally;
Reporting Externally;
Training and awareness;
Retention of records; and
Supporting law enforcement/government initiatives.

The standards that accompany these principles are mandatory for all businesses with some flexibility given to business units allowing them to mitigate any of their own specific risks but using a standard framework. i.e. the same questions are asked but there may be different answers given the varied risks in the different businesses and varied locations.

In some areas we are able to be more prescriptive or provide better guidance given the information available to us (laws, regulations, guidance notes). The point is that in the areas of KYC and monitoring, given the FSA overall requirement for adequate systems and controls, we already see KYC and monitoring as integral to this and take account of them in our standards.

Critical to the Aviva approach is the need to ensure real accountability and responsibility at the business unit end and not just with an approved person (MLRO). The aim of Aviva (and the recent training programme is symbolic of this) is to have “anti money laundering = business as usual”.

Training and awareness is one area where more anecdotal information would be welcome in explaining the types of money laundering typologies and how criminals look to circumvent controls. Current examples are often vague and given the relatively small amount of insurance examples it can be difficult to persuade managers of the potential risks and the need for continued vigilance.

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

Law enforcement agencies should be best able to respond, however Aviva's experience to date is that they appear to be more interested in the factual data and are more than happy with one or two lines on the reasons for the suspicion. Other experience would imply that, of course, if a firm is able to prepare an actual picture of clear criminal activity, or money laundering, this would be the real optimum. However a firm is not employed in this regard or required to do this, indeed, there are potential problems with this more proactive investigative approach by firms.

Another consideration to this question is what is the UK plc strategy? Is it to try and stop criminals from having any access to financial services? Or is it to have financial services do all it can to spot and report suspicions? Or is it a combination of the two? Or is it something entirely different?

Given that PoCA has no de minimus value there is a perception that the objective is to attempt to identify all criminal assets and/or activity thus allowing UK plc to do all it can to confiscate those assets. This is an objective Aviva would applaud particularly in the area of insurance fraud.

Aviva is extremely keen to do everything it can to assist 'UK plc' in meeting its financial crime goals – but it needs to understand exactly what these are. At present Aviva believes that it does this through an effective, thought out, anti money laundering regime and, in particular, effective reporting procedures (even from the general insurance sector) rather than just a rudimentary 'tick box' approach to ID and KYC.

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

As mentioned above the costs have to be proportionate to the perceived risk. The insurance/fund management sector already has COB requirements that are most likely in the product area where enhanced KYC could be seen as a useful mitigant to money laundering risk. The real issue is who should take, retain and provide that information. There will be disproportionate cost and increased customer dissatisfaction if there is vast duplication of effort. Again by way of illustration is it really necessary for Aviva to take KYC (and indeed ID?) information if there is COB information available and/or where the funds, of regular premiums, are received from a regulated entity. One further consideration here is the fact that in a significant number of cases the investments are 'one-off' with minimal contact with the customer other than periodic statements. As such the ability to regularly update KYC (without significant cost) is difficult and could be disproportionate to the perceived risk.

Lastly mention should be made on General Insurance where the costs of full blown KYC would be cost prohibitive given the perceived risk. Aviva has (and this applies also to the Life business) the ability, where an unusual event occurs, to conduct KYC prior to the release of funds. I.e. mitigating controls on 'exit'. This is performed on a regular basis and has been successful in identifying possible SARs.

The costs potentially involved include:-

Collecting the information and retaining it;
Ensuring compliance with data protection;
Training of staff and intermediaries;
Changing processes and procedures; and
Changing literature/application forms.

The benefits to KYC are possible marketing initiatives and in the general insurance area, a possible assistance in the reduction of fraud.

The costs of transaction monitoring would include:-

Manpower (IT people to change systems) NB. The insurance sector really only sees a rule based system as being appropriate;
Software licences;
Investigation time/resource in dealing with ‘exceptions’; and
Set up costs.

The perceived benefits again only relate to possible marketing initiatives, some improved fraud prevention/detection (albeit much is already done in this area) and a reputational/regulatory protection of the firm’s brand.

Aviva would be happy take on such costs (and already does so in a number of areas) provided discretion is given to firms regarding the risk involved and the description of ‘transaction’. In reality given the products involved, and how customers interact, any monitoring would be more than likely be a rules based system to provide exceptions on certain event occurring rather than a ‘full blown’ intelligent system such as search space. Aviva, again, is continuously considering how to improve this.

To really sell the argument to industry there has to be real evidence of the value in performing these tasks and incurring such costs particularly in the area of a blanket approach to KYC where already duplication is evident.

The value of monitoring to produce reports is probably easier to prove (albeit even more evidence to this would assist for example by more anecdotal material from NCIS or the ARA).

By way of example it may be worth some analysis with those large retail banks that have introduced automated systems. A figure suggested is that of all alerts only some 7% actually result in SARs. Of interest would be to see how many of this 7% would have created a SAR in any event through normal human ‘nose’.

Within Aviva we consider one aspect of our monitoring is the ‘59,000 eyes and ears’ of the employees and that any monitoring ‘system’ is only an aid to supplement those ‘more intelligent’ human practices.

It is not yet proven how further regulation, rules or guidance will assist.

By way of further argument is that we have now had some 10 years of law and regulation on ID and systems and controls. Has this reduced money laundering or the use of financial services by criminals – indeed is that the end game? Has it brought more criminals to court or have more criminal assets been confiscated as a result of the introduction of these rules and the significant costs to the industry?

This reverts to a better understanding of what the UK plc strategy is and what are the performance measures? If industry understands what this is then they will be better able and more receptive to possible costs required to support that strategy.

The current perception is that of a rule book approach to ID/KYC where transgressors are punished (even where it is published that there was no money laundering). This perception has bred, in some areas, a culture where compliance with ID rules is the ‘raison d’etre’ rather than a thoughtful approach to countering the criminals’ use of the financial services sector. In other words a fear culture is being created rather than a collaborative regime to try and deal with financial crime in all its varying facets.

Q5. Which options presented do you prefer and why?

Taking account of the answers given above and the current initiatives on anti money laundering Aviva's position is to favour option 4, to do nothing at this time and review the matter again in, say, 2 years time.

The specific reasons are as follows:-

- Current ongoing initiatives, 3rd EU directive, JMLSG guidance notes, SAR review. These may well require firms to incur changes in procedures and processes. To add more at this time would, in our submission, be too much. These should be given time to settle in before any further rules or guidance are considered.

- Aviva believes that it already considers the issues of KYC and monitoring seriously in its money laundering risk assessments. This is probably the case for the majority of major firms and perhaps the focus of regulatory attention should be on those that currently do not – especially in the area of reporting suspicious activity.

- If the FSA already has concerns with firms then perhaps these concerns should be dealt with and corrected first rather than embark on new rules.

- The current high level rule on mitigating ML risk should already require firms to justify what they do on KYC and monitoring. (as set out in Annex 1(b) and paragraphs 3.4 to 3.6 of DP 22). Aviva has accepted this and therefore has tackled KYC and monitoring in its risk assessment and subsequent AML standards.

- Additional rules and probable costs in these areas for some firms now would not bring a noticeable improvement to the overall objective in financial crime reduction.

- The real way forward is for better collaboration between the various stakeholders on how best to target criminals using the financial services sector.

Stuart Hammond
Group Money Laundering Reporting Officer
Aviva plc

Group Money
Laundering Prevention
St Swithins House
11/12 St Swithins Lane
London EC4N 8AS

Tel : 020 7068 1698
Fax : 020 7068 1446

4th February 2004

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

BARCLAYS

Dear Mr Shonfeld

Re: Barclays' response to FSA Discussion Paper 22 'Reducing Money Laundering Risk – Know Your Customer and Anti-Money Laundering Monitoring

Barclays welcomes several of the statements made in the FSA's Discussion Paper 22, particularly the continuing embedding of the risk-based approach. It is also refreshing to see that the distinction between identification and verification and truly knowing and understanding your customers has been made. We are greatly encouraged by this, particularly as it is not reflected within legislation.

We have worked closely with and contributed to the industry response from the BBA and support the views and opinions expressed in that document. In addition, however we do have further comments, based on our own operational experience that we wish to have considered below:

Active approach to identification and monitoring:

Para 1.3
We consider that it would prove difficult or impossible for institutions, particularly smaller ones, to meet their high-level regulatory obligations without some form of mandated KYC or monitoring framework, particularly in relation to sanctions. Whilst we fully support an active approach, and have set up a specific unit to research trends so that we are pro-active in this field, criminal methods change and evolve, and the framework can only be effective if it is supported by timely and appropriate feedback from law enforcement. We believe that this is work that could be effectively done in partnership with the various law enforcement agencies to help focus the analysis and ensure more effective reporting.

Para 1.6
With the greater emphasis on a risk-based approach to identification and monitoring of customers and trends we now need to look at alternative ways to do this work and in a manner that blends security and commercial flexibility. We need to look beyond the tick–box approach that involves reliance on paper documentation, that has a high probability of forgery, to electronic methods that will draw together a myriad of information to identify the customer accompanied with a robust system of monitoring. Whilst it is unrealistic to expect official endorsement of particular products, formal acknowledgement of their use and guidance on the way they can be calibrated and used would be welcomed. We live in an increasing world of remote banking service provision and verification has to recognise these changes if the market is to be fully served from within the UK.

Risk-based approach:

Para 2.9
We welcome the FSA's continued commitment to the risk-based approach, which can provide benefits due to a targeted approach to identification and monitoring of customers and accounts.

A risk-based assessment to the product, customer and jurisdiction is a welcome inclusion. We would like to see a specific money laundering risk-assessment framework be put forward or at the very least, guidance on how this work should be undertaken. This would assess the product and take on procedures to determine how a criminal might use it for money laundering purposes and to ensure that controls are implemented to mitigate the particular risk.

It should be noted, however, that we should not assume that criminal methods and typologies would remain the same. There will always be a requirement for institutions to re-visit these assumptions in order to ensure that the assessment truly reflects the known risk.

Know Your Customer:

Para 3.14
It has already been stated that we welcome a risk-based approach to identification and know your customer (monitoring). Our structure and procedures mean that we would require a minimum standard identification throughout the Group for new to bank customers, with additional layers placed on top based on the risk assessment of the product or service being offered. This would assist with the customer experience and ensure that migration between products and Group businesses are managed. It would also prevent criminals using products that might require minimal identification to obtain 'higher risk' products in the future.

As mentioned above (para1.6), verifying the data provided by applicants is difficult and Barclays would welcome regulatory clarity about the position of verification products currently offered by credit reference agencies. This would also assist in a 'level playing field' as different institutions can implement a risk-based approach whilst utilising electronic verification and the customer experience will remain consistent when using different financial institutions.

Para 3.15
We agree with the concept of this statement. However, if experience dictates that certain data fields are required then these should be mandated so that effective KYC is driven by need rather than by perceived customer willingness to provide information.

Para 3.16
It is encouraging to see the appreciation of the fact that customers use a variety of service providers for their financial needs. This does make the identification of suspicious transactions and truly "knowing your customer" more difficult. The more a customer spreads their business around niche or specialist providers, the more difficult it becomes to get an overall picture of their "usual" activity.

Para 3.18
This is a crucial statement. It acknowledges that it is simply not practical to expect institutions to be able to update know your customer information regularly. In the increasing world of remote banking customers who rarely contact branches, seeking remote reviews is difficult and expensive. The extent to which reviews and updates are conducted should be linked to a risk-based approach and clearly documented.

Anti-Money Laundering Monitoring:

Para 4.8
Whilst you are correct that all these factors have contributed to ensuring that institutions are focussing on anti-money laundering, there is a distinct difference between terrorist financing and sanctions. Sanctions are a useful way of combating the movement of funds, whether suspected terrorist funds or payments in breach of economic embargoes, to particular jurisdictions. Terrorist funding is about the use of of fraudulent loans and credit facilities, purchase or sale of goods of value to fund operational or strategic activity and it is essential that intelligence about these trends and developments are brought to the attention of institutions.

Para 4.11
Your statement that insitutions are best placed to identify unusual transactions on account is correct. However, the ability to determine which transactions are suspicious is dependent on timely feed back and the amount or breadth of customer data held by individual institutions.

Para 4.13
We are assuming that this statement concerns threshold reporting. There are issues with instigating such a system, not least that the legislation and Regulations do not accommodate it. The lower the level that is set the greater number of transactions that will be captured. It can also result in staff regarding low value transactions as being less suspicious. It is probable that there is insufficient evidence to support this supposition and it is also possible that once criminals become aware of these values (and there can be no doubt that they will) they will split transactions to get underneath these report levels.

Para 4.30
It does seem likely that automated systems will always have a lower alert to report ratio than manual staff generated reports but that is probably inevitable. It is safe to say that functionality and capacity will undoubtedly increase but it is in the area of automated reporting where it is essential that law enforcement, and NCIS in particular, work with the financial sector to produce useful and informed reporting parameters.

Unless focused, results based, intelligence is provided in a format that allows rules based reporting to be refined, automated systems will fail to progress. There is an added danger that staff in institutions that have introduced such systems, start to rely on them and allow their own suspicion to be over-ridden.

Options and questions:

As we have previously mentioned we have contributed to the joint BBA response and as such fully agree with their comments in this regard and there is nothing further that we would wish to add.

Yours sincerely

Despina Roberts
Policy Manager

Berwin Dolphin Securities

Q1 = We recognise that the collection of KYC information is the starting point in any client relationship and an essential part of an active approach to the monitoring process. Basic steps to identify and assess the risk of their client base are fundemental, if firms are to be compliant with the Rules and meet their regulatory and legal obligations.

It is arguable whether the production of utility bills and passports actually reduce the risk of money laundering or simply make life more difficult for the criminal. Data collection and the requirement to establish source of funds, identity of third party payments etc. can deter crime, making it increasly difficult for unethical entities to pass or receive funds to or from unverified entities. If firms are to comply with anti-money laundering legislation and the POCA they must ensure that all relevant facts are current and available.
Q2 = In order to undertake a risk-based approach to anti-money laundering, firms must understand their client's requirement and needs. Existing information collected since the introduction of money laundering regulations is useful but not sufficient. Firms will need to look at their existing clients and classify them according to the perceived risk into high, medium and low risk categories. The classification would need to take into account not only source of funds,trading levels, transaction size, corporate structure but also geographical areas and countries of incorporation. Setting these parameters would initially be difficult to determine for firms with a large and diverse client base. In addition the parameters would need to be constanly reviewed for any changes in the firms normal business stance.

Training and education of staff and in some instances the assistance of outside agencies would be essential. Firms would undoubtedly have a problem with resource and cost. Staff dedicated to a risk-based monitoring programme would be required to constantly review and monitor any parameters set.
Q3 = It is difficult to assess the type of monitoring or reports which would be required, as this would depend on the individual firm and their business type, however we believe that the following would be useful to both regulators and law enforcement agencies in respect of monitoring and production of reports:-
1) Hard copy and electronically held KYC information. Including addition verification regarding source of unds/beneficiaries and any connected parties or entities.
2) Client ledger reports including dealing, income and deposit ledgers (all cash and stock movements) 3)Frequency, size and destination of withdrawals.
4) Frequency size and source of deposits received.
5) Valuation listings including acquisitions and disposals.
6) Transaction monitoring reports both for individual clients and for specific client groups.
7) Monitoring of accounts based or incorporated in NCCT countries as per FATF listing. 8)Monitoring of accounts based or incorporated in high risk countries recently removed from the NCCT list as per FATF listing ie Russia.
9) Account executive risk assessment monitoring.
10) Product analysisand client use of products ie. trading patterns Q4 = The costs most probably outweigh the benefits. The main benefit is of utmost importance to regulated firms, firms undertaking KYC and monitoring are eager to keep their reputations in tact. Compliance with the law and their regulators, can ensure avoidance of reputational risk and the possibility of heavy fines. Information collected could also be used to the advantage of the firm, marketing for instance.

Staffing resource and training would be a major cost issue, staff training being a regulatory requirement. Many firms may need to recruit dedicated qualified staff with specialised knowledge, outside of their current monitoring teams.

Although not currently mandatory, the decision or cost analysis of whether to implement automated systems will pose a problem for many firms. Small firms may be financially disadvantaged
Q5 = Our preferred option would be option 2 "Include new high-level rules and guidance, or both, on money laundering risk management" provided as is suggested, the obligation would be risk-based due to the "reasonable steps" qualification. This would allow firms to take a flexible approach to build their own systems and procedures establishing a risk-based programme, depending on the diversity of their client base. Making it a requirement for firms to document its systems and procedures of how it identifies, monitors and controls it client base in relation to the anti-money laundering requirement.

The need to verify clients over and above the identification requirement is already a necessity for firms who wish to remain compliant with POCA and the SARs disclosure requirement. We believe that the majority of firms currently take a responsible approach to anti-money laundering and KYC. The JMLSG guidance notes are a useful tool for regulated firms, however many firms are concerned that too much emphasis is placed on the guidance notes and that they become viewed as the Rule rather than simply guidance. Firms are also concerned that they may mis-interpret the JMLSG notes and fall foul of their regulatory body or law enforcement agencies. It is also a concern that any mis-interpretation can lead to confusion between firms when passing verification documents.

Past guidance notes issued by JMLSG were drafted in the main by BBA with a bias towards the banking business. The introduction of trade bodies such as APCIMS onto the committee will hopefully give a broader interpretation for investment firms and if new high-level rules/guidance with regard to anti-money laundering risk management are laid down, then this may level the playing field.
Consent = Yes

Remote Host: 193.130.174.202
Remote IP: 193.130.174.202
User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Referer: http://www.fsa.gov.uk/pubs/discussion/dp22_response.html

.

30 January 2004

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

Dear Daniel

FSA Discussion Paper 22: Reducing Money Laundering Risk

The Bristol Money Laundering Forum (BMLF) welcomes the opportunity to comment on this discussion paper. We are keen to contribute to a fundamental review of the regulation of anti-money laundering (AML) by the FSA. We welcome the FSA's willingness to engage in dialogue with the Industry and interested parties on the key issues.

About the Bristol Money Laundering Forum

The BMLF is a recently formed group of AML professionals. The BMLF aims to provide an opportunity for senior operational AML personnel to:

- Discuss current issues and share best practice.
- Maintain and enhance contact with local fellow AML professionals based in the Southwest.
- Respond to current consultation and discussion papers.

The BMLF consists of a cross section of IFAs, Banks, Building Societies, Solicitors and Life Insurance firms. Members represent the following organisations.

AXA Sun Life
Bristol & West

Nationwide Building Society
Hargreaves Lansdown
Legal and General
Cheltenham and Glouscester
Beachcroft Wansborough
Deloitte and Touche
Burges Salmon
Zurich Financial Services
AMP
St James's Place
Burns Anderson
Pioneer Friendly Society

Scope of this Response

This letter does not constitute a formal response on behalf of all the member firms. The views expressed in this response reflect the views of the individuals attending the BMLF. The BMLF has also taken the opportunity to feed its views into the Association of British Insurers response to DP22.

Detailed response to questions raised:

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

A1: In banking and deposit taking virtually all Suspicion Activity Reports (SARs) are submitted following consideration of some form of KYC information. It is rare for a transaction to be suspicious in isolation from all knowledge of the customer or client. Logically, therefore, more reports (and more effective reports) should result from the effective monitoring of relevant KYC information.

The challenge with KYC information is deciding what is proportionate to the business relationship being established and linking that knowledge to consistent and effective transaction monitoring.

It is difficult to imagine how a firm could meet its current regulatory and statutory requirements without co-ordinating these two factors. In doing so, firms need to decide the point at which the gathering of KYC information and monitoring of transactions ceases to be appropriate to their business and regulatory obligations and becomes more relevant to investigating possible financial crime.

For insurance and personal investment products we believe the key to effective KYC lies in proportionality. These products have relatively low levels of transaction volumes and therefore the most effective utilisation of resources would be deployed in an effective and proportionate monitoring system. The FSA will need to consider the cost benefit implications of monitoring systems for different firms, and recognise that in some cases a manual system may be the most appropriate. This is not to suggest that KYC is not of value for these products, indeed KYC and transaction monitoring are linked strongly.

Member life insurance provider firms' experience of insurance and personal investment products is that the main reason for identifying and reporting suspicious transactions relates to the transaction itself as opposed to issues raised by KYC held.

Q2: How should firms pursue a risk-based approach to AML?

A2: Firms need to understand their products, customers and transaction types and document the risks involved. Firms should review their internal risks and rank these relative to each other. Firms need to review the risks relative to outside data using:

- Networking at conferences, MLRO discussion groups etc
- Seeking guidance from their FSA Supervisor

- Industry press
- Use of consultants
- Industry bodies

Firms should relate the resource they apply to AML to the:

- Risk profile of the firm, based on products, market, strength of procedures and compliance, geographical spread of operations
- Expectations of developments in the marketplace

Firms should manage risks closely through Approved Persons:

- Using effective, well targeted MI
- Using registers and work flow techniques that suit the firm
- Emphasising the accountability of senior management
- Implementing effective escalation procedures.

If insufficient knowledge or information exists within the firm to enable it to assess
risks with confidence, it should refer to its FSA Supervisor or seek support from consultants. This approach would be particularly beneficial in relation to new initiatives such as electronic identity checking and the setting of parameters and scoring.

For many firms the concern will be that they may find themselves the subject of enforcement action if it is subsequently decided they took too lenient an approach in their assessment of risks. Therefore the industry would welcome guidance from the FSA as to areas that may be considered high risk.

Know Your Customer

There is an argument that it would be beneficial for the FSA to prescribe the amount of KYC required per product type. This could promote a level playing field amongst the Industry and may also lead to a more consistent customer experience. Customers will know that wherever they open a particular product all providers will ask them the same set of questions.

It can be argued that in the particular area of Identity Verification and KYC that the FSA place too much emphasis on firms adopting a risk-based approach. Firms' application of high level guidance will vary widely. If two firms offer a current account with full money transmission facilities, then the risk nature of the product and hence the amount of KYC should be the same in both firms.

Transaction Monitoring

Whilst linked, it is important to separate out the two issues of KYC and Transaction Monitoring. In our opinion, the answers to this question in respect of these separate issues are different.

In terms of account monitoring, our view is that it should be left to each firm to decide what is appropriate to their operations on a risk-based approach. Firms that allow electronic trading may effectively have no option other than to implement a robust electronic system that will allow them to keep track of account activities. In the case of firms that deal with low risk products with relatively infrequent transaction volumes, a more simple exception reporting system may be appropriate since the costs of implementing electronic system reporting could be considerable

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

A3: This is for them to decide but it is surprising that they cannot use the photographic evidence that many firms are able to provide.

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

A4: KYC Costs

∉ Collecting information and obtaining customer consent.

- Retaining and using information
- Avoiding potential Data Protection Act costs
- Explanation and awareness raising with intermediaries and customers
- Designing business processes to collect and collate
- Addressing legacy systems and historic record keeping issues
- Additional stationery
- Staff training
- Monitoring and auditing
- Collecting supplementary or updating existing information

KYC Benefits (apart from complying with regulations)

- Potential information for marketing purposes
- Possible reduction in fraud

Transaction Monitoring costs

- Manpower, software (rules based or neural systems - the latter is estimated to be 4 times more costly than rules based systems), software licences, cost of pursuing additional exceptions that turn out not to be suspicious and, for automated systems, significant set up costs

Benefits

- There are likely to be marketing benefits, particularly from certain automated systems but also generally from being more aware of customer/client behaviour patterns.
- Possible reduction in fraud

Q5: Which options presented do you prefer and why?

A5: Option 4 is the preferred choice of the majority of our members. The area of AML regulation has been one of intense recent activity and the new JMLSG

Guidance Notes are due to be published shortly. Given the intention to undertake a further radical re-write of the JMLSG Guidance notes, we feel that it would be premature for the FSA to seek further change in the regulatory landscape at this stage.

Given this rate of change, it may be that additional high level FSA rules at this stage would not add great value to efforts to combat AML. Firms would still need to implement the detail in their own businesses, and this would in turn result in a risk based, diverse application and interpretation. It may be a more appropriate course of action for the FSA to delay the implementation of any further rules until the Industry has had the chance to input into the review of the JMLSG Guidance Notes

Option 1 is also seen by several of our members as having advantages. Specific FSA rules and guidance (particularly in respect of KYC) could aid with the application of KYC requirements in a more consistent manner across the industry.

Please contact me if you have any questions regarding this response.

Yours sincerely

Pekka Dare

Legal Compliance Manager/ Deputy MLRO

AXA Sun Life

On behalf of the members of the Bristol Money Laundering Forum

BVCA *investing in enterprise*

3 Clements Inn
London WC2A 2AZ

T 020-7025 2950
F 020-7025 2951

bvca@bvca.co.uk
www.bvca.co.uk

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

29 January 2004

Dear Mr Shonfeld

DP 22 – Reducing Money Laundering Risk

We are writing on behalf of the British Venture Capital Association in response to the above Discussion Paper.

The BVCA represents the vast majority of United Kingdom-based private equity and venture capital firms.

Our response focuses on what we believe is the key question in the DP - which of the four main options should be adopted by the FSA.

Since the introduction of the FSA Handbook of Rules and Guidance in late 2001 the area of anti-money laundering and related laws/regulations is almost certainly the regulatory area which has attracted most attention at the international and national level.

FATF developments and the implementation of the Second EU Money Laundering Directive together with the Proceeds of Crime Act and the recently adopted Money Laundering Regulations in the UK have seen a significant move forward in the ML framework at governmental/quasi-governmental level. In addition there has been a range of amendments to the JMLSG Guidance Notes - partly to reflect those government initiatives but also to reflect developing good practice in an area which has received significant attention from the financial services industry over the period. Looking forward the industry will be asked to absorb further initiatives from FATF, a Third EU Money Laundering Directive and a significant rewrite of the JMLSG Guidance Notes within the next one to two years.

Against this background it seems self-evident that further changes in the FSA rule book should only be introduced if:-

a) There are clear deficiencies in the current/developing anti-money laundering framework in the UK which can best be addressed by FSA rule changes rather than other forms of legislation/regulation/guidance;

b) The FSA is finding it difficult to pursue disciplinary action against offenders.

As neither a) or b) seems to us to be an issue we favour options 3 (leave ML unchanged; rely on the JMLSG Guidance Notes) or 4 (make no settled decision now and review the position again in, say, two years time) as set out in the Discussion Paper. As between these two options we have some preference for 3 as we believe that the current rules, which are set at a high level, appropriately address the key issues and are capable of doing so even with future changes in legislation and good practice provided they "adopt" the JMLSG Guidance Notes to provide a dynamic level of detailed guidance to financial services firms.

The only change, therefore, which the FSA should consider to its Handbook is a proper endorsement of the JMLSG Guidance Notes as appropriate good practice as many MLROs and others within the industry regard the current "recognition" contained in ML 3.1.4G as not giving sufficient regulatory support to the professionals in the financial services industry who are seeking to carry out a difficult task against a background of a constantly developing and increasingly complex set of legal, regulatory and good practice requirements.

The best way of achieving this would be the inclusion of an additional evidential provision which might state:

"Compliance with the Joint Money Laundering Steering Group's Guidance Notes for the Financial Sector may be relied upon to establish compliance with [list relevant rules in ML]."

Since the JMLSG Guidance Notes are not comprehensive and provide only a "current interpretation of good practice across the financial sector" it is important that acting in accordance with the Guidance Notes should constitute evidence of compliance but a different approach should not create a presumption of non-compliance. In other words, the use of an evidential provision in this instance should incorporate limb (b) but not limb (a) of the definition of *"evidential provision"* in the FSA Glossary.

Yours sincerely

MARGARET CHAMBERLAIN
Chairman BVCA Regulatory Committee

BRITISH BANKERS' ASSOCIATION

Pinners Hall
105-108 Old Broad Street
London EC2N 1EX

Tel: +44 (0) 20 7216 8800
Fax: +44 (0) 20 7216 8811

2 February 2004

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

Dear Mr Shonfeld

BBA RESPONSE TO FSA DISCUSSION PAPER 22 "REDUCING MONEY LAUNDERING RISK – KNOW YOUR CUSTOMER AND ANTI-MONEY LAUNDERING MONITORING"

The British Bankers' Association, which represents over 250 banks in the UK, welcomes the opportunity to comment on the FSA's Discussion Paper 22 (DP22) "Reducing money laundering risk – know your customer and anti-money laundering monitoring".

General comments

A risk-based approach

Paras 2.5-2.9

1. A risk-based approach underlies DP22 and the approach to KYC and monitoring in the paper. The JMLSG Guidance Notes already embody the elements of a risk-based approach. Risk-based is a new element in the 2003 recommendations of the FATF on customer due diligence procedures. With the FSA's support, it will receive considerably more attention in the radical revision of the JMLSG Guidance Notes that is currently being drafted, and, given its importance in DP22, it may be useful to mention some issues that may arise as a result of its more systematic application. The following comments look first at some characteristics of a risk-based approach, then at possible legal aspects, and lastly its implications for banks' relations with the regulators if a risk-based approach is to operate effectively:

    a. Firms support in principle a risk based approach. It is intuitively sensible, proportionate and cost effective to devote more AML resources to those areas where the money laundering risk is greatest.

    b. By definition, implementation of risk-based guidance is likely to be more varied than one size fits all, prescribed procedures. Individual firms' approaches to a risk-based approach will depend on a variety of factors including size, but it is difficult to draw a clear link between size and attitudes to risk. For instance a small firm with a limited number of clients may feel that it is simpler to apply a uniform rules-based approach, whereas a large firm may see the advantages of a risk–based approach in terms of allocating resources more precisely to areas of greater or lesser risk. But a large firm is also likely to need to explain what is a more complex approach to many thousands of staff, in order to ensure that a risk-based approach is implemented consistently. Generalisations about the application of a risk based approach, even in a category of an industry sector, will need careful consideration.

c. The money laundering risk of a product or transaction may change over time. The more a product or transaction is perceived as high–risk and therefore subject to enhanced due diligence, the greater the incentive for a money launderer to move towards other areas (including greater use of cash) and businesses that are subject to less diligence. Design of a risk-based approach will have to flexible to adjust to such changes. A partnership approach, involving the exchange of intelligence between industry, regulators, government and law enforcement will help to achieve this.

d. A flexible approach is also needed because firms will have different degrees of confidence that they know where their areas of greater, and lesser, risk lie. For example, if a firm has less confidence, it may decide to apply a sampling approach across a range of transactions (akin to an audit) in order to check against money laundering. Another firm with greater confidence in its knowledge of risk will allocate its resources accordingly.

e. The amount of business that is being transacted will affect the degree of risk, since <u>proportionately</u> more effort is likely to be needed to deter and detect money laundering in a larger business than in a smaller one (on the "needle in a haystack" principle).

f. Customers will approach a firm to acquire one product but will subsequently migrate to others, which will have different levels of risk, particularly in a "one stop shop" environment of modern retail banking. A firm will need to take a key decision, whether to carry out at the start of a relationship a level of due diligence appropriate to the range of products that a customer may purchase in future, or whether to carry out enhanced due diligence procedures as the relationship develops. The first approach may create inconvenience for a new customer, but it may generate greater confidence in the firm that it has implemented adequate safeguards to mitigate risk. Firms' decisions are unlikely to be identical, but they will impact on the implementation of a risk-based approach.

g. Given the legal, reputational and regulatory risks they face, firms will require confidence that a risk-based approach is consistent with the "reasonable grounds" criterion in the Proceeds of Crime Act 2002. If it is argued with hindsight that money laundering was not prevented as a result of a firms' assessment of risk which it had made in good faith, and the firm is thereby culpable, firms are unlikely to embrace a risk based approach, which by definition is unlikely to deter all money laundering in areas that are assessed to be low risk. Implementation of a risk-based approach is therefore likely to reflect decisions by the regulator and the courts. Lack of information on either will create uncertainty for firms.

h. Firms' assessments of any given risk are likely to differ. This puts a heavy burden on the firm, raises the question of the appropriate balance between prescriptive and discretionary approaches, and makes the task of the regulator more difficult. A key aspect is the implication of a risk-based approach for a level playing field, in terms of implementation of AML measures. It is likely to be a more complex task to ensure, and to be seen to ensure, a level playing field with a risk-based than with a more prescriptive and uniform approach. But firms' perceptions of the extent to which there is broad equality of implementation of AML systems are a crucial element in ensuring that they do not become an element of competition, in which the inherent risk could be under-estimated. The implications for regulators in ensuring broad equality of implementation, and the consequences of failing to achieve this, will need careful consideration in a Consultation Paper. They are likely to involve more of a partnership approach in assessing risk than hitherto.

i. A risk-based approach is not necessarily a cheap option, as is sometimes implied. Building systems to include high-risk areas is expensive, and staff training costs involved in operating a more flexible system are likely to be higher than with a more standardised approach and will need to satisfy cost-benefit tests.

2. As noted above, a risk-based approach puts the responsibility on firms. It needs to be more flexible and will be more complex than a uniform "one size fits all" one. Many firms will be unwilling to base their anti-money laundering procedures on a risk-based approach without some assurance from the FSA that they will accept a risk-based approach, if properly implemented. If firms fear that, with the benefit of hindsight, they might be penalised when a case of ML is discovered despite a risk-based procedure having been followed effectively and in good faith, they are likely to play for safety and adopt a more uniform rules-based approach. If a risk-based approach is to gain wide acceptance among firms and their staff who will have to implement it, the FSA must be prepared to give appropriate assurances. Firms need to know where they stand on these issues, perhaps especially branches of foreign banks. The FSA's Consultation Paper must discuss these issues.

3. The negligence or objective test in the POCA may also be a legal obstacle to acceptance of a risk-based approach (para 1.g refers). This might be mitigated if there were acceptance that a risk-based approach is inherently unlikely to eliminate all money laundering, but it is the best way to produce a low failure rate in terms of incidence of money laundering, and if this were exceeded a firm would face penalties. As noted above the negligence test in the POCA is not conducive to this approach.

4. These considerations point to the need for

    a. A clear acceptance in the FSA Handbook of, and encouragement for, a risk-based approach for those firms that elect to use it. This would be a basis for a more detailed description in the JMLSG Guidance Notes.
    b. A consensus is needed on precisely what definition(s) are to be used in assessing degrees of risk. Is it (a) the likelihood that money laundering will be attempted in a particular are; (b) the chances of detection should it be attempted; (c) the consequences for the firm if a type of money laundering is detected; (d) a

combination of all of these? The last of these seems inherently the most practical definition.

c. A close dialogue between the FSA, the industry as a whole about the general approach to a risk based approach and the assessment of particular money laundering risks, and with individual firms about the particular risk-based approach that the latter propose to adopt, so that the industry and firms will have some degree of confidence that it is likely to be accepted and not subject to criticism with hindsight, if it has been followed in good faith by the firm and new factors have not appeared which the firm has chosen to ignore.
d. Joint examination of the workability of the "failure rate" concept above.
e. The minimum requirements for firms where the risk, as defined in specific areas, is low will need to be clear; together with agreement on any areas where a risk-based approach is unlikely to be applicable. One such area in the latter category may be terrorist financing where this requires procedures by firms that go beyond standard (risk-based) ID & V checks and subsequent KYC and monitoring. Banks are unlikely to be able to contribute to tackling the issue of terrorist financing without specific intelligence from the authorities.
f. A risk-based approach is likely to work well with a firm that is more committed to minimising the risk that it may be used for money laundering than one that is, for a variety of possible reasons, less committed. Both categories need to be catered for. This points to the need for examples from the regulator of items that are likely to fall into higher or lower risk products, transactions and customers. This will help ensure consistency, and reduce concerns of lack of a level playing field. But firms should also be left with some discretion to adopt a different approach, depending on its particular circumstances and provided that it is prepared to defend its decision to adopt a different approach to its regulator.

KYC *

Para 3.4.

5. Banks see some form of KYC as an essential part of an anti-money laundering strategy, and indeed of a prudent banking strategy. Verification of identity should be one element, but not the sole element, of an AML strategy. An appropriate balance needs to be struck between it and the other elements; in particular, KYC, but this cannot become an excuse for slack verification procedures. KYC should be consistent with the steps that a prudent banker would undertake in any case, and without KYC it is difficult if not impossible to conduct monitoring of customers. A formal requirement to conduct KYC to complement initial ID & V procedures would be part of a holistic approach. It could be a valuable supplement to identity

---

Á * In this note the term "KYC" is used to refer to a requirement to obtain information beyond the basic identity information that firms are required to obtain from new customers (or existing customers whose identity needs to be verified). This is normally described as KYB, and the KYC definition above may create confusion. However in order not to create further confusion and for the sake of consistency the term KYC is used in the sense used in the DP.

verification procedures, particularly for areas such as companies, beneficial owners and controllers of companies, trusts where documentation can be obtained but does not necessarily reveal the beneficial owners or controllers.

6. Examples of KYC are already in the JMLSG Guidance Notes. For persons KYC information might include occupation and income. The implementation from 1 January 2004 of parts of the Savings Directive will may provide access to a tax identification number for those who will be affected by its provisions. In the case of legal persons KYC might include the nature of the ownership of firms (beneficial ownership and holding companies); the purpose of the company; sources of its funds; whether there is a relationship with another branch or a subsidiary; its cash flow (in order to help identify unusual transactions); the markets in which it trades; the size of the company in relation to business turnover, and the quality and reputation of a company, especially its senior management. However not all these types of information will be available to a firm, particularly at the outset of a business relationship, nor will the information obtainable always help in assessing money-laundering risk, nor can a definition of "reasonable steps" be taken to imply that a firm must take <u>all</u> possible steps, or to obtain all possible information about a customer. KYC is as much an art as a science, and is likely to remain so. A KYC approach should not be retrospective nor be expected to override a CCR where one has been carried out. It should be sufficient for firms to obtain KYC; they should not have to "verify" it as with initial identification.

7. If the UK is to have a formal requirement to perform KYC, it should be a part of an EU wide requirement in a 3rd EU Money Laundering Directive.

8. The statement that "firms may find that they are exposed to increased legal risk of failing to meet their reporting obligations if they focus on basic identification evidence and do not collect or use wider KYC information." requires comment. As the footnote indicates, the requirement in Section 330 (2) (b) requires a firm to report "where they have reasonable grounds for knowing or suspecting that someone is engaged in money laundering". There is currently no requirement to collect KYC information, as stated in para 4.2.3G of the ML Sourcebook, and the "reasonable grounds…" cannot therefore be related to the collection, or failure to collect, such information. However the failure to consider such information where it does exist would represent a breach of FSA Rule 4.3.2 and could expose a firm to the risk of not complying with the POCA. A court might consider that "reasonable grounds" would exist if a person (a) had the opportunity to obtain or access information which a "reasonably prudent" banker might collect, and (b) the information would, if properly considered, have led to "reasonable grounds" for suspicion even if in fact the information was not collected. Clearly there is a risk of requiring 20/20 hindsight, but the subjective nature of such judgements is likely to lead to uncertainty pending clarification by a court.

9. **Para 3.7: Scope of KYC information.** It is not clear whether "the various relationships of signatories and underlying beneficial owners" falls into the category of KYC, or whether this information should be sought as part of the basic identification evidence on any account, as per Regulation 9 and Rule 3.1.3 (2), and it should not be included in this category in the DP.

10. The reference to risk at the end of this paragraph needs to be highlighted.

11. **Para 3.10.** Not all (or even most of) the information in 3.7 would be collected for "marketing and product development purposes."

12. **Para 3.19.** Firms agree with the statement in the final sentence.

13. **Para 4.20.** As noted above, KYC and monitoring are elements of an integrated approach to AML. While they are a complement to, not a replacement for, verification of identification, and there will always be a basic ID requirement, the nature of ID requirements needs to take account of the other elements in a risk-based approach. The firm should have discretion, and the responsibility for justifying them to the regulator, to determine what measures (above a basic minimum) it will use in applying a risk-based approach. In particular this may be the case with:

- Low risk customers;
- Customers to whom credit facilities have been granted and where a formal credit approval process meets AML KYC identification and verification standards (the latter is particularly key in respect of a subsidiary company that might have been assessed for credit on the strength of its parent).
- Customers that have been subject to a retrospective review of identification information;
- Overseas-domiciled customer where address verification will often require KYC to supplement documentation. The provisions of the Savings Directive may be relevant here.
- As a supplement to documentation on identity of beneficial ownership, ultimate controllers etc;
- Personal customers domiciled in EU member states where a national ID card is compulsory;
- Individuals connected with corporate accounts that can be verified.

<u>Monitoring</u>

Monitoring should not necessarily involve electronic monitoring, particularly since the high incidence of "false positives" generated by many current electronic systems suggests that there is room for further development, and that in some areas monitoring could be supplemented by analysis of typologies.

<u>Answers to specific questions</u>

1. *How necessary is the collection of KYC information and an active approach to monitoring in reducing money laundering risk and in meeting legal and regulatory requirements, in particular resorting?*

Banks see some form of collection of KYC information and active transaction monitoring as essential; the question is rather the extent and form that they take. Some firms believe (see below) that the implementation of a Rule requiring both enhanced KYC and transaction monitoring, using a risk-based approach, would bring the UK into line with the FATF 40 Recommendations (Nos 5 and 11).

The emphasis on appropriateness in the provision of monitoring systems is important; in particular automated systems should not be seen as a necessary solution for all firms. While some form of monitoring is essential for compliance, the method and approach must be driven by the type of business and whether it adds value. Firms need to be able to judge when "unusual" signifies "suspicious" at present the conversion ratio is low.

2. *How should firms pursue a risk-based approach to anti-money laundering?*

The approach in para 2.9 is sensible. As noted above, criteria for risk assessment should be clear but not prescriptive; individual firms should assess their risks against criteria which may be indicated in guidance but which they see as appropriate. Some discretion should be left to the firm. As noted above, the obligations placed on firms by the present legal framework inhibit a full application of a risk-based approach, and a fully informed judgement of specific risks is not always easy on account of lack of sufficient case histories. Firms will need to take account of others' experience as well an assessment of their own specific risks (which is obviously crucial) and apply a commonsense approach.

3. *What type of monitoring (and reports) would be most useful to law enforcement?*

This question is for law enforcement agencies to answer in the first instance. As noted above, better intelligence is a key to implementation of a risk-based approach and will need an enhanced dialogue between law enforcement and the financial services sector.

4. *What are, or may be, the costs and benefits of KYC and monitoring?*

Paras 3.20 and 4.18 of the DP set out most of the cost implications of putting KYC and monitoring systems into place. The former however makes no mention of staff costs in terms of training, or possible opportunity costs in terms of customer resistance particularly in the retail market.

Benefits may be those arising from a reduction in financial crime. As the DP indicates (para 4.18) no quantification of these benefits is possible without an indication from law enforcement agencies of the contribution made by SARs to reducing crime overall.

5. *Which options presented do you prefer, and why?*

The FSA workshop showed that opinions within the financial services industry are divided. There are powerful arguments for taking no decisions now (option 4 in DP22) because of the rapid pace of change (POCA, a 2nd and possibly a 3rd EU Money Laundering Directive) and technological developments (electronic checks, growth of non- face to face banking, and electronic monitoring systems), and waiting to see how these develop.

These factors would militate against a detailed approach with specific and prescriptive FSA rules, and a number of firms within the banking sector would favour such an approach, at least at this stage.

But most banks see KYC and monitoring (not necessarily electronic monitoring) as having a key role to play in banking. Many banks believe there would also be advantage in recognising this, as a means of reducing the current over emphasis on ID & V requirements. This would need to be in the form of a high level requirement (perhaps with examples) to take appropriate measures of KYC and monitoring but with a link to the guidance notes. This view therefore points to a variation of option 1. As the DP notes in para 5.2, there is considerable diversity of practice between firms. A regulatory approach on the above lines would need to:

- Be broad enough to take account of the differences of risk profile and risk management techniques between firms across the financial sector;
- Be flexible enough to reflect changes in risk assessments, and to account of experience gained;

- help ensure broad equivalence of implementation in respect of equivalent degrees of risk;
- Help explain to customers why they need to provide information.

A further point is that if a decision were delayed now it could weaken the UK's ability to ensure an EU wide AML regime involving KYC and monitoring in a 3rd money laundering directive. A decision to make these a formal requirement in say 2 years' time could lead to an uneven playing field. A "do nothing now" decision could also send misleading signals about the value of KYC and monitoring. But a final view on the options must await a more precise definition of what form the options would take.

Yours sincerely

Jeremy Thorp
Director, Financial Crime,
BBA
2 February 2004

FSA Discussion Paper 22: Reducing Money Laundering Risk – Know Your Customer and Anti-Money Laundering Monitoring.

Submission by the Building Societies Association

Introduction

1. The Building Societies Association represents all 63 building societies in the UK. Those societies have total assets of over £190 billion, about 15 million adult savers and over two and a half million borrowers. Building societies account for over 18% of both outstanding residential mortgage balances and retail deposit balances in the UK. Building societies account for over 35% of cash ISA balances in the UK.

2. The Association welcomes the opportunity to respond the Discussion Paper on reducing money laundering risk.

General Comments

Building societies are committed to financial crime prevention.

A Risk-Based Approach

Paragraphs 2.5-2.9 discusses a risk based approach. Building societies in principle support a risk based approach – in that it potentially allows a proportionate and potentially cost effective approach to anti-money laundering. Some societies, however are concerned about a risk based approach and prefer more prescription. There is concern that a risk based approach leads to an unlevel playing field.

The building society sector has a wide range of building societies in terms of assets size and branch numbers. The attached table helps to demonstrate this. It is clear that a firms approach to a risk based approach differs due to a variety of reasons, one of which is size. A number of the smaller to medium sized societies often argue that it is easier and simpler for them to apply a uniform rules-based approach. This is partially to do with the number of customers they have, the range of accounts (tends to be limited) and the confidence they have that they are complying fully with regulation.

There is a lot of debate in the industry as to what a risk-based approach means. Some believe that the industry themselves (banks and building societies) have a different view to a risk based approach to the FSA for example. The radical revision of the Guidance Notes 2004 should help to address this point.

Given the prospect of large fines, reputational and regulatory risks that firms face they need to be confident that a risk based approach is consistent with "reasonable grounds" within POCA 2002.

A further concern lies with the risk based approach; a society may offer a low risk product which may be targeted by one or more high risk individuals – does this product become high risk? Some parts of the industry argue that if a product is seen as low risk it may be targeted and therefore become a high risk product. This debate needs to be aired. One such area is the basic bank account. Anecdotal evidence suggests that these accounts are being targeted, partly because of the "lower" ID&V requirements. Once a customer has such an account they then apply to move to other accounts such as current accounts.

The BSA runs a Financial Crime Prevention Panel, which is made up of a cross section of building societies and a number of banks (converters who used to be building societies). It is clear from discussions within the group that there are different assessments of risks in respect of products, services and customers.

There is still disagreement within the financial services sector about where a risk based approach is useful or not.

Identity

The initial identification of a customer is an important part of an anti-money laundering regime. It does however have its own problems – the rise in forged identification documents, the problem of the financially excluded (in particular) in producing the appropriate ID and the reliability of such checks as the voters roll.

Building societies would like to see the government's proposal for a National Identity Card bought forward.

There is some concern about the usefulness of the some of the verification checks – such as the Voters Roll for example; anyone can register for the Voters Roll and there are no checks undertaken. There should be a debate about use or access to Government or Government Agencies databases such as NHS lists, DWP records to carry out checks against. If the Government really does wish to fight financial crime work in these areas need to be undertaken.

The Government Agencies do not work together closely enough, for example the information on tax or benefit claimants should be made available more readily to other Government Agencies to ensure that they know what areas of crime to tackle. A joined up approach at this level could provide intelligence in respect of terrorist finance for banks and building societies to use in KYC and transaction monitoring systems, but without such information building societies and banks are limited in the extent to which they can provide useful information to law enforcement agencies.

Anti Money Laundering Monitoring

Many societies stated that the best way of monitoring account activity is through staff members identifying the unusual through their local knowledge, intuition, direct contact with customer and through experience, recognising activity that just does not make sense. No automated monitoring system can replace this, however, such systems can compliment the work undertaken by staff, in particular, in organisations where there are high levels of transactions and/or a high proportion of the transactions are without staff member intervention.

RESPONSES TO SPECIFIC QUESTIONS

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

It is clear that societies view the need to gain comprehensive KYC at the outset as important. The identification and verification of customers at the outset is one element of an anti-money laundering strategy, knowing your customer better a further element. The extent and form of the KYC to be collected needs to be discussed. Gaining more information about a customer at the outset could be extremely helpful, particularly in respect of how that person intends or is likely to use the product or service. Obtaining this information is only helpful or important if a firm intends to use it, or does actually use it. There is the potential for a requirement for firms to collect the information, but not actually have to use it to

Building societies are concerned about a "level playing field" in relation to KYC. Some societies think there should be a consistent, industry standard within the United Kingdom in relation to KYC. There is concern that the problems relating to the apparent difference in ID&V checks will be replicated in the need to obtain KYC information and could result in the loss of customers.

Building societies felt that the practical issues surrounding the collection of KYC – 3.23 were fairly identified. A number of societies expressed concern in their ability to keep the KYC information up-to-date. In order to carry out effective transaction monitoring it is necessary to know something about your customer to know whether a transaction is suspicious – this goes for branch staff with local knowledge as well as electronic systems. The need to keep KYC up-to-date to ensure that transaction monitoring was relevant is important, but the time, costs and abilities of societies, particular the smaller ones to do this on a formal basis may be difficult.

A number of the regional societies all made the point that they know the majority of their customers, or occupations of local people so that they are able to identify suspicious behaviour.

It is not always possible to gather full KYC about a customer at the outset of a business relationship, nor will the information obtained always help to assess a money laundering risk. Societies particularly made this point in relation to Savings Accounts where there is no money transmission facilities.

The collection of KYC at the outset has a strong link to monitoring and reporting. In order to determine whether a transaction is unusual or suspicious, it is beneficial to know as much about the customer as is possible.

It is important that the appropriateness of a monitoring systems be assessed. Electronic systems are not the solution for all firms. Some form of monitoring is required for compliance, but the method and approach has to be dictated by the type of business and whether it adds value. Many societies carry out monitoring to a certain degree.

Not every "unusual" transaction is a "suspicious" transaction.

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

Many firms are concerned about basing their anti-money laundering procedures on a risk-based approach without some assurance or guidance from the FSA that they will accept a risk-based approach, if properly implemented. Many societies would like greater guidance or criteria against which to measure or assess risk. Firms are concerned that they if they adopt a risk based approach they may fail to undertake anti-money laundering regimes properly. Equally if they do follow a risk based approach effectively, but a money laundering case is bought against them then they may have been better opting for a rules based approach to start with.

A rules based approach gives clarity and provides a certain element of certainty. Providing a society adheres to all the rules they have the knowledge that the society is adhering to legislation or regulation and is therefore unlikely to be fined, or have action against them.

A number of societies have said that guideline from the authorities, or assurance from the FSA that their approach is correct or will be accepted would give more societies the confidence to pursue a risk based approach.

Greater dialogue between firms, FSA, NCIS and law enforcement agencies to assess money laundering risks would be helpful so that firms can help assess risks.

Firms assessments of risk differ – this includes customers, products and threats.

One society commented that cash that should be of primary concern not cheques or other banking transfers. The society argues that cheques and transfers may make investigations more complex and create layering there is nevertheless an audit trial. The authorities can investigate these audit trials. Cash on the other hand does not leave an audit trial and does require greater identification as a suspicious transaction.

The approach suggested in paragraph 2.9 of DP22 is a potentially sensible way forward.

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

We believe that this question is for the law enforcement agencies to answer.

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

The costs associated with KYC include **s**ystem changes to accommodate collection and updating of KYC, staff training, changes to application forms/brochures, changes to business processes, possible loss of new business (unless KYC requirements are prescribed and are consistent across the financial services industry). Paragraph 3.20 outlines most of the costs implication of putting KYC into place, but does not cover staff training and the possible loss of business.

A small regional society estimated that for KYC information, new application forms system changes and imaging systems would be required and would result in a capital cost of £100,000 with ongoing maintenance and staff costs of around a further £10-£15,000, adding a further 3p on to the management expenses ratio. The society recognise the benefits of a more robust system, but felt that on a cost benefit analysis they would find it hard to justify the extra costs.

The benefits of a better KYC system is potentially the identification of better quality unusual transactions, potentially a reduction in investigation time, potentially a reduction in fraud and potentially a better and more consistent customer experience (if a level playing field approach is adopted).

Transaction Monitoring Costs

The costs associated with transaction monitoring are significant investment in technology development, staff training in the use of new technology, system support and maintenance costs and additional staff time in investigating “suspicious reports” identified by the system. Some electronic monitoring systems generate “false reports” – these tend to be rules based approaches. Every report generated potentially needs investigating by a member of staff to identify whether it was correct or a “false positive”.

For societies carrying out “manual” transaction monitoring there are staff costs involved – in respect of training “what to look for”, the ongoing monitoring, investigation of unusual or suspicious activity and production of reports.

A small regional society estimated that the capital costs for a monitoring system for the size of their organisation is around £20,000 with ongoing “maintenance” of £5000. To these figures needs to be added ongoing staff costs to investigate the extra reports that are produced. The society estimated that the capital expenditure listed above would add approximately 1.5p onto management expenses ratio. For a small society these are significant costs.

A medium sized regional society estimated the costs at a technical level. In this case the society estimated that on a risk-based approach initial costs for automated monitoring are circa £250k.

Transaction Monitoring Benefits

A good electronic system could potentially deliver good quality unusual alerts, the ability to keep track of all account activity, across all products and all distribution channels. This is of particular importance in relation to non face-to-face transactions, such as Internet banking, postal banking and the use of ATMs. Such systems can potentially increase consumer confidence and greater confidence in UK financial markets.

Transaction monitoring potentially makes it harder for criminals to launder money. Where transactions are identified more information can be provided to NCIS which in turn may result in more convictions.

There is great concern among the industry that firms are becoming “police-men”. The financial services industry has already invested millions into financial crime prevention, and this needs to be backed up by the Home Office, NCIS, law enforcement agencies in respect of crime detection, and the Government in terms of development of a sound database for ID&V checks.

Q5: Which options presented do you prefer and why?

There are mixed views in the building society sector on the options presented. The views are split between option 1 and option 4.

Some societies argued for option 1, that is to include in the Handbook specific rules and/or guidance on KYC and/or monitoring. One reason being, is that money launderers take the line of "least resistance". If it is perceived that some firms are tougher with their anti-money laundering procedures than others, then criminals may gravitate towards the weakest link in the anti-money laundering chain.

If option 1 is adopted it is suggested that specific rules on KYC and monitoring should be put into the handbook, but that the guidance be produced by the industry in conjunction with the JMLSG. Guidance should be produced by the industry, as they best understand their business. The guidance should, of course, specify that it is down to individual organisations to adopt the guidance in a way that is appropriate to their business by adopting a risk based approach.

The over riding view from the building society sector was that option 4 was preferred at this time. Option 4 suggests that no settled decision is made now and to review the position again in, say, two years time. Option 4 was preferred because it was felt that the industry need some time to consolidate; the industry has committed to the 2003 revised JMLSG Guidance Notes, with a further revision in 2004.

A number of transaction monitoring systems are being developed – some institutions have invested in rules based approaches, which are now being overtaken by behavioural systems. These systems require further testing before they are fully implemented.

The radical revision of the JMLSG Guidance Notes 2004 is to include a chapter on a risk based approach. Building Societies should be given time to understand and adopt fully a risk based approach before any rules on KYC and monitoring are made.

Societies are shortly to undertake the current customer review process. This is likely to take some time and will inevitably result in some customer disruption.

As well as dealing with CCR and the implementation of the Money Laundering Regulations 2003 and the JMLSG Guidance Notes 2003 societies are also adopting mortgage and general insurance regulation over the coming year.

There is little robust data about where the money laundering risks lie (although NCIS are currently working on this). This is required in order to be able to effectively monitor transactions, both manually and electronically.

It is unclear whether public sector finance has been forthcoming to NCIS and law enforcement agencies. Greater transaction monitoring may result in a rise in suspicious activity reports. With the increase in sectors reporting to NCIS, since the Money Laundering Regulations 2003, this may place a great burden on NCIS.

The industry is shortly to receive the results and findings from the Home Office taskforce on suspicious activity reports, receive HM Treasury's Anti-Money Laundering Strategy as well as a third money laundering Directive that is currently being negotiated. There is likely to be requirements and work arising from all three publications which the industry will have to address.

KYC and transaction monitoring may play a greater role in the FSA's work on fraud and dishonesty. Further thought needs to be given to this following responses to DP26.

It is important to let all the issues above "bed-down", during the meantime the FSA should work with the industry to undertake further research, gain data and assess systems. On the back of this work clear proposals can then be put forward (from a position of knowledge) in 1-2 years time. In 1-2 years time option 1 could be adopted, giving the industry time to develop the accompanying guidance.

29 January 2004

Cambridge Technology Solutions

Essential. Otherwise how can a firm possibly know with whom it is doing business and what type of business they are transacting?

This is easy in principle - it is a simple equation and financial institutions are well-versed in risk management methods. The difficult part is to know the financial 'value' to place on the downside risks (the other side of the equation - the cost of mitigating those risks - is relatively easy to estimate).
Unless the regulatory environment provides an answer to this unknown factor then it is very difficult for firms to pursue a risk-based approach in anything but the loosest way.
Personal liability is also potentially difficult to assign a value, but at least the assumptions are internal to the firm and therefore under its own control (in contrast to the assumptions it would have to make about the regulatory environment under a 'woolly' regime).

Costs of monitoring:

1. Software licence (may be one-off or per year/month etc. and may vary according to number of users, customers, transactions etc. and may also vary if optional functionality 'modules' are sold separately).

Software pricing is not transparent - there are no price lists published - and the software vendor will charge what it believes the institution can bear (which is related to the size of potential fines amongst other things such as the square yardage of marble in the HQ reception and the quality of cars in the car park). The FSA is the main sales driver, and high profile and high value fines are a fine proxy sales tool for the software vendor.

As stated in the DP22 paper, costs start from a few thousand pounds. Our price is ?25,000 one-off and fixed (i.e. no variation according to size of institution).

At off-shore development rates, this buys approximately 4 man-years' worth of programmer time (which is about the time needed to create an adequate transaction monitoring system).

2. Support and maintenance (yearly): usually 20% of licence price.

3. Upgrade costs (for new releases): we do not charge for upgrades but some software vendors do (particularly for new 'modules').

4. Hardware costs: depends on the firm, but for all but the biggest, this should be minimal (a single server with regular specification, say ?3,000).

5. Impementation cost (either internal, to the vendor or to a third party consultancy): depends on the simplicity of the solution; higher integration and more data sources inevitably means higher implementation cost. As a guideline, this should be a fraction of the licence price (certainly less than half).

6. Staffing costs (people to deal with output produced by the system): potentially the highest cost, and it is ongoing rather than one-off. For this

reason firms need to retain some discretionary control over the sensitivity of the system and the volume of output it produces.

Benefits of monitoring:

1. Avoid fines
2. Avoid reputation damage
3. Potentially use the same systems to detect fraud as well as ML

Costs and benefits of KYC - no comment.

Option 1 (a)
For the sake of clarity and removal of uncertainty.
That is surely one of the principles of good regulation, that firms should know where they stand and should be told what they need to do.
Otherwise the poor MLRO will always be fighting internal battles: there is a tension between the personal responsibility he bears and the commercial reality and as long as the requirements are a grey area the MLRO is likely to lose the battle.

However, overriding all of this is the need to create a nationwide transaction monitoring system. Money launderers do not typically perform layering within the same institution (would you if you were a launderer?), so intra-firm monitoring will always be limited primarily to the detection of placement activity.

We believe that with a simple design, the anonymous sharing of transaction information with a central body is practical, although clearly a major project.

Cameron Financial Services

I think that the approach with regard to this needs to be far more risk based. It is quite ridiculous to think that someone taking out a term assurance policy paying less than (say) £100 per month can be a risk from a money laundering perspective.

It is also unreasonable to think that someone transferring accrued pension rights is a risk.

The concentration has to be on reasonable verifiable risk. therefore current documentation should be needed for higher monthly premium plans and single premiums from non verified sources.

The extra regulation is a cost that is passed on to the consumer so ultimately it is they that pay for unneeded red tape.

.

CARR & ASSOCIATES

Life Insurance and Pensions Consultants - Independent Financial Advisers

20 Tithebarn Street . Liverpool . L2 2DT

Tele: 0151-227-5528
Fax: 0151-227-5529
E-Mail:CarrIFA@aol.com

Private & Confidential
Daniel Shonfield
Financial Crime Policy Unit
Prudential Standards Division
FSA
25 The North Colonnade
Canary Wharf
London E14 5HS

18 September 2003

Dear Mr Shonfield

"Money Laundering"

I am a small - even tiny - I.F.A.

I read DP22 when it arrived, put it to one side and then went to an F.S.A. road show – saw the CD-ROM on the topic and felt impelled to write.

Whilst it is perfectly proper to have anti money-laundering provisions in place, the problem with them at the point of interaction is that: –

(1) In some cases it is difficult to see the relevance, e.g.: –

(1) Mother and father set up a bond to mitigate Inheritance Tax. Bond is in favour of children (in the most recent case 4). Children are appointed trustees and beneficiaries of bond. Full money laundering is required for children. I accept that they are adult, but if money laundering is completed on parents, why is it needed on children? I know the counter-argument that children could have put parents in funds, but a trust that requires 20+ years to work!

(2) Existing client of long standing has family income benefit. This only pays out on death. Premium is £20 p.m. or so. We can now replace it with a policy costing £15 p.m. – a saving of £720 over the contract term. Full money laundering is required by the new provider, (L&G). Please tell me where is the money laundering risk in a policy costing £180 p.a. x 5 paying out £20,000 decreasing over a 5 year period. Even the villains I've met don't want to die so as to succeed in money laundering.

The problems we face are: –

(1) The product provider – for simplicity – pays no attention to the de minimus limits and impose a blanket requirement. It's no use you saying we can use our commercial decision to go elsewhere because that is where the market has gone.

(2) The admin cost outweighs the benefit, both to the State and to us; e.g., client has £10,000 pension fund. He is retiring. He is a smoker. His current insurer doesn't offer smoker annuity rates. He gets £2500 in tax free cash. His fund is then transferred to an impaired life annuity provider.

We have to do the comparison, fill in a fresh set of forms. There might (at this level) be just a £25 p.a. advantage to switching for the client. We have to do full money laundering for the receiving office. Given that the funds are coming from one (or more) authorised U.K. insurer straight to another, why do we need money laundering?

Might I suggest that: –

(1) "The client before 1994" exemption worked.

(2) That you reconsider the de minimus limits.

(3) That you promulgate the fact that if an <u>individual</u> transaction didn't exceed these limits no customer identification is required. Clearly, if a second or subsequent transaction took the client over the limit then that would be a different matter.

(4) That if the application came with funds from a U.K. insurer or drawn on a U.K. bank account in the clients name, no further action was required.

(5) That you have a word with the Crown/Registrar, Births, Marriages and Deaths. They are saying that it is forbidden to photocopy birth and marriage certificates and so certify them as true copies - Crown copyright. "You" want evidence of identity. Not everyone has a proper UK photo driving license, etc. and if the reader of this note has any personal experience, he/she will know that it is lunacy on a grand scale to send originals of birth and marriage certificates to any product provider for them to lose and this firm to get the blame.

In reality, little money laundering would seem to go on where the purchase monies are paid by cheque drawn on the originator's bank account. Where (I think) we all need to be vigilant is when the contribution is paid by cash or by cheque for the benefit to be obtained by a non-family third party.

The requirements for us to jump through hoops sits ill with the realities of cars paid for by cash, bets placed with on and off course bookmakers, and owners of clubs of all varieties where entrance is exaggerated so as to justify the payment of cash into the appropriate club account.

Yours sincerely,

Peter O'Hare

Shonfield 180903

The UK's Fraud Prevention Service
CIFAS, 4th Floor, Tennyson House, 159-165 Great Portland Street, London W1W 5PA
Tel: 020 7290 0530 Fax: 020 7290 0533
cifas@cifas.org.uk

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

8 October 2003

Dear Daniel

CIFAS Response to Discussion Paper 22 – Reducing Money Laundering Risk

CIFAS has been the leading financial services association for data sharing to prevent fraud for the last decade and we have considerable experience in using data to prevent fraud. We specialise in identity fraud and impersonation fraud where we are now the leading Association in the European Union.

I am attaching some background information about CIFAS and a list of our current membership.

We have decided to focus our response on Question 2 in the consultation, as this is our main area of expertise.

Question 2

We consider the current risk based approach to be eminently sensible, as it enables financial organisations to target resources where they are most likely to detect money laundering, or at those areas perceived to be at potential risk, if the controls were less tight.

However this is not without its difficulties and as a fraud prevention association holding a considerable volume of data, and with a responsibility to both consumers and our Members, CIFAS wishes to make the following observations:

- Deposit based savings accounts appear to be very low risk, yet the Know Your Customer (KYC) hurdles for customers are often the same as for much higher risk accounts. Consumers find it hard to understand why a credit card or loan is treated the same as a £20 a month regular savings account. There is a perceived lack of proportionality and the financial services industry could do a better job at explaining the need for these checks.

- Organisations that rely on electronic databases and place no reliance at all on paper identity documents to meet the KYC requirements are believed to be at greater risk than those who do both. Consumers also cannot understand why they can obtain a credit card with say, a £5,000 limit, on-line with no request for identity documents (because electronic databases are used to verify identity) yet to open let's say, a cash ISA with another organisation, they are asked to supply 4 proofs of identity.

  CIFAS considers that a standard explanation of the need for the checks should be adopted across the whole financial services industry and documentation completed by customers should explicitly state identity will be confirmed, and explain in general terms how it is confirmed so that consumers may have greater confidence that checks are being carried out.

- Organisations have individually developed their own policies on what constitutes acceptable proof of identity. For example, the following policies could be found in operation in the UK today:

  - 4 paper proofs of identity – from a list of just 10
  - 2 paper proofs of identity from a list of over 20
  - No paper proofs of identity (but applicants not on the electronic databases refused the product unless they write in)
  - 1 paper proof of identity from a list of 12 and electronic database checks

  CIFAS considers the FSA and the Financial Services Industry should develop a list of identity documents that must be accepted by organisations and a list where there is discretion. This would remove most of the consumer confusion that exists today. There is little designed to annoy consumers more, than making a journey to a branch of a company, only to be told a document does not meet their policy, when another company willingly accepts it. In particular, young people and elderly people are excluded from the market by some of the more rigorous and inflexible policies and it can be very difficult indeed for them, even to open a savings account.

  The CIFAS experience of fraud, is that those organisations dealing non face-to-face and relying on a combination of both electronic databases and paper proofs of identity, appear to suffer considerably less identity and impersonation fraud than those relying on just one or the other. We would expect this also to be true of money laundering.

- Fraudsters are able to obtain sufficient personal data about individuals without them realising there is a problem, until they are chased for repayment of an account they did not open. Combining a reliance on electronic databases with no contact with the customer can mean these frauds are not detected by financial services organisations until after the event. We find that a combination of both appears to serve companies well, especially when there is direct face-to-face contact or telephone contact with the customer and the answers to security questions satisfy the organisation that they are dealing with the genuine customer.

Other Matters

We would endorse Option 1 – specific rules or guidance on KYC. We would like to see greater consistency in the application of the risk based approach through:

- Lists of documents organisations must accept and those where there is discretion to accept, particularly focusing on the needs of young people and the elderly, to avoid financial exclusion

- Formal risk assessments to arrive at the appropriate processes for individual companies

It should be noted that our Association is not part of the Joint Money Laundering Steering Group but we have met recently with the British Bankers' Association who are aware of our suggested approach and intend to involve us in the review of the next edition of the Guidance Notes.

We would welcome the opportunity to be more involved in this debate and to attend the round table discussion mentioned in the papers we received.

Yours sincerely

P E Hurst

Peter E Hurst
Chief Executive

CITIGROUP RESPONSE TO FSA DISCUSSION PAPER 22: "REDUCING MONEY LAUNDERING RISK"

1. On a point of presentation, we do not find it helpful that the term "KYC" is used in the Discussion Paper ("DP") to mean information beyond "basic" identity information. While we appreciate the reason for this proposal, we think that the traditional meaning of "KYC" has been precisely that basic information. Further information on a customer's financial circumstances has been known throughout the industry as "Know Your Business" (KYB) information for some time; indeed, it is in this sense that it is used in FSA's ML Sourcebook. On this basis, we see the usage in the DP as causing unnecessary complication. For the sake of consistency within this exercise, however, we have used the new formulation throughout this response.
2. We have appended some comments on issues arising from the text of the DP, referenced by the DP's paragraph numbers, followed by answers to the specific questions posed in it.

<u>Comments</u>

3. **2.5-2.9**: We entirely agree with the adoption of a risk-based approach. On that basis, our overall view <u>in principle</u> is that, subject to appropriate assessment of risk, KYC information and ongoing monitoring of business are of greater value than the "mechanical" collection of identity documents currently required by FSA's Rules and the ML Regulations.
4. **3.4**: We do not agree with the assertion that "firms may find that they are exposed to increased legal risk of failing to meet their reporting obligations under PoCA if they focus on basic identification evidence and do not collect or use wider KYC information". As the footnote indicates, the requirement on a firm is to report "where they have reasonable grounds for knowing or suspecting that someone is engaged in money laundering". There is currently no requirement, however, to collect KYC information, as stated in para 4.2.3G of the ML Sourcebook, and the "reasonable grounds…" cannot, therefore, be related to the collection, or failure to collect, such information. We accept, of course, that the failure to consider such information where it does exist would represent a breach of the FSA Rule 4.3.2 and could expose a firm to the risk of not complying with PoCA.
5. **3.7**: We generally agree with the information described as KYC. We question, however, whether "the various relationships of signatories and underlying beneficial owners" falls into that category. We regard that information as part of the basic identification evidence on any account, per Regulation 9 and Rule 3.1.3 (2), and think it misleading to include it in this category in the DP.
6. **4.20**: We question the assertions in para 4.20 of the DP. While we agree that monitoring is a complement to, not a replacement for, identification, we continue to see some scope for a reduction in identification requirements where appropriate monitoring is in place. In particular, we see this as relevant in the case of
   - low risk customers;
   - customers to whom credit facilities have been granted and who have, therefore, been subject to a formal credit approval process;
   - customers subject to a retrospective review of identification information;
   - overseas–domiciled customers where address verification, in particular, is unreliable;

- personal customers domiciled in EU member states where a national identity card is compulsory;
- individuals connected with corporate accounts.

In all of the above instances, our view is that the existence of an appropriate monitoring system would, at the least, mitigate the need for separate documentary evidence of identity and address.

Questions

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

As noted above, our view is that both the collection of KYC information and active transaction monitoring are essential to efforts to combat the use of the financial system by criminals. Further, the implementation of a Rule in some form requiring both enhanced KYC and transaction monitoring would bring the UK into line with the FATF 40 Recommendations (specifically Recommendations 5 and 11).

We endorse, however, the emphasis on appropriateness in the provision of monitoring systems; we do not think it right for automated systems to be seen as a necessary solution for all firms.

2. How should firms pursue a risk-based approach to anti money laundering?

We agree with the approach outlined in para 2.9 of the DP. We do not feel that regulation should be prescriptive on the criteria for the risk assessment; in our view, it is for individual firms to assess their customer base against criteria which they see as appropriate.

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

We do not regard ourselves as qualified to comment on this.

4. What are, or may be, the costs and benefits of KYC and monitoring?

Paras 3.20 and 4.18 of the DP fairly set out most of the cost implications of putting KYC and monitoring systems in place. On the former, however, no mention is made of either staff costs, in terms of training, or possible opportunity costs, in terms of customer resistance, specifically in the retail market.

The benefits may be seen as those arising from the overall benefits from the reduction of financial crime. As the DP indicates (para 4.18), however, no quantification of these benefits is possible without an indication from Law Enforcement agencies of the contribution made by SARs to reducing crime overall.

5. Which options presented do you prefer and why?

Our favoured option would be 1(c), an explicit link between the ML Sourcebook and the JMLSG Guidance Notes, as foreshadowed in para 6.12 of the FSA's Consultation Paper CP 199 on "Proposed amendments to the ML sourcebook and consequent changes". We regard specific rules or guidance as unnecessary when the industry's view of best practice is already set out in the Guidance Notes. We believe, however, that options 2-4 would leave too great a scope for an "unlevel playing field" to develop between firms with varying degrees, qualitative and quantitative, of compliance. Providing a link between the formal regulatory requirement of the Sourcebook and the industry's own view of appropriate levels of information gathering and monitoring, as set out in the Guidance Notes, seems to us the most practical solution.

City Equities Limited

OCEAN HOUSE, LITTLE TRINITY LANE, LONDON EC4V 2DL
SWITCHBOARD: 020 7489 5555 DEALING: 020 7489 5500 FAX: 020 7489 5566 WEBSITE: www.cityequities.com

Mr Daniel Shonfeld
Financial Crime Policy Unit
Prudential Standards Division
15th floor
Financial Services Authority
25 The North Colonnade
Canary Wharf
LONDON
E14 5HS

16 January 2004

Dear Mr Shonfeld

Re: Discussion Paper 22

Please find enclosed City Equities Limited's reponse to the discussion paper on 'Reducing Money Laundering Risk'.

Yours sincerely

Philippa Kelly
Senior Compliance Officer

Enc

City Equities Limited
OCEAN HOUSE, LITTLE TRINITY LANE, LONDON EC4V 2DL
SWITCHBOARD: 020 7489 5555 DEALING: 020 7489 5500 FAX: 020 7489 5566 WEBSITE: www.cityequities.com

CITY EQUITIES LIMITED

RESPONSE TO DISCUSSION PAPER 22

<u>REDUCING MONEY LAUNDERING RISK</u>

RESPONSES

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

Identification

The question posed assumes that the Know Your Client (KYC) identification collected is reliable. It is not. The Joint Money Laundering Steering Group (JMLSG) lists types of identification which are acceptable to prove an individuals identity, but we are all aware that not only is identification theft a rapidly growing crime, but it is well known that the type of identification required is widely available, for the payment of comparatively small sums of money, throughout the country.

Anyone can easily find a forger who can supply them with excellent quality forged documents. The belief that the possession of a utility bill in their name proves the identity of an individual, is nonsense. Before FSA can begin to review what type of ID is required, it has to start from the understanding that all the ID now available can be, and is, easily forged.

The simple answer to the question posed is that the collection of KYC information as presently required has no effect whatsoever on a committed and professional criminal who has access to the necessary skills to steal or forge identification.

Honest people will supply genuine information. Dishonest people will not. Although large institutions can and do employ individuals experienced in identification fraud, even they can have difficulty in identifying forgeries. This avenue is not open to smaller institutions, where the costs would be prohibitive.

Scope of KYC Information

One of the major problems faced by any adviser when enquiring of a potential customer about their circumstances, is how much the customer is prepared to tell them. This is not because they are dishonest, but simply because they do not want a stranger to know their business. Money is one of the few remaining taboos in the United Kingdom and as a consequence many customers will only give a limited amount of information about themselves.

One reason for this can be seen in Point 3.8, which states:

Firms often obtain a significant amount of information for other purposes. The availability for information obtained for other purposes is important in assessing the cost and practical implications of KYC ...

This statement shows how chillingly easy it is to obtain personal and confidential details on individuals without either their knowledge or permission. The danger is that we will trample on the human right to privacy to obtain information regarding the activities of a few criminals. This statement appears to be a direct contravention of Article 8 of the Declaration on Human Rights and of the Data Protection Act 1998, where information held on an individual must be appropriate to the service with which they are being provided.

Point 3.9 is slightly more realistic regarding suitability and "obtaining sufficient personal and financial information about a customer relevant to the services that the firm is providing." Under Data Protection legislation one is not allowed to hold more than this.

.../cont

There is little point in mentioning human rights legislation and data protection, as is done on page 13, if at the same time you are actively undermining it in the manner already mentioned. For this reason the whole question of identification cannot be taken at a purely 'local' level but has to be mooted throughout not just the UK, but the EU as well. What is being attempted here is contradictory and can never work. There has to be a reasoned discussion on what is practical and reasonable in the fight against money laundering and its associated crime.

A major problem with the stance taken by FSA with regard to KYC is that it still thinks of individuals as staying with the same company or in the same occupation throughout their working life, living in the same house and having an income that rises by yearly increments.

This is shown by the statement:

When assessing affordability, regard should be had to the customer's current level of income and expenditure and any likely future changes.

This view is out of date. People now routinely change jobs, homes, marriage partners and countries, not to mention credit card companies, bank accounts and all manner of financial products. An example of this is in the changing of mortgage lender, where consumers now change lenders to take advantage of the 'best' deals on offer. This is a new trend, as customers invariably stayed with the same lender throughout the life of their mortgage even as recently as 10 years ago.

Reporting

KPMG's report* (Review of the regime for handling Suspicious Activity Reports) on the Economic Crime Branch of NCIS (1 July 2003) is a devastating critique of an under funded, understaffed (4.5.9) and inadequately trained (4.5.11/13) body. Staff are so unaware of their responsibilities that they do not always check the data they receive against the Police National Computer, which is the first and most obvious starting point for all suspicious reports (4.5.6).

Lack of training and expertise means that the few staff who are there, often do not understand the products and information with which they are dealing (4.513). The branch employs few police officers or financial investigators and the overall issue is given very low priority by the police throughout the country. Indeed, in the sample reviewed by KPMG, over 30% of all reports made to NCIS were lost, the police authorities involved being unable to track them down (figure 4.6).

There seems little point in criminalizing innocent financial services personnel who are trying to do their best in reporting suspicious transactions, when the information they are reporting is being lost or discarded. The knowledge that this is widespread, devalues the efforts of financial institutions against ML (4.2).

Financial services individuals are being expected to behave as untrained, unpaid police officers. Both financial services companies and individuals pay taxes for the police to carry out this type of function. While it is the duty of every subject of the Crown to aid law enforcement, to criminalize them for attempting so to do is quite simply, perverse.

.../cont

Other types of financial crime

The FSA has a statutory duty to reduce financial crime, yet has focused exclusively on money laundering. Financial companies are defrauded out of enormous sums of money every year by customers they know very well. KYC is not an issue here at all.

Fraud is a very serious crime, which has a considerable effect on the markets, honest customers and the economy, yet has never been dealt with by the Financial Services Authority, until DP 26 which has only recently been published. It is part of their statutory duty to do so.

.../cont

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

Information regarding money laundering and how to combat it is now widely disseminated. Anyone can download the necessary details from the Internet, for example, from the FATF and FSA web-sites. Money launderers are fully aware of all the action being taken against them and will be inventing new ways around these problems.

Added to this is the major problem that a lot of terrorist funding may begin as perfectly legitimate taxed and earned income. The IRA has for more than a century been funded by Irish-Americans in the United States, while Osama bin Laden's money was inherited. There are also highly refined non-banking systems, such as the hawala, that are used throughout the world. The idea that money launderers cannot cope with having to provide a gas bill as means of ID or that they have no other means of disposing of their criminal proceeds, is wrong.

Clearly those businesses dealing with cash transactions are at greatest risk of money laundering. Criminals are fully aware of the barriers that have been erected against them by financial institutions and with so many alternatives available to them, are much less likely to bother depositing their money with them.

Point 4.21 states:

Monitoring arrangements should be appropriate in nature, scale and sophistication to the size, nature and scale of the business.

This is a reasonable point, but FSA is let down in its practice of its own rules. FSA monitoring staff have been found to be unaware of their rules, to not have heard of the British Banker's Association or the JMLSG and to treat stockbrokers as having the same risk profile as a clearing bank.

Given this lack of knowledge, it is to be assumed that all financial services companies will be required to purchase automated monitoring systems, irrespective of their suitability for their particular business. Practice teaches that the risk profile of a firm is in reality ignored by the FSA itself.

There are also other problems with the type of systems available, for example, if one treats customers from a high-risk jurisdiction differently from customers from other countries, could this not lead to accusations of racism? While these systems may have a role to play with major retail deposit takers, they are of questionable value to smaller companies. The costs involved in such systems are also prohibitive and again give rise to the question as to why companies are paying to do police work.

Specific rules

The FSA should write the rules on ML and not leave it to another agency. They should take over the work of the JMLSG. The greater the number of bodies involved in producing the regulations, the greater the chance of confusion and ambiguity amongst bother regulators and end-users. The rules should be kept in one rulebook and should not require users to search for the information elsewhere.

The 'reasonable steps' idea is a good one, so long as each firm is informed by FSA of their risk profile. Problems would arise where FSA thought the risk profile was higher than that of the firm, and FSA must agree the risk profile with the firm, otherwise the rules would be seen not as a deterrent to ML, but as a revenue earner for FSA.

.../cont

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

Given that the Economic Crime Branch (ECB) of NCIS does not seem able to employ input staff, it seems obvious that all institutions should make submissions via e-mail with standard format attachment. This type of format is likely to be cheap enough for even the smallest providers to comply.

Institutions will have to be given a special identifying number for their reports in order to prevent criminals swamping NCIS with bogus reports, to crash the already over-burdened system. The reports should contain the following points:

NAME OF REPORTING INSTITUTION:

NUMBER OF REPORTING INSTITUTION:

NAME OF SUSPECT:

LEGAL STATUS OF SUSPECT:	YES	NO
Private Individual		
Limited Company		
Public Limited Company		
Trust		
Pension Scheme		
Other		

DATE OF BIRTH:

GENDER:

NATIONALITY:

ADDRESS:

POST CODE:

TELEPHONE NUMBER:
Home
Work
Mobile
e-mail

OCCUPATION:

EMPLOYER:

IDENTIFICATION SUPPLIED:

GENERAL INFORMATION:

REASONS FOR SUSPICION:
1.
2.

.../cont

Purpose of the Reports

It would appear from Point 4.7.9 of the KPMG report that there is a considerable discrepancy between the view taken by the police and the regulatory authorities as to the purpose of the suspicious activity reports. It would seem to be a good idea if all the relevant bodies involved have at the very least similar reasons for requiring the information.

Those involved in crime are unlikely to even attempt to launder money through the complicated financial services industry when there are so many easier outlets for them to do so. The use of estate agents, jewellers, art galleries, casinos and travel agents in money laundering is well known, and although plans do exist for including them in the ML regime, these plans have been in discussion for years and have yet to be implemented.

There seems little point in asking the financial services industry to report suspicions when it is so easy for any criminal to move to other types of money cleaning operations. The overall impression given by the report is that something has to be seen to be 'done' following 11 September 2001, and as a result a system was put into place, irrespective as to how effective that system may prove..

.../cont

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

There are considerable costs to the industry as a whole from KYC and monitoring, but perhaps the greatest cost is in giving society a false sense of security that the system they have in place is capable of reducing crime. The benefits are less apparent.

There is little point, but a great deal of cost involved, in companies of any size investing in computer software or indeed even bothering to make disclosures, if these are effectively ignored by the investigating authorities. NCIS and the police must have adequate procedures in place prior to any updating of the reporting regime, otherwise there will continue to be massive reporting with no-one dealing with the information.

* KPMG Money Laundering: Review of the Reporting System, 1 July 2003 (Chapter 4).

TRAVERS
SMITH
BRAITHWAITE
LONDON PARIS BERLIN

10 SNOW HILL, LONDON EC1A 2AL
TELEPHONE +44 (0) 20 7295 3000
FAX +44 (0) 20 7295 3500
DX 79 LONDON
WWW.TRAVERSSMITH.COM

BY E-MAIL AND POST
Mr Daniel Shonfeld
Financial Crime Policy Unit
Prudential Standards Division
Financial Services Authority
25 The North Colonnade
Canary Wharf
LONDON E14 5HS

OUR REF MAC/PAB
DOC ID 2047012
EMAIL Margaret.Chamberlain@TraversSmith.com
DIRECT LINE 020 7295 3233

29 January 2004

Dear Mr Shonfeld

FSA DISCUSSION PAPER 22: CITY OF LONDON LAW SOCIETY RESPONSE

This response is made on behalf of the City of London Law Society Regulatory Sub-Committee.

The FSA raises the question as to whether firms can adequately manage their money laundering risk and meet high level legal and regulatory obligations without collecting specific KYC and monitoring information. The FSA suggests a number of options for Handbook provisions on this issue.

Specific Rules and/or Specific Guidance

We do not think that specific rules and/or guidance on KYC and/or monitoring is either desirable or practicable. The range of firms covered by FSA authorisation makes useful guidance on this topic almost impossible to draft. Since any rule would seem to need to be drafted in terms that would need supporting by guidance, we think this is not the appropriate route. There are already high level rules and principles, as noted by FSA which could be breached in relation to a failure to have proper KYC and monitoring procedures. We do not think a specific rule would improve this. It would be better for the FSA to take steps to highlight the fact that it has a general expectation that firms will be doing whatever is appropriate in this area.

Our strongly preferred option at this stage is to leave ML unchanged and to rely on the JMLSG Guidance Notes. There is a significant amount of work currently being taken across the industry in relation to the Guidance Notes to try to make them more appropriate to the context of the different kinds of business carried out by authorised firms, and we think it would be most useful for the FSA to await the outcome of this exercise before determining its appropriate response. We think that at this stage for authorised firms to have yet further rules and guidance at a time when this main industry guidance, the JMLSG Guidance, is itself under review, would be unnecessarily burdensome for firms and that it would be better for there to be one set of guidance which may they then be expected to apply as appropriate. Options 3 and 4 are therefore our preferred approach. We think that taking one of these options together with use of the risk mitigation tools referred to in paragraph 5.16(ii) should be sufficient.

The FSA asks for comments on whether firms are confident that they understand the FSA regulatory requirements and what is expected of them. In our view, it is difficult for firms to answer this question completely - since the FSA rules reflect on a law which in itself contains significant uncertainties as to what it is that has to be reported etc. (the FSA may be aware of our correspondence with the Home Office on this topic, a copy of which is enclosed). As there are areas where firms have to exercise judgement and take risk based decisions, it must be difficult for them to know whether in doing so they are meeting the regulatory requirements. However, it is difficult to see what can be done to improve that position.

Yours sincerely

MARGARET CHAMBERLAIN

COMPLIANCE
INSTITUTE

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

4 February 2004

Dear Daniel

The Compliance Institute warmly welcomes the opportunity to comment on Discussion Paper 22, and would like to congratulate FSA on a well-written and interesting paper which provides a comprehensive survey of the problems that face the industry in dealing with money laundering, and the possible solutions that may be adopted to deal with them.

However, our view is that option 4, deferring any definite action, is the one to be adopted. We feel that FSA themselves put the case for this option very well when they say in DP22 that it would enable them to take account of the revision of the Guidance notes, and "have the benefit of longer experience of the impact of Police and Criminal Evidence Act, and of the decisions made on the Suspicious Activity Reports in the light of the KPMG review".

There may also be developments in monitoring systems and techniques.

We also note that since the period of consultation began, DP26 has been issued. Although this mainly discusses fraud, there is a comment to the effect that the Money Laundering Sourcebook may be rewritten. If FSA are indeed thinking along these lines, it would seem to reinforce the idea that option 4 is the more appropriate course to adopt in respect of DP22 at this stage.

Our answers to the five questions are as follows, but we are putting them forward only on the understanding that FSA do not select option 4. If that is the case, our preference is marginally for option 2, although we do not find any of the other options particularly attractive.

Question 1, How necessary is the collection of Know Your Customer (KYC) information and an active approach to monitoring, in reducing money laundering risk, and in meeting legal and regulatory obligations, in particular reporting? There could be advantages in requiring KYC information over and above the basic identification information, and to monitor how customers are using a firm's products and services, but it would be necessary to conduct a rigorous cost/benefit analysis to ensure that the extra work, and the attendant cost are really justified by the perceived risk.

There could also be very considerable consumer resistance to such processes unless there is public endorsement by Government, media and consumer groups, and a general consensus that the measures are absolutely necessary. Such discussions would have to take account of the Human Rights Act and Data Protection Act.

P O Box 6099
Leicester
LE4 8WT

Telephone:
+44 (0) 116 260 4239
Fax:
+44 (0) 116 260 4241

The Compliance Institute
A Company Limited By
Guarantee,
Registered in England
No. 2487718

Registered Office:
P O Box 6099
Bridge Park Road
Leicester LE4 8WT

There are problems regarding verification of the data collected and, as FSA themselves point out, maintaining and updating it.

Question 2, How should firms pursue a risk-based approach to anti-money laundering?

Firms should realise that confirming identity is extremely important but that it is not the only requirement, and should ensure that all systems and controls take into account money laundering risks and contain provisions for minimising it. This cannot be a one-off requirement but must be reviewed regularly in the light of internal and external factors.

Question 3, What type of monitoring and reports would be most useful to law enforcement agencies.

We feel that this is a question for the law enforcement agencies. However, that may be an appropriate point to mention our concern that according to unofficial comments from the agencies, far too many mindlessly trivial reports seem to be going to them, with which they can do nothing, and which merely waste their time. The main motivation for sending them seems to be a "safety first of all costs" attitude on the part of firms.

It would be helpful for the agencies to agree with firms as to what information they really find useful, and what not. if this were to happen, the agencies might be able to be more open as to what use was made of the information; at the moment, firms tend to hear nothing.

Question 4, What are, or may be, the costs and benefits of KYC and monitoring? In the absence of definite proposals, it is not possible to comment definitively. However, if a 1% Sandler regime were to be introduced, extra costs for KYC and monitoring would be difficult to accommodate for those contracts.

Question 5, What option presented do you prefer and why?

See comments above.

The Institute would be most pleased to enter into further correspondence should FSA feel this to be appropriate. We will be submitting a formal version of our response by post in the near future.

Yours sincerely

Stephen Gore
Regulatory Development Manager

please please please
will you realise the incredible cost to IFAs and Product Providers of Money Laundering chacks

these are tortally unnecessary if the client is able to quote their NI number and tax reference

i am not suggesting big brother
but with the incredibly large amount of information the government and similar organisations hold on line all that is needed is free access to a government web site and the ability to inpot client information

we would get back a certificate (like the unipass certificates we use) giving no information whatsoever but just confirming that money laundering checks were satisfactory - if this were NOT forthcoming we would have to complete extra checks and you would have had an anonymous tip off that something unusual was happening

frankly, if tax and YNI are paid no other check is necessary in the majority of cases

and the Revenue would also have a full list of non taxpayers who were investing money

surely this is better than the current situation

.

DSB IFA

Q1 = The idea is excellent, the practice is pointless bureacracy. Q2 = Let the banks do it - it is pointless to keep repeated the process. The banks are the only people in a position to provide real help to the Police, except in the case of stupid or amateur money launderers (who we can report as suspiciois anyway). Have money laundering on file makes advisers feel "absolved" of suspicions as they have PROOF the clients is not a drug baron.
The current regime is nonsensical.
Q3 = Reporting of odd activity, especially via the banks who are the only people really in a position to monitor. Q4 = From the IFA end it is a pontless and annoying activity for us and clients. It makes life very difficult for the young and old, but causes no problems for genuine money launderers. Q5 = I can see no point in IFAs or insurance companies being involved provided the money comes from a UK bank. Consent = Yes
----

.

INDEPENDENT FINANCIAL ADVISERS

LIFE, PENSION and MORTGAGE CONSULTANTS

Directors:
E. P. SYRETT, F.C.I.I.
Mrs. K. SYRETT, B.Sc.(Hons)
Mrs. G. WILSON, B.A.(Hons), A.C.I.I., A.S.F.A.

E. P. SYRETT LTD.

GOYT LODGE
67 STRINES ROAD
MARPLE
SK6 7DT

TELEPHONE:
0161-427 2101
FAX:
0161-427 6386

Our ref: GW/DK

14 October, 2003

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

Dear Mr Shonfeld

RE DISCUSSION PAPER – NEWS LETTER 22
REDUCING MONEY LAUNDERING RISKS – KNOW YOUR CUSTOMER AND ANTI MONEY LAUNDERING MONITORING

I refer to the above Newsletter and would to wish to comment as follow: -

- Whilst we consider the Money Laundering Regulations to be of a high priority in meeting our statutory obligations, we feel, as an effective contribution to the fight against money laundering, crime and terrorism, in many instances, they are overburdensome. This is particularly the case for smaller IFA's who have a very close, and in many instances, a long-standing relationship with their clients, having seen them on an annual basis for some twenty plus years. Knowing the customer for these clients is surely more significant than obtaining a photocopy of their driving licence or mortgage statement.

- We feel that any Regulations using KYC and monitoring should reflect the above by being more risk specific. For instance, there is surely a greater element of potential money laundering for new clients walking into a high street office with cash to invest compared with long-standing clients adding £50 per month to their Personal Pension Plan, taking out new Life Assurance or Critical Illness for modest premiums, or even transferring between pensions when the cheques are passed between ceding and receiving Schemes directly. Money Laundering rules should target more risky areas.

- Strengthening the know your customer requirements with sensible exemptions, as previously with the pre 1994 rule and monitoring any changes out of "character" offers a more risk based process. It should reduce some of the administrative burden, and cost, by removing the requirement for new validation every time new business, including increments, are submitted to Providers.

Possibly some contracts could be filtered out of the money laundering requirements with say minimum amounts under which there are less stringent requirements.

- ❖ Strengthening the requirement to use Suspicious Activity Reports for "out of character" transactions if used in conjunction with KYC and monitoring would then identify potential risky activities.

We feel that there is an opportunity to produce new KYC and monitoring regulations that can more closely reflect the risk to the individual firm in relation to their Statutory Money Laundering requirements that should reduce time-consuming administrative duplication and costs to the IFA sector in particular.

Yours sincerely

Mrs.Gill Wilson B.A.(Hons.), A.C.I.I., M.S.F.A.
Pension Director

Equinox Capital Management
Q1 = All firms must obey the rles and regulations and the spirit of these conditions Q2 = Yes More active on high risk people and locations

Our business is institutional
Q3 = Fewer as clearly NCIS is unable to cope

THE REAL PRIORITY OF NCIS IS FOOTBALL HOOLIGANS
Q4 = There is no benefit unless you count missing an FSA fine.

It is expense and a tax on business
Q5 = Reduce the grip on heavy handed enforcement
Consent = Yes

.

Equionx Securities

Q1 = Vital
Q2 = Yes espacially if operating in the wholeslae sector
Q3 = Real cases and not just folk reporting because they are scared of the penalties., Q4 = It is all cost and there is no benefit except missing an FSA fine like Abbey National
Q5 = The last one

Remote Host: 212.161.48.124
Remote IP: 212.161.48.124
User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Referer: http://www.fsa.gov.uk/pubs/discussion/dp22_response.html

.

Ernst & Young LLP
1 More London Place
London SE1 2AF

Phone: 020 7951 2000
Fax: 020 7951 1345
CDE & LDE Box 241
www.ey.com/uk

30 January 2004

CO/CRW/CCWA/E15

Mr D Shonfeld
Financial Crime Policy Unit
Prudential Standards Division
The Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

Dear Mr Shonfeld

DP 22 - Reducing money laundering risk

Ernst & Young is an authorised professional firm that conducts its mainstream regulated activities as one-off corporate finance assignments which constitute only a small proportion of its total business. We support in principle the efforts of Government and the FSA to combat money laundering, crime and terrorism and we welcome this opportunity to comment on the FSA's proposals in the above discussion paper.

We have some general comments which are summarised below and explained in more detail in the attached appendix, which also addresses the specific questions in the paper.

- Development of new rules and guidance should focus on managing the risk of money laundering in firms' businesses rather than impose responsibilities for active detection.

- New rules and guidance should recognise the situation of one-off transactions for one-off customers as well as ongoing business relationships.

- Requirements for accessing KYC information held by a firm should not override Chinese Walls and similar procedures that help to manage conflicts and protect confidential information.

- As JMLSG guidance is designed for the businesses of its members, other authorised firms should be permitted to follow more suitable guidance where it is available.

If you require any further explanation or clarification of our comments, please contact me or Chris Anderson (direct line : 020 7951 3141).

Yours sincerely
For and on behalf of Ernst & Young LLP

Clive Ward
Money Laundering Reporting Officer

Appendix to letter of 30 January 2004 from Ernst & Young LLP

Comments on DP 22 – Reducing money laundering risk

General comments

1. The general tone of the paper seems very much directed at firms taking active steps to detect money laundering when there is no current legal or regulatory requirement to do so. This is acknowledged in paragraphs 3.4 and 4.3, although references are provided to a number of Handbook requirements. These recognise the FSA's risk based approach to regulation by imposing requirements for firms to counter the risk that their businesses are used for money laundering. We support these existing Handbook requirements and recommend that the objective of any further development of rules and guidance should be to provide additional help to firms in meeting their existing obligations, rather than bringing them into the scope of active detection, which is properly the responsibility of the law enforcement authorities.

2. The discussion in the paper, and indeed much of the existing Handbook rules and guidance, appears relatively straightforward in the context of relationships such as banks operating current account facilities for customers. The proposed requirements become more difficult to understand and apply in the context of a one-off transaction for a customer who may or may not return at some future time for another one-off transaction, where there is no relationship in the intervening period. We recommend that the proposals, in particular the requirements for maintaining and keeping up to date KYC information and for monitoring a customer's activity, recognise such situations, rather than leave firms attempting to interpret rules and guidance designed for a different context.

3. Many authorised firms conduct business that is not regulated activities and for many professional firms, mainstream regulated activities represent only a small proportion. It is not clear whether it is intended that the KYC information to be kept and accessed in respect of customers for regulated activities should include all information available in the firm or only that related to regulated activities. Additionally, information held by a firm about a customer may have been obtained in a context other than from services to that customer, for example from unrelated services to a second customer where the first customer was involved as a counterparty. Firms will have secure Chinese Walls procedures in order to manage conflicts of interest and preserve confidentiality and the proposals appear to require that these procedures should be breached so that all available information may be used for KYC and monitoring purposes. We recommend that any new rules and guidance make clear the extent of KYC information in a firm that should be collated and recognise that KYC should not override Chinese Walls and similar procedures.

4. JMLSG guidance notes are given much prominence in these proposals, as they are in existing Handbook guidance. Many authorised firms, in particular professional firms, are not members of the member bodies of JMLSG, but are members of professional bodies which issue their own anti-money laundering guidance. The constituent members of JMLSG represent the mainstream financial services sector, such as banks, insurers and IFAs and consequently the JMLSG guidance notes are written in a manner that is appropriate for such business. In many respects, this makes the guidance unsuitable or difficult to interpret for other firms. We recommend that guidance issued by professional bodies is recognised as an alternative to the JMLSG guidance when it is more appropriate for a firm's business, or alternatively that the JMLSG is required to align its guidance with the businesses of the entire constituency of authorised firms.

Specific questions

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

KYC information and monitoring are important elements for firms addressing the risk of their businesses becoming involved in or being used for money laundering. However, we believe that care needs to be taken to avoid imposing disproportionate requirements that could become a costly burden and draw firms too close to detection activities that more properly are the responsibility of law enforcement agencies.

2. How should firms pursue a risk-based approach to anti-money laundering?

What is important is that firms do have an approach to anti-money laundering and that this is pursued based on risk, in order to avoid disproportionate cost and to focus resources where they are likely to be most effective. We believe that it is inappropriate to be prescriptive in Handbook rules as to how firms should do this, but that guidance is necessary to help firms develop their own approach according to the nature of their business and the customers they serve.

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

It is appropriate that this question is answered by those agencies. However, as explained in 1 above, business should not be required to bear a disproportionate burden of cost and disruption through meeting the needs of law enforcement agencies as a primary objective.

4. What are, or may be, the costs and benefits of KYC and monitoring?

The costs of KYC and monitoring will depend on the extent to which requirements are imposed in a manner that is prescriptive and disproportionate. Many well run businesses will gather KYC information as a matter of course in order that they can provide services that meet their customers' requirements. They also regard monitoring as an important element in confirming customer satisfaction and minimising risk in the business. If new rules and guidance impose requirements on firms in a manner that permits them to use the KYC and monitoring processes that are necessary for their own business purposes also for anti-money laundering purposes, only marginal additional costs are likely to be incurred.

With the approach outlined above, the main benefit is that anti-money laundering processes will be recognised as the same processes that are necessary for a well run business to operate effectively and consequently can gain more ready acceptance as part of normal business life.

5. Which options presented do you prefer and why?

We prefer Option 2, to introduce high-level guidance. This would permit a flexible and proportionate approach that allows firms to develop procedures that are suitable for their own business and the particular risks that it presents. We prefer to avoid the imposition of rules, in particular because they may remove the judgement and discretion that are vital for an individual attempting to honour his legal obligation to report a suspicion without having to consider whether rules have been followed in forming that suspicion.

Experian's Response to the FSA Discussion Paper 22

Jim Lound
30th December 2003

Contents

Reducing Money Laundering Risk – Know Your Customer and anti-money laundering monitoring

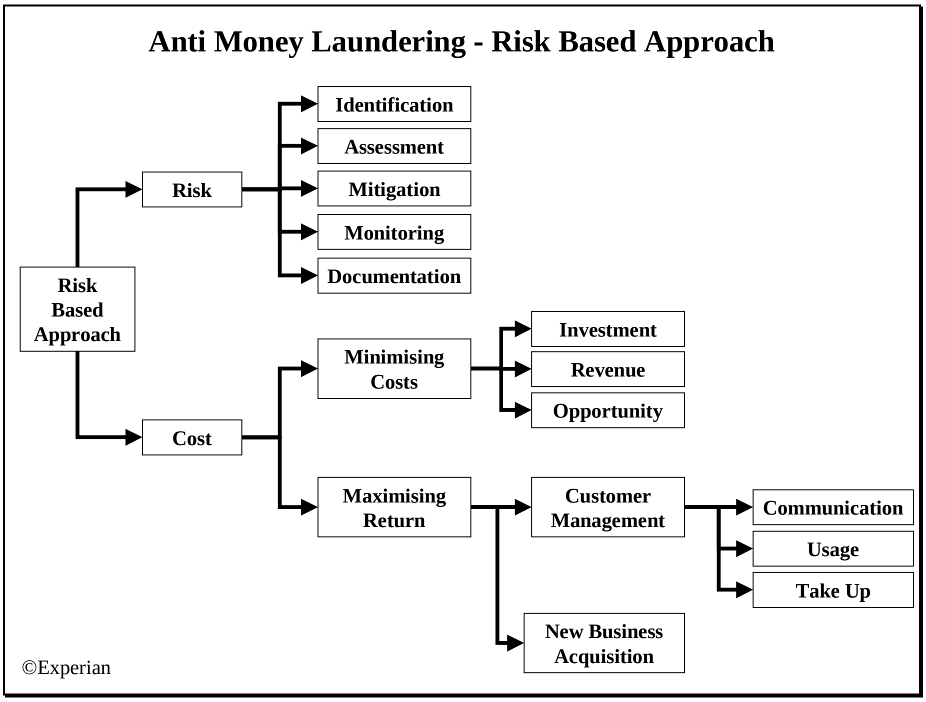
1. The Risk Based Approach

The risk based approach to anti money laundering controls is intended to ensure that only proportionate costs are expended, whilst making the process effective without being an unnecessary burden on the customers.

The risk based approach therefore requires a balance to be struck between the risk and the cost elements.

The risk element comprising of: -
- Identification
- Assessment
- Mitigation
- Monitoring
- Documentation

The cost element comprising of: -
- Minimising the costs
- Maximise the return on the investment



Jim Lound
Experian
30th December 2003

Collectively these elements will have an impact across the whole of an organisation, specifically: -

- MLRO and Compliance
- Fraud & Credit Risk Management
- Operations
- Sales
- Marketing
- Finance

It is therefore imperative that the whole organisation views the anti money laundering controls as being as much a part of the business process, both at acquisition and customer management, as any of the other core functions e.g. sales cost of acquisition of new business.

Many currently view the effort involved as a hurdle to 'get over' which often results in a tick box mentality approach to the task by front line staff. As a result, existing checks are frequently seen as onerous and ineffective.

The challenge is to convince organisations to view the costs and effort associated with the implementation of anti money laundering controls as a necessary check in order to manage the day to day functioning and effective management of the firms' interests.

This will only be achieved if the process can be seen to be: -

- Effective – finds money launderers
- Value for money – worth the cost and effort involved

In today's increasingly remote business world many financial services organisations rarely get the opportunity to interact with their customers and learn about them and what they want from the relationship. The execution of money laundering checks, both at application and during the life of the relationship, results in the collection of valuable data providing an opportunity to, not only ensure that the customer is who they say they are, but also establish their other needs.

2. Know Your Customer

The Know Your Customer (KYC) data should be viewed by the firm as a corporate data asset.

KYC is not just about anti money laundering controls.

But anti money laundering control is about KYC.

KYC is a data asset and is required by many of the day to day functions undertaken by the firm: -

∉ Assessment of fraud risk
∉ Assessment of credit risk
∉ Defining the terms of business e.g. the initial credit limit
∉ Defining the post service strategy e.g. when to review the credit limit
∉ Upselling of products - existing facilities to existing customers
∉ Cross selling of products
∉ Attrition strategy

As well as the assessment of money laundering risk

Whilst the KYC data required may vary dependant upon the function, there is sufficient overlap of its uses to view KYC as a collective set of data.

The assessment of money laundering risk will require a set of KYC data that should be sufficiently common across all firms as to be able to define the minimum set. Dependant upon the type of business, each firm should also have additional KYC data requirements relevant to their particular market and products.

KYC data should not be limited to the data available at the initial application stage.

KYC data needs to grow and be maintained in order to maximise its contribution towards the functioning of the firm. This includes the need to have anti money laundering controls that are applied during the life of the customer relationship.

Taking some examples of KYC data elements and their potential contribution towards mitigating the firm's risks and maximising profit: -

The level of confidence that the identity exists	Fraud and money laundering (ML) risk
The level of confidence that this is the person associated with the identity	Fraud and ML risk
The customer's income and spending patterns	Credit risk, ML risk, terms of business, post service strategy, upselling, cross selling, attrition strategy
The customer's existing account holdings	Credit risk, ML risk, terms of business, post service strategy, upselling, cross selling, attrition strategy
Is the customer likely to receive overseas transfers?	ML risk, cross selling, attrition strategy
The level of confidence that the application data has not been manipulated	Credit risk, ML risk
The customer's time at their current address	Credit risk, ML risk, cross selling
The customer's time in their current employment	Credit risk, ML risk
The customer's type of employment	Credit risk, ML risk, cross selling

The term KYC has become synonymous with the hurdle that is seen to be anti money laundering controls.

If the term KYC was changed to Customer Relationship Management (CRM) data this would make the firms' Marketing and Sales Directors sit up and listen and be interested in making their CRM data as comprehensive as possible in order to assist all their sales and marketing related activities. Indeed it is not just the Sales function that has an interest in this information; ongoing credit risk management also needs to understand the customers' current situation and the behaviours that might ensue.

It would be seen that the cost of acquiring and managing the KYC data becomes more acceptable with the current perceived burden of responsibility being lifted from the shoulders of the MLRO and Compliance. This would allow the MLRO and Compliance to stop working and thinking in their own silos and become more integrated into the business and not be regarded as a resource drain.

In short, a holistic view of customers is essential to any organisation seeking to achieve the maximum opportunity from the relationship in terms of maximising sales and minimising risk. The requirements to support such a strategy are the same as to ensure that the customer is not a criminal and/or money launderer.

Any additional costs, specifically associated with the KYC requirements, should be minimal, possibly only associated with the retention of records and audit trails. Even then, responsible lending requirements and the needs of analytics and modelling have considerable overlap.

3. **Monitoring**

Being alert to how a customer is using a firm's products and services and therefore to signs of money laundering requires the on-going monitoring of transactions associated with the customer. To be effective the monitoring of transactions cannot be undertaken in isolation of the KYC data. It is, therefore, essential that the KYC data is maintained and is up to date as possible.

A transaction viewed in isolation may be regarded as medium risk but when associated with the up to date KYC data it may indicate an increased risk. For example, the customer may have changed residency but the customer has not directly informed the firm.

A high risk transaction can reactively trigger a review of the up to date KYC data. Conversely, monitoring significant changes in the KYC can proactively trigger a review of the transactions over a pre-defined period of time.

Jim Lound
Experian
30th December 2003

4. Use of Electronic Data

The use of electronic data in the validation and verification of identities and the distillation of this data into a risk index is already recognised as a valid method of identity checking in the JMLSG guidance notes.

This provides a more robust and consistent measure at a fraction of the cost when compared to the use of documentary evidence. The use of electronic data also improves the customer experience when opening new facilities with firms.

The extent of the reduction in costs will vary between firms, but to give an indication savings of 90% can be achieved when compared to the cost of appraising, processing, storing and retrieving documentary evidence.

From a customer service perspective, the use of electronic data provides a less intrusive and more convenient method of assessing the confidence in their identity.

In a risk based environment, where the extent to which anti money laundering controls are applied need to be balanced against the costs incurred, the use of electronic data provides a significant opportunity to reduce the risk of ML activity occurring.

This tangible cost reduction and improved productivity of the firms' human resources should grab the attention of the Operations and Finance Directors.

However, there is evidence to suggest that in some firms there is still a reliance on documentary evidence where the main justification is that the documents are tangible, the user can see and touch them and they have been accepted practice for many years even though there is a recognition within the firm that this practice is questionable and expensive and may contain no real value anyway.

Electronic data sources can be used to populate and maintain KYC data throughout the customer relationship. The use of electronic data procured externally to the firm, for example from organisations such as Experian, can provide data that relates to the customer's wider world of interaction with society that the firm may not be aware of.

Furthermore the benefit of using information from a third party rather than from the consumers themselves has already been proven in the credit and risk environment.

As mentioned previously KYC, as a corporate data asset, can be used to satisfy a whole range of functions associated with managing the customer relationship.

Sanctions data is another source of electronic data. The sanctions data needs to be checked at the time of the initial application and at regular intervals throughout the customer relationship in order to monitor any significant changes or new additions to the data.

Many organisations use Behavioural Scoring and monitoring techniques to understand the changes in a consumers profile and how that might impact on their ability to service facilities in the future. There is little difference in the needs and process required for monitoring for unusual activity of a potentially criminal nature. Again, such techniques are in common use by Experian clients utilising the tried and tested on-line and batch access to sanctions data at the initial application stage and as part of a regular monitoring service.

5. Effective Customer Management

The on-going application of anti money laundering controls should not be viewed as an isolated event. It should be viewed as an integral part of the customer management activity.

Making contact with a customer can be an expensive business and therefore making effective use of the opportunity is essential. Knowing when to contact a customer, in order to maximise the revenue opportunity and to effectively manage the various risks, including the ML risk, is the key to successful customer management.

With regards to the anti money laundering controls, the period of elapsed time between reviews needs to be proportionate to the risk. Wire transfers, for example, would need on-line checks against the sanctions data at the time of the transaction whereas a low risk product may need to be reviewed only once a year.

Using external electronic data sources to trigger the contact with the customer is a very cost effective and efficient way of updating KYC data. This is particularly true when key life events can be identified that may pose a significant risk in ML terms but alternatively may present an ideal opportunity to cross sell and upsell products. This should grab the attention of the Sales and Marketing Directors.

For firms that have more than one product, knowing a customer's account holdings is vital in KYC terms both from a ML perspective e.g. "why does this customer have 31 investment accounts?" and from a cross selling perspective e.g. "why are you offering me this account when I already have one?"

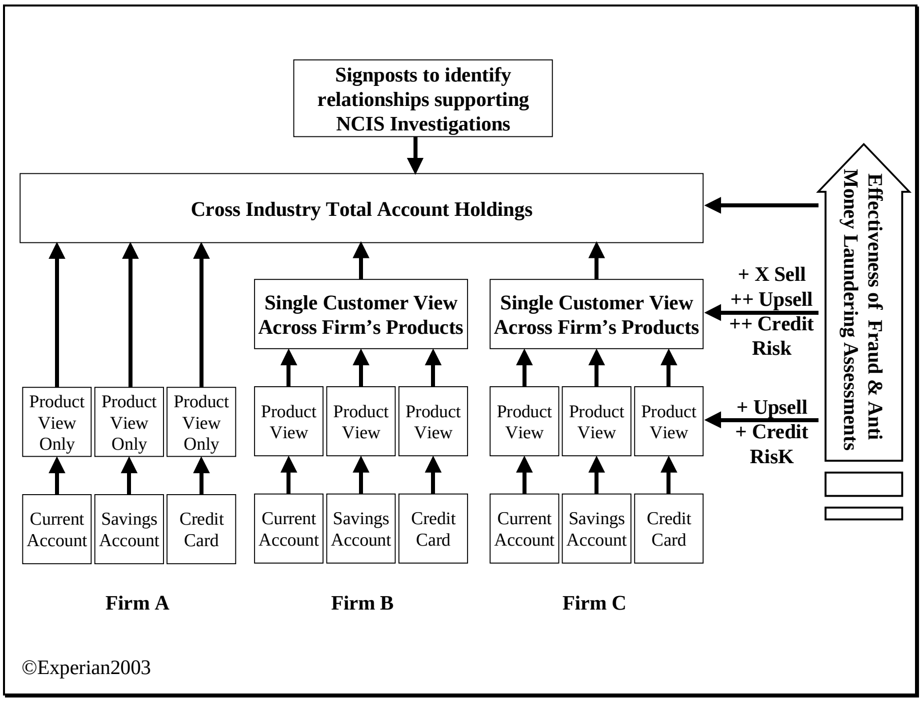
For those firms that do not have a customer database the use of a third party data processor, such as Experian, can provide a platform on which to create a single customer view and incorporate this within a customer monitoring capability.

Having established the ability to create a single customer view within a firm, from a ML risk perspective the ability to create a high level single customer view of an individual across all the firms would be a great asset from the perspective of being able to question "why is this individual opening their 28th bank account?"

Having established a high level single customer view, investigators such as NCIS, could use this view to provide a series of signposts to know where to look when investigating an individual where a suspicious report has been lodged.

The following diagram is a representation of the cross industry total account holdings hub.

Diagram depicting the cross industry total account holding hub: -



This approach would contribute towards more effective fraud and anti money laundering controls as the view of the individual moves from a restricted single product view, where the only data available is associated with the activity relating to the product, towards a complete view of the individual across the firms.

At the level of the single product view, the customer management capabilities are effectively restricted to upselling. The credit risk assessment would not be able to take into account other account holdings that, in the case of investments, may indicate a reduced risk.

At the level of the single customer view within the firm, the customer management capabilities in relation to upselling are significantly improved and cross selling becomes a viable activity. The credit risk assessment capability is also enhanced.

Experian already hosts the Credit Account Information Sharing scheme on behalf of the financial services industry. Experian can, in addition, host the cross industry total account holdings hub.

In addition, scoring and modelling techniques available from experienced providers such as Experian can facilitate an effective and, from the organisation's point of view, a cost effective solution.

6. Conclusion

This paper sets out to provide a contribution to the debate initiated by DP22 and in particular answer the four questions specified in the Executive Summary item 1.8.

In conclusion the key messages are: -

- Anti ML controls need to be viewed as a core element of the firm's business
- KYC data and processes should be viewed as a firm's corporate asset
- KYC is not just about anti money laundering controls
- KYC and Monitoring play a vital role in the anti money laundering controls
- KYC data contributes towards the Monitoring process
- Electronic data provides a cost effective and robust source of KYC data
- Identity checks using documentary evidence are expensive and ineffective
- A single customer view within and across firms is a vital element of maximising return
- The key to effective prevention of crime and money laundering is to reposition KYC into a total customer management strategy designed to support the requirements of all concerned thus: -
  - The lender maximises profit
  - The consumer maximises service and gets the advice and products they want and need
  - The Regulator is comfortable that effective controls and checks will prevent the use of the UK financial services sector for the support and perpetration of criminal activity and specifically money laundering.

The UK has the opportunity to demonstrate to the EU and beyond that it has the capability and the resolve to tackle not only the problem of money laundering but also the broader problem of financial crime.

Jim Lound
Experian
30th December 2003

Fidelity Investments®

Oakhill House
130 Tonbridge Road
Hildenborough
Tonbridge, Kent TN11 9DZ
Telephone: (01732) 361144
Fax: (01732) 838886

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

13 February 2004

Dear Mr Shonfeld

DP22 – Reducing Money Laundering Risk

Fidelity is a fund manager engaged in the provision of long-term savings products, fund management and mutual funds to all the major markets of Europe and Asia. Our client base extends from the individual to the pension funds of large multi-national corporations and our response to the Discussion Paper is based on that experience and offered in that context.

We welcome the opportunity to contribute to the discussion on this very important issue. The DP raises some significant and difficult questions, to which our responses are attached below.

However, there is an area which we would like to place front and centre of any discussion on this topic; the need for any UK approach to be compatible, indeed complementary with approaches in other countries. We would expect the UK not only to champion what it believes to be the correct approach in international fora, but to be sensitive of the needs of organisations such as Fidelity which operate across a multitude of borders.

The advent of the EU's Financial Services Action Plan will mean the greater availability and choice of services and products among the citizens of the EU. We can expect cross-border traffic to increase. UCITS3 for example enables more types of mutual fund to acquire the UCITS passport and be offered for sale throughout a soon-to be-enlarged EU. If the UK's approach differs markedly from that in other Member States it runs the risk that firms will find it difficult to develop a single operational model to support a pan-European business.

Should you like us to explain any of our comments or explore the issues further pleased contact me on 01732 777214.

Yours sincerely

Gareth Adams
Executive Director – Regulatory Strategy

RESPONSES TO DETAILED QUESTIONS

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

A business needs to know sufficient about its customer to enable it to:

1. provide services that are appropriate;
2. communicate with the client (both as regards reporting and the taking of instructions); and
3. exercise proper custodianship over any assets in the safe keeping of the business (simple security and anti-fraud measures).

There are instances when a business can treat something as a proxy (or partial proxy) for such information. For example, if dealing with a client through an authorised intermediary, a fund management company should be entitled to rely on the intermediary to select which services are appropriate, and to act as the communication point for that client. Similarly, if a customer provides details of his bank account, then a fund management company ought to be able to send money to that account comfortable that sufficient controls are exercised within the banking system so that money does reach the client and is not diverted.

The amount of information that a business will require of a client over and above these basics will depend upon the nature of the business being offered. As Fidelity does not provide advice we do not request information regarding financial circumstances, occupation or objectives for opening the account. The implication of this is that the suggested supplementary client data to be acquired would serve no business purpose, and would be cost for no direct benefit.

The collection of KYC information within the money laundering deterrence context serves two purposes. At one level it acts as the establishment of identity, so that those wishing to launder money cannot assume a fake or otherwise innocent identity to "own" the transactions. At another level it can provide the basis for determining what an unusual or suspicious transaction is for that customer.

It would be naïve to believe that identities cannot be easily created or stolen. Indeed identity theft has been rising up the list of law enforcement priorities as instances have mushroomed, powered by technology such as the internet which makes identity theft and the exploitation of a stolen identity so much easier. It is not to be condoned, but it is, increasingly, a fact of life.

Two questions have to be asked about the effectiveness of a KYC requirement within the context of this purpose. Does it deter people from using the financial system for money laundering? Does it assist with the conduct of an investigation once suspicions have been raised?

Our belief is that it does not act as any meaningful deterrent and our experience of suspicion-based reporting is that few if any questions are raised during the acquisition of verification information.

However, we do accept that it may be helpful to firms and indeed to law enforcement authorities when investigating a case.

The other level at which KYC can operate is as setting the context for what is appropriate or normal as regards the operation of the account. Paragraph 3.7 suggests some of the extra information that might be requested to assist in this. Our concern is this. A money launderer is unlikely to respond to any of the questions suggested with something that would cause his planned transactions to be viewed as suspicious. His answers will either be appropriately tailored or sufficiently vague to allow sufficient flexibility of action and so render any monitoring based on the answers to be ineffectual. Self-certification is almost certainly self-defeating in this instance. If, on the other hand, a firm were required to vouch for or audit the information provided this would create an unmanageable burden for the industry.

In terms of developing automated systems for the monitoring of unusual or suspicious transactions, it is not possible, within the context of the more affordable systems, to have an entirely open-ended range of parameters against which to measure account activity. We would also stress that for a fund management company the behaviour of a client as regards his or her long-term savings is not necessarily conditioned by their day to day circumstances. While anti-fraud systems in place at credit card companies can access detailed past spending patterns and match those to purchases, no such comparability exists in the fund management world.

We do not therefore see increased KYC information as being necessarily valuable in assisting with the development of automated monitoring systems

Where we feel that KYC information may be useful is once a suspicion has been raised. In the review of a specified account it is possible to use KYC-type information to assist in determining whether or not to make a disclosure. We would argue that much of the information necessary can be acquired from a variety of sources external to the firm and that acquiring them within the conduct of a specific enquiry is not unduly burdensome. In fact it allows for up-to-date and targeted information gathering. The mass acquisition of client data (with the concomitant need to update regularly) just in case it might one day come in useful would be generally burdensome and useful in only the smallest number of cases.

We have been concerned for some time that regulators' focus on KYC procedures has meant that insufficient thought and resources have been deployed in the active monitoring of accounts. The focus has been very much on ensuring that the client files are up to standard so that they can be checked by inspectors. Given our reservations about the value of such KYC data, it has been frustrating to have expended the amount of effort that we have on this aspect of money laundering deterrence.

While identities can be relatively easily stolen or faked, it is far harder for a money launderer to hide the fact that money of a certain size is moving from one place to another with a certain frequency. If this is accepted, then it forms the basis for an active risk-based monitoring policy based on the structure of the account and the transactions – and does not require volumes of background information.

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

As far as the regulator will permit.

There are certain financial products which are less attractive to the money launderer. Pensions, for example, require more work to be done in terms of setting up an identity, have relatively modest limits as to what may be invested, and are inflexible as to withdrawals. ISAs and PEPs have, again, modest investment limits, require an identity that works as regards the Inland Revenue, and are not available to trust or corporate account holders. Products that are more attractive include those with the ability to make payments to third parties, withdraw cash or write cheques, have short instruction-to-execution lead times and where a trading type of activity will not look out of place.

This is not to suggest that fund managers should be complacent about the risk of money laundering, but that objectively they are less likely to be targeted. Set against that, we expect the money laundering typologies to be more sophisticated in the fund management world. To the extent that NCIS and other interested authorities are able to share and educate the fund management industry on how they are used and abused by the launderers that would be helpful. It would help not only in raising the bar for many firms, but also in helping establish a consensus for what constitutes good market practice.

Our concern with a risk-based approach is that a subjective series of judgments by the firm are later subjected to a subjective series of judgments by the regulator in the light of different experience and events. We do not disagree that judgements must be constantly re-evaluated and re-assessed, but are concerned that if firms believe they will always be second-guessed by someone who has the answer sheet they will be dissuaded from adopting a risk-based approach and will adopt systems designed to appease the regulator, not those systems which actually might be effective deterrents and detectors. Firms which arrive at a wrong decision but in good faith and in the right way should not be penalised as if they had made the wrong decision for the wrong reasons.

The 2004 JMLSG Guidance Notes, while imperfect, represent a very decent distillation of industry thinking and offer an opportunity to build market practice. It would make firms more confident in adopting a risk-based approach informed by these Notes if the FSA could afford them some form of official recognition.

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

While the agencies themselves are best placed to respond we have some thoughts based on our own experiences. There is little that matches the intervention of a thoughtful and informed individual, experienced in the business and mindful of the money laundering threat, in the processing of client transactions. As more and more of processing moves to a straight-through basis the challenge becomes how to ensure that quality of oversight in a more automated environment. Particularly in the world of fund management we have some scepticism about the use of automated monitoring other than as a very basic filter for patterns that might be of concern.

Our focus has to be on quality as against quantity and believe that is what the agencies would wish us to focus on.

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

We believe that most businesses are perfectly well aware of the value of client data in respect of how it can drive the business and enable the business better to serve the clients' needs and therefore collect what they need. Given that, any increase in the amount of KYC information would have to be justified purely in terms of the potential to increase the quality of a firm's money laundering deterrence. As stated above, we do not see that the indiscriminate acquisition of data and the need to keep it up to date add to quality. We also acknowledge that KYC information can be useful once a suspicion has been raised, but believe that it is more efficient and effective to acquire that information only as and when required at a time when we have a focus and the information will be up-to-date.

Monitoring clearly has a role to play, but only if it is attuned to the risk-profile of the organisation and the particular characteristics of the product being offered. If not, not only will you generate lots of "false-positives" that will gum up both firms' and law enforcement agencies' resources, but you also run the significant risk of missing the real launderer in all the background noise.

Q5. Which options presented do you prefer and why?

There has been a very significant amount of change in this area of regulation and precious if any feedback as to the effectiveness of those changes. We therefore believe that the FSA should review again in two years' time – Option 4. We would urge that the FSA use that time to:

> Research with firms and law enforcement agencies which techniques and methods of information-gathering and monitoring generate the best quality reports and share that with the industry
>
> Research with firms what type of information (e.g. re typologies) and feedback they would find most helpful from law enforcement agencies (as well as pursuing what those agencies say in response to Q3). We believe that FSA has a role to play building co-ordination and synergy between the industry and the various parts of the establishment involved and that there remains un fulfilled potential in that role.
>
> Build consensus with its EU partners as to a set of European-wide standards (perhaps similar to the JMLSG Guidance Notes)

Financial Services Consumer Panel
AN INDEPENDENT VOICE FOR CONSUMERS OF FINANCIAL SERVICES

Tel: 020 7066 9346
E-mail: enquiries@fs-cp.org.uk

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

30 January 2004

Our ref: WGA

Dear Daniel

DP22: Reducing Money Laundering Risk

The Consumer Panel welcomes the opportunity to comment on DP22 and it naturally welcomes the government's initiative in seeking to reduce money laundering and financial crime, which is ultimately always paid for by the customer. It is supportive of the thrust of the proposals, many of which are anyway central to good business practice. Nonetheless, there are many aspects of the proposals which indicate inadequate consideration of the impact on consumers, particularly the most vulnerable consumers.

The main comments the Panel would wish to make concern 'Know Your Customer' and identification verification rather than monitoring.

Firstly, the FSA (and the government) is also committed to extending the range of people who use financial services, whether to save or by opening a bank account for the receipt of benefits and pensions. We are particularly conscious that there are large numbers of consumers currently trying to open a bank account for the first time and that this trend is expected to continue. These potential new customers are likely to include older consumers who are unused to dealing with banks, those for whom English is not a first language and individuals with learning difficulties. In June last year the Banking Code Standards Board carried out a 'mystery shopping' exercise[1] to assess whether banks and building societies were offering basic bank accounts to potential customers whose banking needs would be met in this way. Only a little over half of the mystery shops resulted in the right account being offered and the BCSB concluded that "training is especially needed on requirements of identification. Even when the decision on acceptability is taken centrally or regionally, staff need a greater appreciation of the alternative documents that may be acceptable where applicants can legitimately not produce 'primary' documents."

[1] Banking Code Standards Board "Survey of Subscriber Institutions on Basic Bank Accounts" published July 2003

We are therefore anxious that no guidance (or rule) should be proposed which does not take account of potential inconvenience or embarrassment to the consumer, or which effectively excludes certain groups from such services. Many of those currently outside of the sector cannot easily provide the standard or 'primary' ID verification documents; we would be concerned that a recommended list might add to the difficulties facing such people. Similarly, over-intrusive questioning or long delays in acceptance might put off potential new entrants to the sector. (This could actually lead to further crime, as unbanked money is more vulnerable to crime.) It is essential that rules and guidance are both proportionate and flexible. Account should also be taken of the risk-averse environment in which firms operate. In the Panel's view some banks' internal communications processes leave a great deal to be desired. In the absence of clear guidelines, branch staff are likely to turn new customers away if they are uncertain about, for example, the various types of 'alternative' identification which should be acceptable, as indicated by the BCSB research. Banks must ensure that their branches are fully aware of the broad parameters within which they can operate, exercising their judgement fairly and sympathetically when deciding whether to open an account for a new customer. Any proposals should therefore be "stress-tested" with likely new customers from a range of different groups before being implemented.

Secondly, whilst KYC information is needed for many services, we would have some concerns if details obtained for anti-money laundering purposes was then used for marketing (without the expressed agreement of the customer). This could act as a disincentive to provide such information.

Thirdly, as ever more detailed questions are demanded for ID verification (the current raft being about first and last schools, and a "memorable" name), it will be important that good consumer information and awareness work also takes place so that individuals understand why such interrogation is taking place. We are confident consumers will be content to be helpful if they know the rationale, but could resent such cross examination for no apparent reason.

Lastly, we trust that any CBA will include the cost to customers as well as simply any costs to providers.

Yours sincerely,

Chairman
Financial Services Consumer Panel

FRIENDS PROVIDENT
Friends Provident Life and Pensions Limited
Pixham End, Dorking, Surrey, RH4 1QA
Telephone 0870 608 3678 Fax 01306 740150

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

2 February 2004
Our Ref: KAJ/KB/1002

Dear Mr Shonfeld

DRAFT RESPONSE DP22 REDUCING MONEY LAUNDERING RISK

We welcome the opportunity to comment on the Discussion Paper 22 – Reducing Money Laundering Risk.

First, I should like to comment on the three general issues raised in paragraph 5.16.

1. The measures that we have in place to prevent money laundering, facilitate its detection and monitor its incidence are as follows:

- Having an appropriately considered and documented approach to money laundering controls within the organisation and communicated accordingly.
- The existence of a person specifically appointed as MLRO, together with a team of people in support.
- Appropriate systems and controls within the organisation to ensure staff understand their responsibilities, report their suspicions, which are evaluated and reported to NCIS where necessary.
- Training and record keeping provisions.
- Systems and controls, both automated and manual for monitoring, the recognition of and reporting suspicions.

2. It is difficult for us to estimate ***"the actual or potential costs of an active, but risk based approach by firms to KYC and to monitoring"*** since many of the costs associated with our anti money-laundering arrangements are spread throughout a number of departments.

3. Are firms ***"confident that they understand our regulatory requirements and what we expect of them"?*** As with all financial firms, Friends Provident has had anti-money laundering procedures in place even before the FSA had a specific statutory duty in relation to this matter. We are confident that we understand the regulatory

requirements (both the FSA Rules and the Joint Money Laundering Steering Group Guidance notes) and that appropriate information has been given to (and is constantly available to) our staff. The number of SARs received by the MLRO indicates that people are alert to their responsibilities.

However, we recognise that this is not static and that we must remain vigilant to emerging issues. The FSA have, rightly, talked about adopting a risk based approach to money laundering but there does not seem to be a consistent statement of what it considers these risks to be. This, coupled with the lack of relevant feedback from NCIS on they use the information to detect cases, could lead to the accusation that the FSA is taking a too theoretical approach to the subject with insufficient consideration of the impact on different types of firms.

Turning to the specific questions raised in 5.17, we would comment as follows:

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

We appreciate there is a need for KYC information to be collected in order to pass on meaningful data to the law enforcement agencies. However, a balance has to be struck between collating sufficient information to allow these agencies to effectively do their work and too much information which could be seen as intrusive by customers, the vast majority of whom are law abiding citizens. In addition, the extra costs on firms required to gather the information could escalate disproportionately.

Notwithstanding the above, we believe that a certain amount of KYC data should be collected and that a risk-based Anti-Money Laundering programme is essential in order for firms to be effective in managing their substantive money laundering risks and associated reputational risks.

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

The existing JMLSG Guidance steers firms to the factors that they should be taking into account when determining their risk profile. In our own case, we do not handle cash, the majority of our customers are introduced through other authorised firms, premiums for regular premium business are collected by direct debit with UK banks and more and more payments to customers are paid directly into the same bank account. Information of this type will enable firms to make their own assessment of the risks that they will be used for financial crime purposes.

At a more general level, we feel that the FSA has an important role to play in setting out its views on the particular risks presented to different sectors and what factors they consider when making those assessments.

While we understand that some (particularly smaller) firms would appreciate more guidance in the FSA Handbook, we would prefer to rely on the updated guidance issued by the JMSLG for the practical day-to-day regulations. This will avoid duplication and associated confusion. If the FSA believes that it should issue more guidance, then it should be the sole reference point for firms.

Q3 ***What type of monitoring, and reports would be most useful to law enforcement agencies?***

Information passed on to the law enforcement agencies must be accurate, relevant and timely and the most useful monitoring is likely to be in respect of unusual and significant transactions related to high risk products and customers who in themselves could be regarded as high risk e.g. "politically exposed persons (PEPS)".

It is important that firms are not put in the position of being the detectives and doing the law enforcement agencies work for them. Procedures are already in place for reporting individual suspicious transactions and most firms will be able to spot trends. It is the responsibility of the law enforcement agencies to assess all of the information it receives and investigate as appropriate.

The emphasis at the moment appears to be on "defensive reporting", and Carol Sergeant's letter of September 2003 to Chief Executives regarding multiple transactions needs to be taken on board, as she seems to be suggesting a way forward to reduce the number of transactions reportable where there is a clear link between them. In line with her comments, we support the view to remove/reduce defensive reporting.

The introduction of POCA has seen the number of reportable cases increase considerably and in the main, has been attributed to individuals now being concerned about by the consequences of not reporting. A focussed approach needs to be found to prevent/avoid large-scale notification merely for the sake of it.

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

We fully support the position that we need to take responsibility for the collection of Client Identification information. However, we should not look at this question in respect of regulated firms alone, but the entire process incorporating the regulators and law enforcement agencies as well.

We collect KYC information ourselves in the case of direct business and via intermediaries for the rest of our business. The information gathered from these sources, together with information obtained from additional monitoring, both electronic and observation, forms the basis of any report to the law enforcement agencies of suspicious transaction

Additional information collation and further reporting requirements mean more cost for firms which will inevitably be passed on to the customer. We must be satisfied that these additional costs bring a real benefit to the financial services industry. An important factor in understanding what additional benefits are delivered is to receive relevant and meaningful feedback from the law enforcement agencies on how the information provided to them contributes to the detection of financial crime.

Q5 Which options presented do you prefer, and why?

We feel that at this stage a combination of options 3 and 4, would seem to be most appropriate, especially as the main guidance to the industry from the JMLSG is due to be revised, as well as further directions expected from H.M Treasury in light of the KPMG review. Any significant additions made to the Sourcebook at this time would seem to lead to both confusion and duplication.

Allowing the position to bed down for a while and review again in 2005 would seem to be a sensible approach, which we would welcome.

We hope that our response will be of help to you, but please do not hesitate to contact us if you require any further information.

Yours sincerely,

K.A. JOHNSON
COMPLIANCE MANAGER

FSA Discussion Paper 22: Reducing Money Laundering Risk

A Response by the FOA to the FSA's Discussion Paper

January 2004

DP22: Reducing Money Laundering Risk

1. Introduction

1.1 The Futures and Options Association (FOA) is the industry association for some 160 firms and institutions, which engage in the carrying on of derivatives business, particularly in relation to exchange-traded transactions. The FOA's membership includes banks, brokerage houses and other financial institutions, commodity trade houses, power and energy companies, exchanges and clearing houses, as well as a number of firms and organisations supplying services into the futures and options sector.

1.2 The FOA welcomes the publication of DP22: *Reducing Money Laundering Risk* (DP22) and commends the Financial Services Authority (FSA) for fostering debate on Know Your Customer (KYC) and monitoring. As the FSA has acknowledged, DP22 deals with areas of varied industry standards. The FOA hopes, therefore, the debate will assist in resolving the significant uncertainty that firms face in this area, particularly with respect to risk-based approaches to anti-money laundering, and will lead to a proportionate and more uniform regulatory response. In general, the FOA believes that pre-consultation debate is essential to give the industry an opportunity to provide input to the FSA's policy development at a formative stage.

1.3 The FOA also wishes to congratulate the FSA on its recent DP22: *Know your customer and anti-money laundering workshop*. The wide cross section of invitees, including representatives from law enforcement and government agencies, led to interesting debates, which illustrated, *inter alia*, the difficulties the FSA will face in attempting to reconcile the views of all interested parties. The FOA believes, however, that this workshop was a very useful exercise, which the FSA should repeat in future.

1.4 The FOA agrees, in principle, that firms will need KYC information and transaction surveillance in order to satisfy their legal obligations under the Proceeds of Crime Act (PoCA) and the Money Laundering Regulations 2003 (the Regulations). Whilst the FSA has acknowledged that "*there are no specific legal or regulatory requirements*" for KYC and monitoring, we do question the extent to which the existing high-level regulatory obligations in SYSC referred to in DP22, can be construed as "*relevant*"[1] to KYC and monitoring.

1.5 In particular, we note that firms wishing to carry out a current customer review may apply to the FSA for a variation of Part IV permission to include a requirement on their permission, and hence a legal obligation, to access the full electoral register where appropriate. This is illustrative of the fact that legal opinions differ regarding the extent of the regulatory obligations created by SYSC 3.2.6R. Hence, if there is doubt as to whether SYSC 3.2.6R extends to identification of existing customers, there must be even greater doubt as to whether it is relevant to KYC information concerning, and monitoring of, these customers.

[1] DP22, para 4.3

1.6 Additionally, SYSC 3.2.6R requires firms to "*take reasonable care to establish and maintain effective systems and controls…*". Arguably, this duty of "*reasonable care*" may be satisfied otherwise than through formal transaction monitoring. Indeed, we would suggest that 'surveillance' rather than "*monitoring*" is a more appropriate term, since the former includes staff keeping a close watch over transactions (otherwise referred to, as "*passive*" monitoring) whilst the latter includes a more routine element (i.e. active monitoring) which may not, necessarily, produce better results.

2. Know your customer

2.1 In theory, FOA members agree with the majority of the FSA's comments with respect to the importance of KYC information and its usefulness in managing money laundering risks. The FOA's main concerns with regards to the KYC section of DP22 are, however, of a more practical nature.

2.2 Clearly, to be able to identify what is suspicious, a firm has to have an understanding of what is normal, so far as it is able to identify, for a particular client. Systems that use KYC information to flag transactions requiring attention are already in use in the banking/credit card industry. However, whilst it may be relatively easy for a retail bank to be able to identify regular income and expenditure patterns for retail clients, as the FSA recognises in paragraph 3.16 of DP22, it is harder to do so when clients diversify their investment portfolio across a number of providers. It is even harder still, when the client is an authorised person, acting on behalf of its underlying clients, that trades with any number of counterparties, depending on, inter alia, factors such as the investment, trade costs etc. The FOA believes it is important that the FSA appreciates fully the difficulties of obtaining KYC information from clients in wholesale relationships, such as give-up arrangements, that generate considerable, but variable, volumes with minimal contact. In these circumstances, it is unlikely that Executing Brokers operating in the wholesale markets will be able to profile their clients, other than to identify the product range and markets in which they normally trade.

2.3 Paragraph 3.7 of DP22, details the KYC information suggested in the good practice documents in Annex 4. We note that this list includes information that is predominantly focused towards private customers / retail business (e.g. "*source of wealth or income")* or which, as discussed above, is difficult to obtain for wholesale clients, (e.g. *"the anticipated level…of the activity that is to be undertaken*"). The FOA believes, therefore, that the FSA should conduct additional research with wholesale market participants to ascertain the type of KYC information that could be obtained in respect of clients in these markets and the likely benefit of this information to law enforcement agencies. As ever, the FOA would be happy to facilitate further discussion on theses issues, should this be of assistance to the FSA.

2.4 If the FSA were to implement risk-based rules that required firms to take "*reasonable steps*"[2] to obtain KYC information, senior management of firms would have the flexibility to design 'tailor made' procedures, rather than having to

[2] DP22, para 5.6

follow a 'one-size-fits-all' approach. However, such provisions would also give senior management more responsibility and without the clarificatory guidance from the FSA (as opposed to the JMLSG Guidance Notes, as indicated in paragraph 5.7 of DP22) senior managers may feel nervous that their judgment of what is appropriate could be open to challenge from the FSA on a case-by-case basis. In addition, given the differences between firms (such as, type of business, client base, overall size and also whether it is part of a large group structure with access to, and support of, larger IT departments and bigger compliance budgets), even within the same industry group, the approaches adopted by firms to comply with risk-based rules will, necessarily differ. It is important, therefore, that the FSA develops risk-based supervisory processes for anti-money laundering, which focus on the effectiveness of systems and controls and which, are not perceived to be 'second guessing' managements' decisions with the benefit of hindsight.

2.5 The amount of KYC information available in the wholesale markets also tends to vary and, in some circumstances, information may be minimal; for example, for execution-only clients who do not have direct contact with the firm or who trade infrequently. It could be argued, successfully, that these circumstances are higher risk but this does not resolve the problem of collecting KYC information. Furthermore, electronic order routing, whereby clients execute their own transactions electronically using the exchange membership of a firm, is a growth area in the derivatives and equities industry (as execution costs are lower to the client): this practice means that the contact with firms is reduced.

2.6 The FOA does not believe that the issue of maintaining and keeping KYC information up to date is considered adequately in DP22. The FOA notes that the FSA has acknowledged that having obtained KYC information "*it may not be easy for the firm to maintain it*."[3] The FSA has, however, stated: "*It would not seem practical, however, to expect firms to oblige customers generally to update the information that the firm has when a material change of circumstances occurs.*"[4]

2.7 Under the Fourth Principle in the Data Protection Act 1998, firms will be required to ensure that KYC information, to the extent it falls within the definition of personal data, is "*accurate and, where necessary, kept up to date*". The FOA believes, therefore, that it is important that the FSA works with the Information Commissioner to provide firms with legal guidance on the steps they will be expected to take to verify the accuracy of, and keep up to date, KYC information.

3. Monitoring

3.1 The FOA welcomes the FSA's statement that "*what monitoring involves in practice will vary according to the type of business a firm does…*"[5] The FOA is also pleased to note that the FSA has recognised[6] the fact that detecting "*unusual*" activity is more difficult in remote relationships, particularly where clients have multiple relationships.

[3] DP22, para 3.19
[4] DP22, para 3.19
[5] DP22, para 1.5
[6] DP22, para 4.8

3.2 As discussed in paragraph 1.6, the FOA believes that staff awareness/transaction surveillance is necessary to satisfy the legal obligations of firms. It is important, however, that any regulatory provisions recognise that surveillance may, in certain circumstances (depending on the risk profile of a firm's business), be carried out by trained staff that have the ability to recognise potentially suspicious transactions, rather than by a routine monitoring process. It is important, therefore, that regulatory provisions do not specify that a particular type of monitoring per se. must be used (or not used) by firms. The FOA is pleased, therefore, that DP22 "*is about both automated and non-automated approaches to monitoring...*" and that the FSA has stated that a firm's "*systems and controls may, but need not, include an automated element*."[7]

3.3 Automated monitoring systems clearly have many advantages, provided exceptions are defined clearly. The FOA recognises that "*the greater the volume of transactions, the less easy it will be for a firm to do without the aid of automation*."[8] That said, however, FOA members are concerned that the use of automated systems may become the benchmark against which all firms are judged. The FOA believes that it is important that the FSA recognises explicitly the relative merits or the full spectrum of monitoring, from staff awareness through to sophisticated automated monitoring systems. It is also important that senior management are given the flexibility to determine the type of monitoring that is the most appropriate for their business and the risk posed by, inter alia, the firm's services/products and customer base. The FOA believes that automated monitoring systems should not seen as a panacea: smaller firms may find that the cost of installing automated systems far outweigh any benefits and even firms using such systems should not lose sight of the need for non-automated monitoring (through 'staff awareness' etc.) to identify suspicions arising, for example, from direct contact with clients.

4. Risk-based approach

4.1 We note that a risk-based approach to anti-money laundering is "*what we* [the FSA] *expect of firms*."[9] The FOA agrees that without "*a risk-based approach firm's costs will be diluted, and the regime will also be overly burdensome for customers."[10]* We question, however, whether the FSA "*Handbook already requires it*," as SYSC 3.1.2G, which is referred to in DP22, is guidance and "*guidance…is not binding on those to whom the Act and rules apply, nor does it have 'evidential effect*."[11] SYSC 3.1.1R, which the guidance amplifies (although the guidance "*need not be followed in order to achieve compliance with the relevant rule…*"[12]), requires a firm to "*take reasonable care to establish and maintain such systems and controls as are appropriate to its business." Arguably, "appropriate"* may not necessarily be *"risk-based*."

[7] DP22, para 4.2
[8] DP22, para 4.23
[9] DP22, para 2.6
[10] DP22, para 2.6
[11] Readers' Guide, para 29
[12] Readers' Guide, para 29

4.2 The FOA agrees that a risk-based approach to anti-money laundering will require access to KYC information and transaction surveillance. That said, the biggest disincentive for firms when considering whether to move to a risk based approach is not lack of KYC information or transaction monitoring, but a concern that the FSA, with hindsight, may criticise the firm's risk assessments. There is also a concern that a risk-based approach to anti-money laundering may not satisfy legal obligations, for example, a risk-based approach does not fit with the requirement to verify the identity of clients or the requirements of the Terrorism Act 2000/Anti-Terrorism Crime and Security Act 2001. Hence, many Money Laundering Reporting Officers consider a risk-based approach to be inherently more risky than a uniform approach, since it is felt, arguably justifiably, that it creates greater corporate and personal liability. Notwithstanding the options in DP22, the FOA believes that it would be helpful for the FSA to issue clarificatory guidance on the factors that a firm (or the FSA) should (or will) take into account when developing (or reviewing) a risk-based approach to anti-money laundering.

4.3 In addition, as discussed previously, given that a risk-based approach to anti-money laundering will result in different approaches being adopted by firms within the same industry group, FOA members believe that it is important that the FSA develops risk-based supervisory processes for reviewing the approaches developed by firms.

5. Specific Questions posed by FSA

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

The FOA believes that both the collection of KYC information and transaction surveillance are necessary to reduce money laundering risk and meet legal requirements, although, as discussed previously (c.f. paragraph 1.4 et seq.), we question whether extant regulatory requirements extend to KYC information and monitoring. The FOA also questions whether an "*active*" approach to monitoring, necessarily, produces better results than surveillance through, inter alia, staff awareness (see paragraphs 1.6 and 3.2).

It is important, however, that the KYC information and transaction monitoring required by regulatory provisions is effective in terms of costs and benefits; that is, the KYC information collected, and monitoring performed by firms need to be meaningful for law enforcement agencies, rather than a 'form over substance' approach to satisfy per se. regulatory requirements. It is also important that there is recognition of the fact that, even if a firm does obtain KYC information and perform transaction surveillance diligently, it will not mean, necessarily, that the firm is able to eliminate the risk of money laundering and different firms may not be able to reduce the money laundering risk to the same extent.

As an example, an Executing Broker will never have the complete picture in relation to its clients' business, as many clients will use multiple brokers, and sometimes several Clearing Brokers. Hence, it will be very difficult for an Executing Broker to monitor transactions on an exception basis for unusual activity in terms of volume, and even cross-markets, although, such a firm will be able to identify if, for example, a coffee roaster starts trading in another commodity through the same Executing Broker. This may be flagged as warranting further enquiry, but, since clients trading in more than one commodity are not unusual, it may not, necessarily, be a suspicious transaction. As discussed in response to question 2 below, a Clearing Broker may, however, be better placed to monitor a client's activities; assuming the Clearing Broker clears all of the client's business.

Clearly, the more a firm knows about a client, the easier it is, potentially, to spot suspicious activity and hence reduce the money laundering risk. However, there is a concern that what is deemed adequate KYC information today may not, particularly with the benefit of hindsight, be deemed adequate in, say, three years time. Hence, in addition to focusing on the collection of KYC information, it would be helpful if the FSA could give guidance on what they deem to be "*reasonable steps*" to keep KYC information up to date.

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

To develop a risk-based approach, an analysis should be undertaken to assess the risks of a firm being used for money laundering, with reference to a number of factors (if relevant), including, but not limited to:

- Jurisdiction of the client, and effectiveness of anti-money laundering legislation in that jurisdiction, i.e. is the jurisdiction a member of FATF?
- Whether client's bank accounts are held with a credit institution in a FATF jurisdiction?
- Whether the client is a natural or legal person and, if relevant, the type of legal person e.g:
  - Unincorporated body
  - Partnership
  - Privately owned corporate
  - Listed corporate (or subsidiary/associate of listed parent)
  - Financial institution located in FATF country
  - Financial institution located outside FATF country
- Experience/track record of client
- Activities across markets/cross products (as known to the firm)
- Type of service or product

FOA members believe that it should be left to a firm's senior management to analyse the firm's risks and to justify its risk-based approach accordingly. The JMLSG Guidance Notes, which will cover risk-based approaches to anti-money laundering in 2004, will be important in creating a uniform industry practice in this area.

For firms operating in the futures and options markets, it is important to consider, when developing a risk-based approach, whether the client relationship is an executing or clearing relationship.

The ability to identify money laundering within an Executing Broker may be diminished due to the role the Executing Broker has as part of a transaction e.g. it never holds cash. Similarly, a Clearing Broker may only be one of a number of clearers for a client, so may not always be aware of a client's full position. An Executing Broker is at the beginning of the chain in relation to the purchase or sale of derivative contracts, however, it can never know whether a buy or sell transaction is to open or close a position and whether any transaction is part of an exchange or OTC linked strategy. Hence, an Executing Broker is unlikely to have sufficient knowledge to make judgments about the client's trading activities, although it may be able to collect other KYC information that will enable monitoring to be performed on a risk-based approach.

On the other hand, a Clearing Broker retains cash (and / or collateral) as initial margin and will make margin calls from time to time. A Clearing Broker, may also be aware of its clients' trades/strategies, but only if all transactions were cleared through it: even then, a Clearing Broker's ability to understand a client's strategies may depend on the sophistication of the client. A Clearing Broker is, therefore, better placed to monitor a client's activities for unusual transactions, as it may see all activities (assuming it clears all of its client's business) and particularly, source of funds and details of bank accounts.

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

In the FOA's opinion, this question should be answered by the law enforcement agencies; however, the FOA believes that it is important that firms appreciate the needs of these agencies, particularly with respect to the value of information. In the past, as the FSA is aware, there has been a paucity of feedback from NCIS or law enforcement agencies. The FOA is, however, pleased to note the improvements being made by NCIS, and others, in this area; for example, the NCIS *Current Intelligence Assessments* and the new *Proceeds of Crime Update: Money Laundering News,* produced by the Assets Recovery Agency. The discussions at the FSA workshop were also of particular interest; for example, the comments that KYC information on source of funds is often more valuable in an investigation that evidence of identity, which can be forged. That said, the FOA wonders whether the Money Laundering sourcebook (ML) should clarify the need to report irregularities identified during the account opening process, for example, identification of a name on a public list, which will require a report under the Terrorism Act 2000 and the Anti-Terrorism Crime and Security Act 2001. As the FSA is also aware, following the KPMG Review of the Suspicious Activity Report regime, a task force has been established to, inter alia, consider and implement the recommendations of KPMG. We, therefore, believe it appropriate for the FSA to await the completion of this task force review, before considering this issue in further detail.

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

Collection of KYC information, and effective surveillance of transactions may assist firms in reducing their legal, regulatory and reputational risks; in particular the risk that a firm could be used by money launderers.

However, depending on the assessment of "*adequacy*", collecting KYC information could be labour intensive, particularly if information is gathered from independent sources or if information provided by clients needs to be verified. Whilst identification verification information clearly needs to be verified, FOA members would have significant concerns if there was a requirement to verify all KYC information, since, amongst other things, this could have significant cost/resource implications.

It could be argued that non-automated surveillance has cost implications in terms of ensuring staff are adequately trained to monitor effectively; that said, the FOA recognises that the Regulations require firms to "*take appropriate measures so that relevant employees are…given training in how to recognise… transactions which may be related to money laundering."* In terms of automated systems, implementing exception reporting is also expensive in terms of both developing and/or buying packages to fit the business, which is why a risk-based approach must be adopted to be cost effective. It is essential to avoid the 'form over substance' stance, where exception reports are produced only to satisfy the FSA that monitoring is being performed, since rarely will such monitoring result in a SAR. However, invariably, one package cannot cover all business activities, particularly as different execution platforms are used, and different back office systems for derivatives, equities, fixed income and prime brokerage activities.

Hence, provisions requiring a firm to collect KYC information or "*actively*" monitor transactions are likely to have resource implications for firms, resulting in either additional costs, or, the de-emphasising of other tasks. In addition, if firms are required to gather significant amounts of KYC information, there is a concern that business may be lost to other jurisdictions where KYC requirements may be less onerous for clients or firms. There is evidence that some clients are already choosing to open accounts with overseas brokers rather than go through the AML customer identification procedures, which include gathering the KYC information set out in the JMLSG Guidance Notes, required by UK brokers.

Q5: Which options presented do you prefer and why?

The FSA's workshop on DP22 demonstrated the difficulties of reaching a consensus with respect to anti-money laundering. In simplistic terms, we believe that the views of firms are strongly polarized - although not evenly weighted – between those firms that would prefer more detailed guidance on the FSA's expectations and those firms that believe that, rather than create clarity, additional FSA provisions could result in overlap, potential conflict and confusion between ML and the JMLSG Guidance Notes.

This response was compiled on the basis of views expressed by the FOA's Anti-Money Working Group, which has 35 members representing investment banks, clearing houses and executing brokers and commodity market participants. It is important to note that: (a) not all members of the Working Group expressed a view on the options in DP22; and, (b) a unanimous consensus was not reached in favour of one particular option. Instead, as discussed below, support was shown for Option 1(c) and Option 3 (which is considered similar to Option 4 in terms of outcome): Option 4 (either in its own right or in combination with Option 1(c)) was, however, the preferred option of the majority of FOA members who expressed a view. It is important to recognise, however, that these outcomes may not, necessarily, reflect the views of all members of the FOA.

In general, FOA members agreed that firms should have to account for the level and effectiveness of their transaction surveillance and the quality of their KYC information. With respect to the options, which we note are not mutually exclusive, our detailed comments are as follows:

Option 1:

Include in the Handbook specific rules and/or guidance on KYC and/or monitoring,
(a) New specific rules
(b) New specific guidance
(c) Extend the specific link between ML and the Guidance Notes beyond identification to cover (at least) KYC and monitoring.

- **Options 1(a) and (b)**

  Many FOA members see little benefit in making further additions to the FSA Handbook, and in particular the ML, at the present time. The FOA understands that the FSA has indicated recently its concern that UK firms may have difficulty in keeping pace with the number and variety of regulatory developments at European level. Any significant alteration to existing UK Money Laundering rules will only add to that burden, particularly as the EU is now turning its attention to a 3rd Money Laundering Directive.

  Many firms are only now coming to terms with the full extent of the money laundering requirements, of which ML forms but a part. To make a significant addition to that structure, without adding clarity with respect to firms' legal obligations, could, therefore, be seen as unduly burdensome for some firms. It is also clear that the new Regulations will need time to be fully tested.

  In any event, regardless of the current problems of timing, it is not clear that new specific FSA provisions will ever be appropriate. The recent FSA seminar made it clear that the vast array of issues that arise in different sectors means that a one size fits all approach is never likely to work in practice. Indeed, there are so many sectoral differences as regards the appropriate approach to KYC information and, particularly, monitoring that rules or guidance would have to be either so vague as to add little of significance or so specific as to significantly increase the size of ML. There is also a concern that, rather than create clarity, new, specific, FSA provisions could result in overlap, and potential conflict and confusion between ML and the JMLSG Guidance Notes; this is particularly important as FSA guidance will be based on the FSA rules whilst the JMLSG Guidance Notes give guidance on the criminal law.

  Finally, and perhaps most importantly, if the Government felt it unnecessary or inappropriate to introduce specific obligations regarding KYC information and monitoring, FOA members wonder if it really is appropriate for the FSA to promote the implementation of such provisions using its own powers. Any FSA rules could create a significant additional burden, which may not have been intended by the Treasury (or the European legislators). To link the new specific provisions to the overarching legislative framework, the FSA would effectively need to state what they believe the Treasury intended when they referred to '*such other procedures of internal controls and communications as may be appropriate'* in the Regulations[13]. What should be deemed reasonable by reference to this requirement is surely a question of fact and degree and one which can only be answered with full knowledge of a specific situation (or at least of a specific industry) on a case-by-case basis. It is arguable that additional FSA rules or guidance would merely restrict, contradict or otherwise interfere with the intentions of the legislature.

∉ **Option 1(c)**

As the JMLSG Guidance Notes are being re-drafted to cover KYC information and monitoring, **a number of FOA members have expressed a preference for Option 1(c) (either in its own right or in most cases, in combination with Option 4),** provided the specific link to the JMLSG Guidance Notes is by way of high-level guidance (c.f. ML 3.1.4G).

Option 2:

Include new high-level rules or guidance, or both, on money laundering risk management.

FOA members believe that the current position, that is, the FSA Handbook sets high-level standards while the JMLSG guidance sets out more detailed industry-specific guidance, should be retained and strengthened going forward. However, as discussed above, FOA members see little benefit in making further additions to the FSA Handbook in respect of anti-money laundering.

There is a concern that the expression 'high-level' is often translated as meaning vague or ambiguous. The suggestion that firms should be required to document their money laundering procedures under FSA rules would do nothing to assist firms in understanding the extent of the obligations under the similarly 'high-level' obligations in the Regulations. Again, although it will depend on the drafting of any rules or guidance, this option seems unlikely to assist firms in understanding the precise extent of their day-to-day obligations, which go wider than ML.

Since the FSA are approaching the area of risk management through their operational risk initiatives and SYSC, we question, therefore, whether there should be detailed provisions specifically covering money laundering risk, as opposed to more general risks facing a firm. In addition, as the FSA provisions are likely to be generic in nature, they are unlikely to address specific circumstances in way that the JMLSG Guidance Notes endeavour to do; indeed, as discussed previously, there is a risk that new FSA provisions may create conflict with, rather than reinforce, the JMLSG Guidance Notes.

13 Regulation 3(1)(b)

Option 3:

Leave ML unchanged; rely on the JMLSG Guidance Notes

The FOA believes that Options 3 and 4 are closely linked and, in the short term, represent very similar outcomes. **Some FOA members are supportive of both Options 3 and 4**, on the grounds that, given the amount of change, the industry needs time to take account of the new Regulations and the 2003 and 2004 JMLSG Guidance Notes (not to mention the 3rd EU Money Laundering Directive), without further prescription from the FSA. **However, the support for Option 3 is conditional on it not precluding the FSA from taking future action in this area** and a few members expressed concern that reliance solely on the JMLSG Guidance Notes may raise potential competitiveness issues**.**

FOA members believe that, in general, the JMLSG guidance notes have worked fairly well to raise standards within the industry. The current arrangements provide detailed guidance that is differentiated by sector; this is unlikely to be the case with FSA regulations. As the JMLSG is developing a risk-based approach to anti-money laundering in the 2004 Guidance Notes, which we understand should meet many of the FSA concerns set out in DP22, the majority of FOA members believe that the FSA should, at least, wait and see the results of this work before considering additional regulatory requirements. Options 3 and 4 would both allow time for the Regulations to come into force fully and be implemented by firms and for the publication of the 2004 Guidance Notes. The options would, therefore, allow the JMLSG to demonstrate that its guidance on a risk-based approach to anti-money laundering, KYC information and monitoring is appropriate. The main difference, however, is that Option 3, if explicitly stated in FSA guidance in SYSC (as opposed to ML, as per Option 1(c)), would give firms a regulatory, best practice, benchmark.

It is clearly important that the FSA's ability to ensure standards are being maintained and to take action where it identifies non-compliance is not diminished by reliance on the JMLSG Guidance Notes. The FOA believes that is appropriate that enforcement action is taken where there are systemic failures of systems and controls that leave a firm, and the market, open to the risk of being used for money laundering. It is important, therefore, that notwithstanding the reliance on the JMLSG Guidance Notes, the FSA is still able to take enforcement action (as recent cases indicate) under SYSC and ML.

A number of FOA members (who favour Option 1(c)) do not, however, support this option due to the status of the JMLSG Guidance Notes. Firstly, the JMLSG Guidance Notes are not a safe harbour under the FSA rules; although when (or if) approved by HM Treasury, the courts must consider whether a person followed the 2003 Guidance Notes, when deciding whether an offence has been committed under s. 330 PoCA and/or Reg. 3 of the Regulations. Secondly, it is not compulsory to follow the Guidance Notes. Hence, these FOA members believe that more certainty and direction is needed from the FSA and HM Treasury.

Option 4:

Make no settled decision now and review the position again in, say, two years time.

As discussed above, both Options 3 and 4 would both allow time for the Regulations to come into force fully and be implemented by firms and for the publication of the 2004 Guidance Notes. The options would, therefore, allow the JMLSG to demonstrate that its guidance on a risk-based approach to anti-money laundering, KYC information and monitoring is appropriate.

Option 4 is the preferred option of the majority of FOA members who expressed a view (either in its own right or, as discussed below, in combination with Option 1(c)), as it would enable FSA to assess the development of 2004 JMLSG Guidance Notes (including the risk-based approach to anti-money laundering) before considering whether additional regulatory provisions are necessary. That said, FOA members would not wish to see the FSA develop, at a future date, more detailed rules to sit alongside the JMLSG Guidance Notes, since, as discussed, this would result in two sets of guidelines, with the inevitable overlaps, contradictions and uncertainties, which would flow from that.

A number of FOA members (who favour Option 1(c)) do not, however, support Option 4, as they believe that more certainty and direction is needed from the FSA; particularly as it is demonstrating that it is willing to levy significant penalties against firms for anti-money laundering rule breaches (regardless of whether a firm itself has identified its weaknesses or has actually been used for a purpose connected with financial crime). In addition, there is a concern that recent themed visits have indicated that the FSA's expectations may, in some areas, be higher than the existing industry standards. **Some other FOA members would prefer a combination of Option 4 and Option 1(c),** for the above reasons.

FINANCE & LEASING ASSOCIATION'S
COMMENTS ON THE FSA'S DISCUSSION PAPER
ON 'REDUCING MONEY LAUNDERING RISK' (DP22)

The Finance & Leasing Association (FLA) is the leading UK representative body for the consumer credit, motor finance and asset finance industry. FLA members achieved £83.0 billion of new business in 2002, of which £58.0 billion was credit granted to private individuals and £25.0 billion was provided to the business sector. FLA welcomes the opportunity to comment on the FSA's Discussion Paper.

FLA members' core businesses fall into one of two categories:

- Financial products, mainly fixed term credit, much of which is relatively low in value. Many FLA members selling such products are not regulated by the FSA.
- "Big ticket" asset finance, which is considered to be low risk given that:
  - the lessee cannot acquire ownership of the asset during the term of the lease;
  - payments are collected by direct debit (which can be verified at source);
  - cash payments are not accepted as a normal course of business.

Examples of products provided by FLA members are:

- motor finance;
- retail point of sale finance;
- home improvement finance;
- equipment finance;
- fixed term loans; and
- secured loans.

The expectation of a customer buying a car or a white good is of a smooth, efficient process. This includes signing a credit agreement to finance the purchase. For finance houses Know Your Customer (KYC) is based on their expectations of the average customer rather than, for example, needing to know details of all of an individual's bank transactions. Firms will normally have systems in place to detect unusual transactions.

“Big ticket” asset finance providers undertake checks for the Directors in principal control and companies search as part of normal underwriting procedures. As part of the credit underwriting process they check that the client is registered on the Stock Exchange. Where it is not a public limited company, standard guidance is followed including verification of the beneficial owners. Prior to agreeing to finance an asset, the lessor will usually visit the customer. There should be an understanding of the client’s business (Know Your Business - KYB); for example, that the asset for which funding is sought, is consistent with the business. Efforts are centred on activity that falls outside of these norms: asset finance providers have systems in place to identify any suspicious transactions.

FLA therefore favours an approach in which identification of the customer is proportionate to the risk of their being involved in money laundering. A risk-based approach is inherent in the JMLSG Guidance Notes. This will be even more so in the radically revised version of the Guidance Notes, which is currently being drafted.

FLA supports the inclusion of guidance on monitoring in the FSA’s Handbook as per Option 1 from the Discussion Paper. However, the FSA needs to ensure that broadening the link between the Money Laundering Sourcebook and the JMLSG Guidance Notes will not create any conflict. FLA stresses the need for the Guidance Notes to draw distinctions between products where there is less requirement to strictly follow KYC procedures i.e. the product is low-risk. In addition, any specific rule making on KYC in the Money Laundering Sourcebook must also follow the risk profile of the product so that detailed requirements on KYC for high-risk products are not equally applied to low risk products.

In summary, FLA believes in a risk-based anti-money laundering approach which, by definition, reflects the fact that some products are less susceptible to being laundered. The JMLSG Guidance Notes set out the appropriate levels of KYC and FLA supports moves towards more sector specific guidance.

Yours faithfully

Edward Simpson
Senior Policy Adviser
Finance & Leasing Association

Direct Line: +44 (0)20 7420 9654
E-mail: edward.simpson@fla.org.uk

GLASGOW COUNCIL CREDIT UNION (GCCU)
FSA Ref No. 213558

Response to FSA Discussion Paper 22

Reducing Money Laundering Risk (Know your customer and anti money laundering monitoring)

Key Contact:
June Nightingale – Manager
0141 274 5401
j.nightingale@glasgowcouncilcu.com

Response

In respect of Discussion Paper 22 – ***Reducing Money Laundering*** – I wish to raise the following points:

- The content of the Discussion Paper is conducive to stimulating debate with regard to Know Your Customer practice and criteria and Monitoring of the use of products and services by customers/members. This is achieved through presenting clearly, current industry practice and the legal and regulatory obligations that exist. This has enabled GCCU to draw comparisons between industry practice and our own inherent systems;
- GCCU firmly agree that money laundering systems, controls and monitoring should be based on the risk profile and industry facets of individual firms. As a prominent member of the credit union movement in the U.K. GCCU have developed money laundering systems and controls which are allied to risk profile and the credit union movement as a whole;
- Of the four options presented, GCCU is of the opinion that the FSA would be best placed to make no decision at this stage re: status of rules and/or guidance and follow this up with a review of progress in two years time (2005 as mentioned in the Discussion Paper). This would allow for the following issues to be analysed in a more meaningful way:
    - The progress made by the JMLSG in reviewing their guidance notes;
    - Review of the developments in industry practice and the perceived need for high level guidance;
    - Review of the developments in monitoring systems, controls and practices;
    - Review of industry reporting link to NCIS and whether the culture of ‘reporting all transactions’ has continued or subsided; and
    - Review of the impact of the Proceeds of Crime Act and its link to Know Your Customer and Monitoring rules.

In conclusion, the collection of Know Your Customer information and a proactive approach to monitoring is crucial to the on-going objective of reducing money laundering and meeting legal and regulatory obligations. The fundamental issue behind such systems is the need for effective risk mapping and a clear knowledge of individual risk profile in order to ensure that systems are efficient and effective but not overly onerous.

I trust that these issues will be taken into consideration when developing further guidance. If you require clarification of any of the above points then please do not hesitate to contact me directly.

JUNE NIGHTINGALE
MANAGER
GCCU

26th January 2004

Dear Sirs,

I would like to comment on the current money laundering procedure that we have to go through, and put a few points into perspective.

I regularly attend Horseracing and Greyhound Racing meetings, during which tens of thousands of pounds changes hands in minutes, with bets of several hundreds pounds being regularly struck throughout the course of a meeting..

I, on the other hand have the embarrasing situation, of demanding proof of identity from clients investing into life and pension products. Who is going to money launder a few hundred pounds a year into a pension knowing that they can't touch it till age 50.

It's a joke, it's hassle and it is an embarrassment, and should be scrapped forthwith.

Yours Sincerely

Glyn D J LInder
Independent Financial Adviser
Norwich

GOY
HARRIS
CARTWRIGHT

STOCKBROKERS & INVESTMENT MANAGERS

GOY HARRIS CARTWRIGHT & CO. LTD.
NORWICH HOUSE 22-30 HORSEFAIR STREET
LEICESTER LE1 5BD

TELEPHONE
0116 2045500

FACSIMILE
0116 2543621

www.ghcl.co.uk

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

Our Ref: DP22/RI

24 September 2003

Dear Mr Shonfeld,

Discussion Paper 22 Reducing money laundering risk

In my capacity as Money Laundering Reporting Officer, I wish to formally respond to the Discussion Paper noted above. As you would expect both the Director of Finance and Compliance and Deputy Money Laundering Reporting Officer and I have read the paper and discussed it in detail. In addition to responding to some of the questions that you have raised I do have some ancillary points I wish to make, therefore please forgive me if this is a little long-winded.

It is our opinion that the best of the options presented is to make no decision now but to review the whole situation again at an agreed future date. This would allow every Financial Services Firm to undertake their own internal reviews and assess how they could improve all aspects of their anti-money laundering prevention capability.

As is pointed out in the DP, KYC does not exist in law beyond the need to obtain verification of identification and residence of customers. We at GHC however do already undertake efforts to obtain more information than is required. We accept that this is good business practice. We have instigated a rolling compliance monitoring programme which contains a significant anti-money laundering bias, and is we believe, a standard that should apply to smaller brokers and IFA's. However it appears to us that the DP indicates that the Regulations are keen on firms using electronic monitoring methods that some of the big six banks utilise. I do not believe that such a method would be cost-effective for a company of our size and nature. We are more dependent therefore upon adequate training of our staff to recognise suspicious activity on a day to day basis and awareness of the whole problem from a practical perspective. The cost of employing electronic methods would be prohibitive and would result on a whole new layer of employees for monitoring to be created, we believe that it is preferable to empower the existing employees to be aware, accountable and vigilant.

The question of what type of monitoring and reports would be most useful to law enforcement agencies should surely be aimed at the agencies themselves. Given the recent KPMG report it seems that there may be wholesale changes in the system, indeed at the recent APCIMs anti-money laundering seminar, which you spoke at, the representative from NCIS indicated that they would be making significant changes in systems and staff over the foreseeable future to improve levels of assessment and to facilitate more expedient detection of risk-trades/situations. The current regulatory guidance which indicates that the number of suspicious reports being made to NCIS being taken as an indication of the quality of ML procedures within a firm has, I believe only achieved the opposite effect. Firms are now reporting 65,000 suspicious incidents per annum, which, I am led to believe, contain "we are only doing this because we have to" reports, this is backed up by conversations with other MLROs who report the same thing.

The DP does not make clear which sort of products and/or services the proposal to obtain greater information will apply. I believe GHC is typical of stockbrokers who offer discretionary, advisory and execution only accounts. Will the measure be made retrospectively, that is where we would have to contact existing clients? It is our opinion that we cannot continue to re-contact existing clients as legislation changes over original requirements. We feel it is imperative that any legislative changes should only apply going forward.

Is it reasonable to ask an execution only type client to make the same disclosures that a discretionary client might? We would seek clarification that the level of KYC in respect of an execution only client should be lower than the others, but we would of course have to take due regard of the ongoing nature/risk of the transactions on these accounts.

It is not unreasonable to assume that most clients will feel that questioning the source of their funds, for example, however diplomatically handled, will be intrusive and accusatory. In the case of GHC some of this information is already requested on a Confidential Client Questionnaire (CCQ). Clients do not necessarily want to disclose for instance net worth, and are currently under no legal obligation to do so. Even if they did disclose net worth or source of funds they could simply say that it was a legacy, or they had the money in the bank. We would not be able to prove differently. All we are effectively able to do is to make the file note that the client wishes not to disclose. In such cases would there be a comeback on the firm?

I believe the paper does not address the question of how additional information requested from a client will not compromise the third principle of the DPA 98, which states that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. Will the FSA or the customer be the judge of what is considered adequate and not excessive and if so, will Firms be given guidance?

We all recognise the need for effective anti-money laundering policies and monitoring procedures. I do not believe however that ever-increasing legislation will necessarily achieve that. Good business practice remains to a degree common sense. All of our staff undergo anti-money laundering refresher training on a yearly basis. It is our considered opinion that continued staff vigilance will be more cost-effective for a company of our size than expensive monitoring programmes. Continual legislative changes will almost inevitably increase costs for companies such as ours, which we would most probably have to pass on to customers and will have the effect of penalizing those who we seek to target least. Effective money-laundering detection will need the co-operation of the industry, the regulators, the consumers and the legislature; the imposition of "face-value" procedures will not resolve the problem. This effort needs to be practical and commercial as well as being targeted properly – money launderers will have access to forged documents in large amounts and have the necessary resources to carry out their work. Joe Public does not need to be penalised any more.

I note that the FSA has recently run a consumer campaign aimed at educating existing and potential consumers of financial services as to why they are required to prove their identity. Would it be the intention of the FSA to run a similar campaign if new, more stringent rules are brought in via legislation?

I appreciate that you will most likely receive a mountain of responses to the discussion paper but I hope that this illustrates some of the problems that we foresee.

I have appended my direct answers to the questions posed in an appendix below.

Yours sincerely

Robert Ilic
Money Laundering Reporting Officer

Appendix

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

The necessity to collect KYC cannot be assessed in isolation, there are many factors which must be assessed, such as how the client has been introduced i.e. through an IFA or other regulated entity, whether they are having KYC assessed as part of initial suitability, the level and complexity of trading, the type of account (i.e.) discretionary or X/O. KYC is an existing element of the rules for advisory or discretionary clients and must be sufficient. Its introduction for other must be weighed up against the benefits v costs and the likelihood of an issue being detected.

On the other hand an active approach to monitoring is a necessity, although it can be passive in that it need not be defined but base don ongoing training.

Reporting is, we believe, one of the key factors in the issue. As long as the FSA reflect the fact that the issuance of suspicious transaction reports will be seen as an indicator of ML efficacy, it will result in individual firms making reports which they do not truly believe to be material, such reports however will result in a continuance of the overburdening of NCIS and the failure of the system to deal with "real" reports quickly enough.

Q2 How should a firm pursue a risk-based approach to Anti Money-laundering?

This needs to be done through the guidance of the JMLSG and FSA and the use of a common sense approach to detection and reporting. The basic account opening procedures are in place already, it is the ongoing assessment that needs to be tackled now, with actual cases being notified, irrespective of whether they are proven or not, on a no names basis, to show exactly how the money launderers operate.

Risk does not need to be defined but needs to be given parameters i.e. €15k limits in aggregate over the course of a year (it would be unlikely that a serious money launderer will deal in sums of this size) The clarification of account type that reduce the perceived risks i.e. ISA's etc. Again it is a common sense approach coupled with the reminder that it is the Firm and its employees who are responsible for reasonable efforts to detect and report.

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

The question of what type of monitoring and reports would be most useful to law enforcement agencies should surely be aimed at the agencies themselves, they need to provide guidance as to the form and content of the reports as well as providing detail as to what the police will require for an effective chance of prosecuting. Given the recent KPMG report it seems that there may be wholesale changes in the system, indeed at the recent APCIMs anti-money laundering seminar, which you spoke at, the representative from NCIS indicated that they would be making significant changes in systems and staff over the foreseeable future to improve levels of assessment and to facilitate more expedient detection of risk-trades/situations. The current regulatory guidance which indicates that the number of suspicious reports being made to NCIS being taken as an indication of the quality of ML procedures within a firm has, I believe only achieved the opposite effect. Firms are now reporting 65,000 suspicious incidents per annum, which, I am led to believe, contain "we are only doing this because we have to" reports, this is backed up by conversations with other MLROs who report the same thing.

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

The costs are added systems and personnel, supervision, compliance, stationery, client goodwill, regulatory cost, external agency costs due to increased reporting. The incremental benefits in respect of smaller brokers, we believe would be minimal. The existing requirements are sufficient.

Q5 Which options do you prefer and why?

It is our opinion that the best of the options presented is to make no decision now but to review the whole situation again at an agreed future date. This would allow every Financial Services Firm to undertake their own internal reviews and assess how they could improve all aspects of their anti-money laundering prevention capability. It would also allow the speed of regulatory change to settle down and provide some much needed stability to this area. The Treasury and the JMLSG would have completed their legislative changes and we could operate from a fresh and hopefully complete set of guidance.

Handelsbanken

London Branch
2 February, 2004

Daniel Schonfeld, Esq
Financial Crime Policy Unit Prudential Standards Division
Financial Services Authority
25 The North Colonnade
Canary Wharf London E14 5HS

Dear Mr Schonfeld

DP 22

I apologise that this response is a little late and unstructured. I realise unfortunately I do not have the time for a detailed submission. The Discussion Paper, however is a high level document and I hope you will fine these comments useful.

Generally, I agree that an active approach is necessary for assessing the risk of money laundering occurring and for obtaining ID. Similarly, an active approach to monitoring is in the general interest of the firm as a tool in developing business as well as detecting crime.

Given the FSA's role as principal prosecutor and rulemaker, the Rules, like the Market Abuse regime, should apply beyond regulated businesses to all activities covered by the primary legislation. In that case, neither the Money Laundering Regulations nor JMLSG Guidance would seem to be necessary. FSA Rules and Guidance could be rewritten to consolidate all the source material on Money Laundering Prevention. The Steering Group could be reconstituted as a Panel to advise the FSA and ML would become exhaustive.

Sanctions against financial crime and the definition of what constitutes the crime should be clear and unequivocal. The concept of risk-based measures to prevent crime as a defence to prosecution does not fit easily in a criminal regime, although I am sure there are precedents for this. I believe it would help to publish different sanctions policies where firms and individuals are concerned. On paper the MLRO is personally exposed to a high risk of prosecution for what are, in reality the delinquencies of others.

I believe the FSA could give Guidance on how it expects to prosecute so that, for example, without the need for substantive changes in the law, it could indicate that failure to implement procedures might result in criminal sanctions against firms whereas individuals could expect only disciplinary measures, unless they had knowingly assisted in money laundering.

As far as the timing of changes is concerned, I think the FSA should not rush into changes and definitely not patch and paste on to the existing regime. The opportunity to step back and produce clear, cohesive rules and guidance from a single, authoritative source should not be missed.

Yours sincerely

Martin Hankey
Head of Legal & Compliance Services

Svenska Handelsbanken AB (publ)
Trinity Tower 9 Thomas More Street
London E1W 1GE

Telephone
+44 (0) 20 7578 8000

Telefax
+44 (0) 20 7578 8300

Telex
894716 SVNSKC G

Registered in England and Wales No. BR 000589
VAT Registration No. GB524 9824 25

Incorporated in Sweden with limited liability
Registered in Sweden No. 502 007-7862
Head office in Stockholm

Regulated by FSA

HBOS plc

CS/2/GRR/DG/MDH

Trinity Road
Halifax
HX1 2RG

28th January 2004

Mr D Shonfeld
Financial Services Authority
25 North Colonnade
Canary Wharf
London
E14 5HS

Direct Line 01422 333238
Fax No 01422 334177

FSA Discussion Paper 22

Dear Daniel

Thank you for giving us the opportunity to comment on DP22. We have had considerable input into the BBA's response, been involved in discussions on the ABI's response and also seen IMA's reply. These replies from the trade bodies include the key points which we want to make on DP 22.

In particular, we would highlight the following:

- It is important that there are some baseline criteria, agreed by FSA, which firms should take into account when adopting a risk based approach. Close co-operation with NCIS, the Terrorist Financing Unit and similar bodies is also key to devising an appropriate risk based methodology and identifying suitable types of ongoing kyc information.
- A consequence of encouraging firms to adopt their own risk based approaches may well be that a level of competitiveness will enter this area of regulation. To date, the close co-operation of firms on AML, on the understanding that this is not a competitive issue, has been a key factor in raising its profile and agreeing the way forward.
- There is an expectation that there would be a "safe harbour" defence if, despite acting reasonably and in good faith in introducing a risk based approach, a firm was, nevertheless, found to have been the victim of launderers or terrorists.
- The introduction of any new rules or guidance should not be retrospective.
- From a customer perspective, there are advantages in enabling firms to adopt a risk based approach. At the same time, particularly for a large firm, such an approach is not necessarily a cheaper option as there is likely to be the need for several different procedures for different types of product, requiring a variety of training and systems solutions.
- Following several years of continuing significant legislative and regulatory change in this area, firms need to be given the opportunity to embed changes, and implement systems developments, in the knowledge that further significant changes are not

imminent (unless there are reasonable grounds for believing they are essential to address a new development in financial crime or terrorism funding). Therefore, over all, our preference would be for option 4 – "make no settled decision now and review the position again in, say, two years time".

We look forward to participating in further discussions about the way forward in the areas covered by the DP.

Yours sincerely

D Gordon
Head of Money Laundering Prevention and Data Protection
HBOS Group Regulatory Risk

Heath Lambert Consulting's response to Discussion Paper 22
Reducing Money Laundering Risk

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

The amount of "know your client" information will vary depending on the firm and the type of transaction undertaken. For "face to face" investment business "know your client" information is likely to include identifying the source of funds, the objectives for investment and the likely term it is to remain invested. For non face to face lower risk business however "know your client" information is likely to be restricted to the basic verification requirements and ensuring that a transaction is not in any way unusual in consideration of the circumstances it is made.

"Know your client" information places firms in a position where they are able to assess risk and identify potential money launderers. The request for such information communicates to potential money launderers that the opportunity for money laundering is reduced. With more and more emphasis being placed on non-advised, "non-face to face" sales however, the opportunity for obtaining "know your client" information is somewhat reduced.

Monitoring of anti – money laundering will be appropriate to the size of the firm and the nature of its transactions, however the promotion of awareness through staff training and robust procedures is essential to ensure that legal and regulatory obligations are met.

2. **How should firms pursue a risk-based approach to anti-money laundering?**

First firms need to assess the money laundering risk to the organisation. Clearly some firms face more risk than others depending on the type of business undertaken. For example a firm accepting client money and making investments will be more of a risk than one which deals with long term insurance where there is no surrender value.

Training and education of staff in the issues of money laundering and providing a prominent contact point for queries and reporting goes a long way to minimising risk. By educating staff of the issues they should be aware of and making anti-money laundering issues a key part in everyday procedures and a key part of "know your client", the risk is minimised considerably. If staff are not adequately trained, the risk of the firm being a target for money laundering opportunists is increased.

3. **What type of monitoring (and reports) would be most useful to law enforcement agencies?**

As noted, monitoring will be dependent on the type of business the firm undertakes; however a standard system of reporting with clear guidelines to one central agency is appropriate.

4. **What are, or may be, the costs and benefits of KYC and monitoring?**

Clearly there are costs involved in obtaining "know your client" information and monitoring. For instance; training of staff to ensure that they know how to obtain and use the information, recording the information, ensuring the requirements are followed and monitored and maintaining ongoing vigilance for further transactions.

The benefit of these measures, whilst will not appear to reduce the overall effect of criminal activity, can reduce individual firms being the target of a money launderers. In addition, once it is common practice amongst firms, the industry as a whole becomes less of a target, as there is increased vigilance and tighter controls. So although the benefits may not seem immediately evident to firms it is part of an overall process to reduce the risk of money laundering in the industry.

5. Which options presented do you prefer and why?

Option 3 – leave ML unchanged; rely on the JMLSG Guidance Notes with the option to further review in the future. Whilst the FSA have effectively taken on the statutory powers to enforce money laundering rules and prosecute for breaches of those rules, adherence to the current Joint Money Laundering Steering Guidance Notes has become accepted and reasonable practice for responsible firms.

Colin Murphy
Compliance Officer

26th January 2004

Daniel Shonefield
Financial Crime Policy Unit
Prudential Standards Division
25 The North Colonnade
Canary Wharf
London E14 5HS
Email dp22@fsa.gov.uk

Response to Discussion Paper 22 – Reducing Money Laundering Risk

I am writing this response on behalf of the operational policy team within H M Customs & Excise with supervisory responsibility for businesses registered with us under the Money Laundering Regulations (MLR) – that is Money Service Businesses (MSBs) and from 1st April 2004 High Value Dealers (HVDs).

Our response is focused on KYC. We propose that you adopt option 4. Also that you use the review period to liaise with other supervisory / appropriate bodies to ascertain if the absence of a specific legal or regulatory requirement to apply KYC, particularly the key element "customers' source of funds" is damaging to the objective of detecting and deterring money laundering. If evidence is found supporting the case, that you seek Treasury consideration of amended regulations to include elements of KYC.

The MSB register includes some 2000 operators trading from approximately 30,000 premises. It is responsible for about 15% of disclosures to NCIS. Customs supervise the regime primarily by a visiting programme educating businesses about their MLR responsibilities and checking their AML systems to ensure compliance. So far, since the MSB register was introduced in June 2002, we have completed about 1500 of these visits.

In the areas of money exchange and money transmission MSBs are in competition with businesses regulated by the FSA. As regulators / appropriate bodies we therefore need to ensure that the regulatory burden is consistent between the different sectors to avoid market distortion.

Though the MSB sector is dominated by a few large businesses, many MSB operators are small businesses with relatively unsophisticated accounting and AML systems. It is difficult to generalise their reaction to MLR supervision but I think it would be fair to highlight a few persistent strands

- MSBs are uncomfortable with the onus of identifying suspicion being their responsibility.
- They want more guidance about how to identify suspicion
- They believe the law is too complicated, our supplementary guidance too general and other ML guidance irrelevant.
- They are unwilling to operate KYC (as outlined at para. 3.7 of your paper) for fear of diverting business away to less scrupulous competition.

As you point out in the discussion paper businesses regulated by the FSA frequently are engaged in ongoing business relationships with their customers and gather KYC information for other purposes. MSBs on the other hand are primarily concerned in one- off transactions. Gathering the full scope of KYC information (per para.3.7) would be disproportionate and inappropriate.

The discussion paper makes reference to businesses adopting a risk based culture towards AML (para 3.17). We entirely support this view. Customs adopts a similar approach to all its activities, including the visit programme to MSB operators I mentioned earlier.

When embarking upon a transaction there are two key factors upon which a business can make a judgement about the risk of money laundering: the customer and the business sought to be transacted. The former is subject to regulatory control under MLR but the latter is not. The key suspicion indicator within a transaction is normally the customers' "source of funds". We believe there may be a strong case for making this aspect of KYC a regulatory requirement and would welcome FSA considering this as a further option.

As you point out (para 1,3) there is no legal or regulatory requirement to apply KYC. Why should businesses do so? MLR presently requires businesses to "establish such other procedures of internal control and communication as may be appropriate for the purposes of forestalling and preventing money laundering". We could interpret this as requiring the use of KYC information to pick up any unusual activity but it is not a strong base.

Another incentive for businesses to adopt KYC procedures is the "objective test" introduced under the Proceeds of Crime Act (POCA) whereby a business can commit an offence if it fails to make a disclosure if, when its suspicions are aroused, it wilfully turns a blind eye to the obvious, fails to adequately ascertain the facts or fails to make adequate enquiries to assure itself of the legitimacy of the transaction. (JMLSG notes on POCA – Feb 2003 para 5.8) The sanction within POCA appears to be premised on the fact that suspicions are already aroused whereas the argument for including "source of funds" in the regulations is that it may help to determine suspicion.

You mention a variety of options in chapter 5. We dislike options 1 and 2 on the basis that the application of the key elements of KYC should be consistent across all sectors within the MLR. We believe any changes to your (and our) guidance should emanate from changes to the regulations. Those changes should help to simplify requirements and maintain fair competition.

We support option 4. In addition to the points you make in support of this option we could usefully use the time to identify whether the absence of a regulatory framework backing the application of KYC is a serious risk to the UK achieving its financial crime objective. Common sense indicates that failing to question the source of a customers' funds will result in a lower rate of ML detection and deterrence but presently Customs has only anecdotal evidence that this is the case.

Kind regards

Frank Tucker

28 January 2004

HM Customs & Excise
Money Laundering Team
Excise Operations
3 West Ralli Quays
Stanley Street
Salford M60 9AL
Phone 0161 827 0305
Email: frank.tucker@hmce.gsi.gov.uk

HSBC

Telephone Number: 020 7991 8645

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

03 February 2004

Dear Mr Shonfeld

HSBC Response to Discussion Paper 22 Reducing Money Laundering Risk

We welcome the opportunity to comment on the above discussion paper. We strongly believe that in order to maximise the effectiveness of our efforts, money laundering prevention should be the subject of ongoing debate, both within the financial services industry, and more widely with other business sectors and the various interested authorities. We have participated in discussions on your paper at the BBA and other trade associations who have responded to you in detail to the issues raised. We have therefore restricted our response to our conclusion and a number of high level points.

Our overall assessment with regard to the options set out is that a high level requirement in respect of KYC and monitoring would be appropriate, supported by guidance in the JMLSG Guidance Notes. We do not believe that new detailed regulatory material is required. Many firms are in the process of introducing automated monitoring and undertaking remediation exercises such as the current customer review and it is important that time is given to assessing the effectiveness of current initiatives and actions.

We believe that an integrated risk-based approach to identification/verification, KYC and monitoring, together with the reporting of suspicions, are the key areas in which the financial services industry can help in the prevention of money laundering. The development of a risk-based approach, taking into account the "reasonable grounds" criterion in the Proceeds of Crime Act 2002, across a diverse financial services sector in terms of size, activities, products etc., will be complex. This will present challenges to the industry, the FSA and other authorities which need to be recognised and managed, adopting a partnership approach. In particular, in carrying out its supervisory responsibilities the FSA will need to adopt a flexible approach when assessing a firm's risk-based programme.

HSBC Holdings plc
Group Compliance, Level 42, 8 Canada Square, London E14 5HQ
Tel: 020-7991 8888 Fax: 020-7991-4719

HSBC

The effectiveness in terms of money laundering prevention in respect of each of the above components, or their combined effect, has not to our knowledge been measured in any formal or scientific way. There needs to be a recognition that this must be assessed more formally at some juncture in order that the efforts by the financial services industry and others can be focussed in the most effective manner and the associated costs justified.

Our experience of the design, development, implementation and maintenance of an in-house automated system has shown that the experience, expertise and commitment of IT, Compliance and Business personnel is key to success. As the majority of in-house and external systems are in the early stages of implementation it is hard at this stage to decide how "effective" these processes are. It is becoming clear that further development is required to improve significantly the conversion rates from "alert" to "suspicion". We are committed to such work, both individually and in partnership with other financial institutions and the authorities.

In order to be of most value to the authorities it is important that monitoring systems highlight potential criminal activity at an early a stage as possible and identify any connected accounts for review. To assist the development of sophisticated monitoring techniques it is imperative that the authorities perform appropriate analysis and provide feedback to ensure that all financial institutions benefit from the aggregated knowledge that is only available to the authorities.

Yours sincerely

David W J Bagley
Head of Group Compliance

5TH FLOOR, 32 LOMBARD STREET,
LONDON EC3V 9BQ, U.K.

HUA NAN COMMERCIAL BANK LTD.

LONDON BRANCH

Authorised and regulated by Financial Services Authority

TEL: 020-7220 7979
FAX: 020-7626 1515
TLX: 887033
SWIFT: HNBKGB2L

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

By Fax: ~~0207 066~~ 5645 NOT

27 January 2004

Dear Daniel

Comments on the questions posed in DP 22

I write as Compliance Manager and MLRO for the London Branch of Hua Nan Commercial Bank since it opened in 1998.

Like most other MLRO's of my acquaintance I am concerned at some of the practical implications of interpreting and applying the anti-money laundering rules and the burden of responsibility of doing this in a risk based environment. The risks to the firm, or individual MLRO, that gets it wrong are all too clear, especially where hindsight might be brought to bear on an individual case. The principles are clear and I have no problem there at all. The challenge in a small unit is the interpretation of rules and guidance which are applicable to the whole gamut of financial firms. This branch is at the smaller end of banks, having only 12 staff and a small number of transactions. Monitoring is, therefore, relatively easy, but the interpretation of a lengthy rule book sometimes presents a significant hurdle.

It is in the light of these general sentiments, which are intended to let you see where I am coming from, that I have attempted to provide some responses to your questions.

1. **To include new specific rules in the FSA handbook.** The rule book is already complex and not always easy to interpret and apply when dealing with ongoing issues. Furthermore, a rule book is static, whereas money launderers are continually creating new ways to circumvent the system. Therefore, new rules may not be the best way forward.
2. **To include new guidance in the FSA handbook.** Guidance could be helpful in setting up policies and procedures but is likely to be of less help in dealing with day-to-day issues.

3. **To include a new set of rules to cover monitoring.** Despite my reservations in 1 above, I consider that rules covering monitoring might be of help. How useful the rules were would depend very much upon how successful you were in framing a concise set of rules that could be applied over the whole industry and how soon they could be in place.
4. **Rely on the existing JMLSG Guidance Notes**. In theory this is the approach that I would favour. However, I have yet to receive a copy of the new version and it is not sensible to offer a firm view on this option until I have had the opportunity to review it.
5. **Make no change now and review the situation in 2 years time.** This could well prove to be the preferable option. It would allow time for practitioners and supervisors to understand how the current anti-money laundering regime was working and for any new rules to be based on an established and agreed need. This approach assumes reliance on, and sensible interpretation of, the JMLSG Guidance Notes. In a sentence: it might just be best to wait until we all have some experience of monitoring before trying to write the rules, even if this is rather getting the cart before the horse.

MLRO's will always have to take responsibility for their decisions and will always be exposed to risk in a risk based system. I believe that all MLRO's of my acquaintance are keen to comply with the spirit of the money anti-money laundering regulations. There is, however, a fear that a genuine misjudgement will, with the benefit of hindsight, be seen as negligence (or worse) upon investigation. This fear could lead to excessive reporting, with the inevitable overloading of the system to the detriment of its effectiveness. The good judgement of MLRO's is critical to the effective operation of the anti-money laundering procedures. If option 5 were to be adopted MLRO's would bear a heavy responsibility. In any event, there is no system or set of rules that can make infallible decisions to separate the unusual from the suspicious.

In conclusion, I think that changes to the FSA Handbook should, at this stage, be avoided as far as possible, accepting that this course of action, or inaction, would pose risks for all concerned.

I have tried to keep this letter short, as I am sure you will receive many submissions, and hope you find these views helpful, despite possible inconsistencies in opinions expressed in different parts of the letter. Should you wish to clarify any of my comments or seek further information please do not hesitate to contact me.

Yours sincerely

Tony Williams
Compliance Manager

IFAct Framework

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

20th August 2003

Dear Mr Shonfeld,

Re: Discussion Paper 22

OVERVIEW

Our company is a regulatory consultancy dealing primarily with IFAs and general insurance mediation firms that are currently regulated by GISC. The vast majority of these firms undertake both commercial business, and personal business for retail customers. Their turnovers range from £1,000,000 to £500,000,000 per annum.

We communicate regularly with some 400 firms, either by running workshops in respect of FSA regulatory requirements for firms that are preparing for authorisations, or for IFAs that are already authorised, we undertake regulatory compliance audits and a compliance updating service.

Response to the above paper is in the context of these firms.

1. For all of our clients KYC is absolutely essential before they can hope to provide their clients with suitable advice. Adequate KYC should provide firms with adequate information, which will enable them to spot an unusual transaction and if necessary, submit a report. The majority of firms with whom we communicate, and for many we run their money laundering awareness course, they feel it is essential that their staff are aware of money laundering not only to work with enforcement agencies to reduce financial crime, but to protect their own firm and employees from inadvertently being involved in criminal activity.
2. For IFA clients, we feel that the vast majority of them already undertake robust customer identification procedures, and would be well placed to spot a suspicious transaction. Many of our clients already make regular reports to NCIS if they have any suspicions. For general insurance and mortgage mediation clients, we feel that customer identification is probably unnecessary as their vulnerability to money laundering is relatively low. However, we do

feel that this practice guidance or indeed rule from FSA should require firms to have a MRLO, and that this controlled function should be obliged to make all employees aware of money laundering and the firms procedures to assist law enforcement agencies in the reduction of a financial crime.

3. We are unable to answer this question.

4. The costs of customer identification are already being borne by IFAs and they are living with these costs.

The costs for a general insurance or mortgage mediation firm are again relatively small for KYC but they may be significant if they are required to identify each customer.

5. Well feel that option 2 would be our first choice. The rationale being that high level rules guidance would allow firms to implement systems that was entirely appropriate to the money laundering risk profile which they presented and allow firms to understand their individual responsibilities and to take proportionate preventative measures.

Yours sincerely,

John Derry-Collins
FLIA FInst SM AMITD FCol MInstD

RESPONSE OF THE INFORMATION COMMISSIONER

REDUCING MONEY LAUNDERING RISK:
KNOW YOUR CUSTOMER AND ANTI-MONEY LAUNDERING MONITORING
FINANCIAL SERVICES AUTHORITY DISCUSSION PAPER 22
AUGUST 2003

1. The Information Commissioner promotes and enforces compliance with the Data Protection Act 1998 (‘the Act’) and, as it gradually comes into force, the Freedom of Information Act 2000.

2. We welcome the opportunity to comment formally on the matters set out in the consultation paper. We particularly welcome the clear recognition in the discussion paper that there are data protection obligations and privacy issues to be addressed in certain circumstances.

3. Our response reflects the structure of the discussion paper and outlines briefly the principal data protection implications we have identified in the issues raised in the paper.

4. We are content for our comments to be made publicly available.

The Data Protection Act 1998

5. The Data Protection Act 1998 implements the EU Data Protection Directive 95\46\EC which has as its first objective the protection of ‘the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to their processing of personal data’. The Act regulates the processing of individuals’ personal information by requiring those determining the purposes of the processing and the manner of that processing:

- to comply with eight enforceable data protection principles (Annex I); and
- to provide certain details of their processing activities to the Information Commissioner for inclusion on a public register, unless they are exempt from notification.

6. The eight data protection principles do not translate in practice into a rigid set of clearly defined rules which apply in the same way in every circumstance. Instead, they - and the exemptions from the principles set out in the Act - provide a general and potentially flexible framework for regulating the processing of personal information. This framework provides for those circumstances where different and sometimes competing public policy objectives have to be considered and balanced with data protection and privacy objectives. In appropriate circumstances the protection normally

/…

accorded to an individual's information may have to be limited or withdrawn. Our starting point is to promote the protection of individuals' information and through this their privacy, but we acknowledge that that protection is not absolute in all circumstances.

7. It is not unknown for data protection to be characterised as a fraudster's charter, inhibiting initiatives to prevent or detect fraud and handicapping the relevant authorities in the proper discharge of their law enforcement work. It isn't. Nor is data protection a money launderer's charter. It is a shield for the innocent majority, whose privacy should not be sacrificed unthinkingly in the search for the guilty minority.

8. The protection afforded by the data protection regime and the rights provided under the legislation do not just apply to individuals in their private life. Information relating to sole traders and in some cases information about partners in a business partnership or directors in a company may be subject to data protection legislation.

Chapter 2: Introduction

9. It seems to us that a risk-based approach to identifying money laundering risks would need to include consideration of relevant data protection requirements if the processing of any personal data were involved. Where there are tensions between the money laundering and data protection regimes, we consider it preferable for these to be brought into the open and addressed directly. If a risk based approach were to promote this openness and encourage properly informed consideration of the issues we would consider it desirable from a data protection view.

10. Where tensions exist between the two regimes and if one regime must predominate, whether the money laundering obligations or the data protection obligations take priority should reflect the particular circumstances. There should be no automatic assumption that one particular regime would always 'trump' the other.

Chapter 3: Know Your Customer (KYC)

11. We have noted the discussion of customer privacy and data protection in sections 3.21-3.23.

12. Clarity of purpose is an essential element of the data protection regime, underpinning many of the data protection principles.

13. In broad terms the fair processing provisions of the first data protection principle mean that those obtaining personal information, those whose personal information it is and, if different, those providing the personal

/…

information should understand the immediate purpose(s) for which that information is required and the uses which will subsequently be made of it. Clarity about the purposes of the processing is a prerequisite in those circumstances where the consent of the individual is required before certain processing may take place. The second data protection principle requires that any further processing of personal information must not be incompatible with the specified and lawful purposes for which that personal information has been obtained. Independently and in combination, these provisions means that information obtained for anti-money laundering purposes would not necessarily be available for use by the organisation for another business purpose.

14. The third data protection principle states that ‘Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed’. This principle would need to be carefully considered when decisions are made about which personal information should be processed for anti-money laundering related purposes. Information that may be appropriate for one purpose may not be similarly appropriate for another purpose. Closely associated with third principle issues is the requirement of the fourth data protection principle that ‘Personal data shall be accurate and, where necessary, up to date’.

Chapter 4 Anti-money laundering monitoring

15. We have noted the comments on customer privacy at section 4.19.

16. As discussed above, one of the key elements of data protection legislation is that the individual should be aware of the purposes for which his information will be used. Those considering wholesale monitoring of customers’ existing accounts would need to consider carefully the basis on which they undertake such monitoring. Would such processing satisfy the fairness element of the first data protection principle? Would such processing satisfy the lawfulness element of the first data protection principle? Which of the schedule 2 conditions would the processing be based upon?

17. Monitoring by automatic means raises additional data protection issues. Those undertaking automatic monitoring would need to be satisfied that both the automatic system itself and the broader framework within which that automatic system sits would meet the fair processing requirements of the first data protection principle. As the discussion paper states in relation to monitoring in general ‘the unusual is not the same as the suspicious’ (4.12).

18. Data protection legislation provides individuals with rights in relation to certain fully automated processing (section 12 of the Data Protection Act 1998) and these too may need to be taken into account by those developing or using such systems.

/…

Chapter 5: Options and questions

19. The first data protection principle requires personal information to be processed lawfully. It also prohibits the processing of personal information unless:

- the processing meets at least one of the conditions listed in Schedule 2; and
- in the case of personal information defined in the Act as 'sensitive data' the processing meets at least one of conditions listed in Schedule 3.

20. The complex nature of the anti-money laundering regime means that those processing personal information in order to comply with the different obligations imposed by that regime are not necessarily able to base all their processing on the same Schedule 2 condition. The relevant condition may vary according to the particular processing being undertaken or there might be uncertainty about whether the particular processing meets any of the listed conditions. In some circumstances the question may arise of whether the individual's consent is required for the proposed processing to take place.

21. We are aware that concerns have been expressed in the past about how particular anti-money laundering obligations may sit with compliance with the Schedule 2 conditions. We have taken the view here that if there is uncertainty a clearly identified legal obligation covering the relevant processing of personal information would set the matter beyond doubt. One of the Schedule 2 conditions is that 'the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract'. We see clarity and certainty about legal obligations in this area facilitating compliance with data protection legislation and also easing the relationship between the data protection and anti-money laundering regime.

22. Looking forward it would be unfortunate if any future anti-money laundering activities or initiatives were to be inhibited because of any uncertainty about the precise basis on which the processing of any personal data could take place. In data protection terms a clearly stated legal obligation on which processing of personal data could be based would be preferable to a less precise obligation which might lead to uncertainty about the basis on which processing of personal data could take place. We consider a specific Rule would assist those processing personal data to meet their Schedule 2 data protection obligations.

Concluding comments

23. We would welcome the opportunity to discuss our comments with the FSA and also any further issues with data protection or privacy implications which may arise as work on this aspect of the anti-money laundering regime is taken forward.

ANNEX I

SCHEDULE 1

THE DATA PROTECTION PRINCIPLES

PART I

THE PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The Data Protection Act 1998

ANNEX A

COMMENTS OF THE
INSTITUTE OF CREDIT MANAGEMENT
ON THE
FINANCIAL SERVICES AUTHORITY (FSA)
CONSULTATION PAPER
ON REDUCING MONEY LAUNDERING RISK – KNOW YOUR CUSTOMER AND ANTI – MONEY LAUNDERING MONITORING

The Institute of Credit Management is the largest professional credit management organisation in Europe. Its 9,000 members hold important, credit-related appointments throughout industry and commerce. Although the Institute has some members employed in areas regulated by FSA codes of practice, those members who are not regulated by the FSA have to look elsewhere to ensure compliance with money laundering requirements, eg to the Joint Money Laundering Steering Group's Guidance Notes.

The Institute can see that, with the Government's stated intention to introduce ID cards and the fact that the Government and its agencies already hold considerable information about individuals, the possible extension of "Know Your Customer" (KYC) information requirements may require a wider public debate to secure a consensus. Without such a consensus there is a danger that the excellent progress on anti money laundering to date could be undermined.

The responses to the questions below assume that basic identification requirements are met.

Question 1

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

The Institute understands that, while most firms attempt to collect KYC information on account opening, on personal accounts such information is limited. Section 3 of the discussion paper identifies the practical issues, especially verification, but does not suggest any practical solutions. It seems to the Institute that, as a general rule, customers consider their financial affairs on investing (as opposed to borrowing) as their private business. The Inland Revenue already knows financial details through the various returns that financial institutions make, eg amount of interest paid. It would seem sensible if such information could be shared with the National Criminal Intelligence Service (NCIS) to provide a larger picture that might enable "big fish" to be targeted.

With the increasing emphasis on potential misselling, the Institute is aware that organisations will seek more KYC information, eg through 'fact finds'. KYC should therefore be more readily available in the future. The Institute is mindful that there will always be a proportion of customers who will require "execution only" on the basis that they know what product or service they want or perhaps wish to keep their other financial circumstances private. There would therefore need be a two-tier approach with such customers, as they could be money launderers selecting “execution only” products or could simply be customers with strong views about privacy. The Institute can see that in such circumstances it could make the identification of money launderers very difficult.

Question 2

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

The Institute considers that cash should be the primary concern as cheques or other banking transfers, while making investigations more complex, at least leave an audit trail. The authorities can investigate such audit trails once they have identified a “big fish” by means of existing data, eg that held by the Inland Revenue (see the response to question 1 above).

Cash, however, does not leave an audit trail and thus requires more careful identification as a suspicious transaction. It seems to the Institute that in order to work effectively this requires a mixture of human instinct supported by systems. The human instinct can be developed by educating staff about what to look for, but a cultural climate, disapproving of illegal activity, eg the black economy and benefit fraud, also needs to be created. The Institute is aware that the FSA has significantly improved the focus of financial institutions in relation to the education and training element. Financial institutions, for their part, by their educational and competency requirements, recruit people who are generally honest and law abiding. This can always be improved, however, and continuing FSA attention will help to do so.

There is also a cultural issue to be faced. If society starts to perceive regulations as “Big Brother”, then individuals will not be as vigilant. The Institute therefore reiterates the need, as expressed in our introductory paragraphs, for a consensus approach. Moreover, systems are an essential support in all but the smallest organisations. These will identify, from set parameters, those transactions that are more than unusual and that have not been reported as suspicious by the cashier.

The Institute would also suggest that, on a risk-based approach, time is not necessarily a critical factor. Provided that the account holder has been properly identified, the reporting of suspicious transactions can occur a number of weeks, or even months, after the event. This is particularly so when it is a cumulative pattern over a period of time that eventually tips the account(s) into the ‘suspicious’ category.

Question 3

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

The Institute considers that cash monitoring and reporting should be of most concern to financial institutions, and therefore most useful to law enforcement agencies. Such information is only indicative, however, and requires further investigation. The main focus of law enforcement agencies should be on unexplained lavish lifestyle and assets. This could be facilitated by the Inland Revenue, Land Registry and the law enforcement agencies exchanging their own intelligence. In turn it should be possible to seek confiscation of assets if “big fish” suspects are unable to prove a legitimate source. If the message is made clear to the public that significant wealth cannot be accumulated (or retained) dishonestly, it seems to the Institute that this would provide a significant deterrent. The Institute furthermore suggests that all official information such as tax or benefits should be shared, where necessary, with other government departments in order to tackle large scale money laundering.

While the Institute anticipates that there will be almost universal agreement to target "big fish" (drug dealers, terrorists etc) there may be less commitment for targeting "minor" black economy frauds such as misusing children's accounts to evade tax. It seems to the Institute therefore that some guidelines may be necessary as to the level at which fraudsters/money launderers should be targeted, and the different approaches to be used depending on the scale of the offence. Without a clear and practical minimum, the Institute fears that the impact could be to increase the black economy in cash. That is not to say that minor offences should be ignored but that the full weight of anti money laundering measures should not be used to identify them.

Question 4

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

One member of the Institute who works within a regulated firm made the following comments:

"At a technical level the costs can be estimated. For a large regional building society the costs for an automated monitoring system are in the region of £250k. The continuing cost of KYC would be minimal, as it could be part of the normal process. The short-term benefits in terms of reducing money laundering or criminal convictions can also probably be estimated. Such benefits will be illusory unless society accepts this increased monitoring, however. Without this wider acceptance there is a danger that society will react counter-productively with an increased tolerance to lower level black economy activity."

Question 5

Which options presented do you prefer and why?

The Institute can see the merits of options 2 and 4.

Unregulated firms

The Institute is aware that there are also firms who are not regulated by the FSA but who have considerable responsibilities in relation to money laundering. It seems to the Institute that more could be done to educate and help such firms to undertake those responsibilities properly. One senior member who works for a medium-sized finance house made the following comments on the discussion paper generally and in response to the questions above:

> "**Paragraph 2.6**
>
> In our case (and doubtless others) KYC is actually a part of the credit risk assessment and fraud prevention process/measures.
>
> **Paragraphs 2.6 and 2.9**
>
> The lack of guidance regarding the perceived level of risk in particular parts of the financial services industry (including the lack of publicity on typologies – notwithstanding the information on the Financial Action Task Force (FATF) website etc) has resulted in an over the top response in some areas. The three well-publicised fines on specific banks has exacerbated the situation. Making the typologies more sector-specific would be helpful.

Paragraph 3.14

As 99.99% of our customers are self-employed it is very difficult to verify income beyond audited accounts and the availability of these is not compulsory for sole traders and is being eroded in the case of limited companies by the repeated rises in the audit exemption threshold.

Paragraph 3.18

We would generally update the income information only when a new transaction is proposed or if a credit line is renewed. We wouldn't update ID checks unless the relationship has lapsed (ie no contact from the customer and no live agreements) for more than 12 months.

Paragraph 4.5

We do monitor customers for possible money laundering. Monitoring must be an active approach. In our case this includes checking that the proposed purchases are in line with their business, the source of any cash deposits over 35% on hire purchase deals and reviewing reasons for early settlement of finance agreements. In addition we don't accept cash (notes) deposits over £3,000.

Paragraph 4.8.

Fortunately, in our case, we still see every customer, at least on the first transaction.

Paragraph 4.12

It is very difficult even for trained staff to distinguish between the unusual and the suspicious. An automated solution would be even worse at it! Eventually it must come down to a person reviewing the "exception reports" and making a judgement.

Paragraph 5.12

We would vote for Option 3, subject to seeing the revision due in Q2 2004. The main reason is that we are not FSA regulated and therefore would not want to be subject to their handbook. The JMLSG needs to ensure that the rules take account of the "broad church" of companies that are using their Guidance Notes and not allow the Guidance to be simply bank oriented, however.

Paragraph 5.16 (iii)

As mentioned earlier, I believe that there is a need for monitoring to be active and possibly we have an advantage in having a relatively small customer base (13k) in a niche market.

I don't believe that the message has been delivered strongly enough that since the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2003, the fight is now against crime generally, and not simply terrorists and/or drug dealers. For instance, I still get lists from our banking parent of alleged terrorists, to check against our customer database, but not of alleged criminals!

<u>Question 1</u>

This is very necessary in my view. Proving someone is who they say they are prevents only impersonation, however. It does not prevent money laundering. There is a need for an active approach to monitoring the transaction and account activity.

<u>Question 2</u>

Firms should pursue a risk based approach, particular to the business sector they operate in. More guidance on the level of perceived risk in particular businesses, and typologies specific to that industry, would be helpful in judging the level of diligence required.

<u>Question 3</u>

It probably depends on what type of financial services business you are in. In our sector, reports of high levels of (cash) deposits and/or very early settlement of agreements, without an apparent good business reason would, I believe, be useful to the law enforcement agencies.

<u>Question 4</u>

The costs of meeting KYC requirements shouldn't be much beyond that for credit assessment purposes. Robust credit assessment procedures should mean that meeting KYC requirements fall within this. Any costs would be relatively minor, eg stationery for copying ID, storage and retrieval costs. These would be offset to some extent by savings/benefit from fraud prevention, however.

<u>Question 5</u>

Option 3 as mentioned in 5.13 above."

ILAG

Investment & Life Assurance Group
The Practitioner Voice

Mr Daniel Shonfield
The Financial Services Authority
25 The North Colonnade
Canary Wharf
London
E14 5HS

27 January 2004

Dear Mr Shonfield

DP22: Reducing Money Laundering Risk

ILAG is a professional representative body concerned with the future of the investment, life assurance and pensions industry. It is led by practitioners, and aims to identify and develop industry best practice.

The Group currently has a growing membership of around 50 practitioner companies and associate members. In addition, a number of individual members are affiliated to the Group.

ILAG's preferred option is 4 and the answers to the questions 1 to 4 below should only be taken into account should this option not be the way forward.

In DP26 FSA have highlighted a potential re-write of the Money Laundering Source Book.

In view of this we consider that the only option that FSA can chose at this time is option 4.

We would be happy to discuss this response in more detail

Yours sincerely

Mark Searle
Technical Administrator

Telephone: 031342 312248
Fax: 01342 312609
Email: mark.searle@ilag.co.uk

Question 1: How necessary is the collection of KYC information and an active approach to monitoring in reducing money laundering risk, and in meeting legal and regulatory obligations, in particular reporting?

Whilst there is an obvious benefit in having additional KYC information, this will only materialise where there is some form of independent verification of the information obtained.

It is likely that any unverified information will always support the transaction and business relationship the customer is undertaking.

Additional unverified KYC information supporting the transaction and/or business relationship may lead to what otherwise would have been a suspicious transaction being deemed as not suspicious and therefore not reported.

Any recommendations for monitoring systems need to ensure that they are commensurate with the volume of transactions made, and the perceived risk of being used by money launderers.

Therefore due to the diverse nature of the types of transactions, customers, and sales distribution channels, it is desirable to have high level requirements which individual firms can use in a risk based approach to determine the appropriate systems to meet their requirements.

Question 2: How should firms pursue a risk-based approach to anti money laundering?

FSA's briefing note in July 2003 entitled "Identification of existing customers by regulated firms" highlights:

- The current requirements to establish and maintain effective systems and controls for countering the risk of financial crime including money laundering

- That firms that do not address such risks are exposing themselves to the possibility of action for breach of the FSA rules and/or the UK Money Laundering Regulations

This has given firms some insight into what is required with respect to addressing money-laundering risks, with particular attention to the verification of identity.

Telephone: 031342 312248
Fax: 01342 312609
Email: mark.searle@ilag.co.uk

Firms should extend this to cover all money-laundering risks, and put in place appropriate controls.

This is not a one - off activity, as it needs to be continuously reviewed to take into account all appropriate internal and external factors that may affect them, including any notices of fines where there have been failures in a firms anti-money laundering systems and controls.

Question 3: What type of monitoring (and reports) would be most useful to law enforcement agencies?

Whilst this question has probably been aimed at the law enforcement agencies, it would make sense for the standard reporting form to be simple to understand and use with sufficient flexibility to cater for the majority of the reports that will be made.

Question 4: What are, or may be, the costs and benefits of KYC and monitoring?

Without the details of the proposed requirements, it is not possible to determine what the associated costs would be.

One question we would like to raise, is how does the additional acquisition and on going maintenance costs associated with any extra KYC and monitoring fit in the post Sandler world where charge caps will operate?

Question 5: Which options presented do you prefer and why?

The reasons for supporting option 4 are well documented in DP 22, and ILAG would support the deferment for a period of possibly up to two years. This would allow the industry further time to get to grips with the changes that have taken place and those that we know will be taking place.

It would also make sense should FSA pursue the idea raised in DP 26, of replacing the Money Laundering Sourcebook.

Ends

Telephone: 031342 312248
Fax: 01342 312609
Email: mark.searle@ilag.co.uk

29 January 2004

*** By E-mail ***

Daniel Shonfeld
Financial Services Authority
25 The North Colonnade
Canary Wharf
London
E14 5HS

Dear Daniel,

Discussion Paper 22: Reducing money laundering risk
Know Your Customer and anti-money laundering monitoring

As you know, the IMA represents the UK-based investment management industry. Our members include independent fund managers, the investment arms of banks, life insurers and investment banks, and the managers of occupational pension schemes. They are responsible for the management of over £2 trillion of assets held by institutional funds (eg. pension and life funds), private client portfolios, authorised investment funds (ie. unit trusts and open-ended investment companies) and a wide range of other pooled investment vehicles. In particular, our members represent 99% of funds under management in UK-authorised investment funds.

The issues our members would face in the context of KYC and monitoring for anti-money laundering purposes vary considerably, depending upon which of the above activities they undertake. Broadly, though, we are talking about the provision of investment management versus the operation of collective investment schemes.

Our responses to the specific questions raised in DP22 are set out in a separate Annex. However, we have sought to highlight below the key issues that arise for our members on this subject, which will repeat some of the points made in the Annex.

Risk-based approach

We welcome the confirmation provided in DP22 of the FSA's commitment to a risk-based approach to combating money laundering. However, there is still much to be done in this respect, both by the industry and by the FSA, to elevate this from being a handy term to use in certain situations to something with a real practical application.

For our part, the industry, through the 2004 rewrite of the JMLSG Guidance Notes, is developing guidance as to how to adopt and apply a risk-based approach - hitherto the term arguably has been used as a somewhat bland and unhelpful substitute for providing detailed guidance. A clear statement as to the FSA's acceptance of the enhanced JMLSG guidance in this respect would be helpful. The industry then needs to see evidence of the FSA's commitment to such a stance in its approach to supervision, with recognition of a firm's

65 Kingsway London WC2B 6TD
Tel:+44(0)20 7831 0898 Fax:+44(0)20 7831 9975

www.investmentuk.org

proper application of a reasonable risk assessment process, even where the FSA itself might draw a different conclusion.

The bottom line of any risk-based approach and, indeed, with regard to the so-called "objective test" under by the Proceeds of Crime Act 2002, will always be a *subjective* judgment of the facts as they are known/understood at the time. Firms are naturally fearful that the FSA or the courts, often with the benefit of hindsight, will take a different view and invoke enforcement proceedings on that basis.

The policy line from both the Government and the FSA clearly favours a risk-based approach - this must also be promulgated through their enforcement of the regime.

The systematic approach to risk management, as described in paragraph 2.9, is sensible enough. However, it must be questioned whether or not we yet have the right tools to carry out the initial identification/assessment step. The most effective way to identify and assess risk is from appropriate case knowledge. We must find more case studies that are relevant to the differing products and services offered by various sectors of the industry, whether they have arisen from criminal assets that have been traced through investigation of predicate offences or identified as a result of suspicion reports from the regulated sector. Without these, how can a firm begin to appreciate how, and the real extent to which, their products are used for the purposes of money laundering?

<u>Know your customer</u>

We welcome the recognition in DP22 that it would not be appropriate for all types of firm to know their customers equally well (paragraph 3.17). Indeed, this is an area in which the impact on the different sections of the IMA's membership varies considerably.

On the one hand, investment managers generally need to collect information about their customer (be they private or institutional) in order to agree a suitable mandate for the activity they are going to carry out. This will include an understanding of the circumstances of the investor, the purpose of the investment and potentially, given the value, knowledge of the origin of the funds being used.

However, at the other end of the scale, CIS operators usually provide no investment advice and have no discretion over the investments. Certainly, there are no conduct of business reasons for them to collect additional KYC data and typically firms do not do so. To be required to collect, store and use such information would add considerably to their costs and would intrude upon investors (who may already have been required to provide the information to an intermediary in the process for their own purposes) where we have not done so before. The added value - the real difference it will make in terms of identifying and preventing money laundering - must, therefore, be considered carefully.

<u>Anti-money laundering monitoring</u>

Regular savings/withdrawal schemes notwithstanding, the products and services offered by IMA members are not typically "transactional" - they are vehicles in which funds reside rather than conduits through which funds are passed. However, that is not to say that their residence is necessarily long-term - investors in collective investment schemes, for example, may look to extract short-term gains or otherwise reverse recent investment decisions that perhaps appear to have been misjudged. In summary, although the majority of unitholders will tend to invest for the longer term, the definition of "typical" behaviour has to be very wide.

As such, we see little point in CIS operators attempting to implement sophisticated monitoring programmes, which are unlikely to identify anything that is beyond the boundaries of "normal" activity. Rather, those that have not already done so should be able to focus on exception reporting to identify successive purchase and redemption transactions within a very short timeframe.

Investment management is clearly less susceptible to early withdrawals and the investment activity is usually contained within the portfolio rather than driven by inflows and outflows of money. In many cases (eg. contributions to an occupational pension scheme or funding of school fees or regular income from a private client portfolio), these are understood as part of the KYC process and pre-planned.

What is more, to the extent that a criminal might seek to use the product or service as a vehicle for the process of money laundering (layering, integration etc.), the potential benefit to them will be minimal as in the vast majority of cases firms will insist upon making repayment to the investor themselves, rather than to an unknown third party.

In many cases, investment managers do not actually handle their clients' funds - this is done by third party custodians, who will be regulated in their own right (at least insofar as the UK is concerned). The custodian will have their own anti-money laundering obligations and should be relied upon to ensure that inflows and outflows are from/to the expected counterparty bank accounts.

In summary, we would suggest that there would be no need for investment managers to put in place any specific activity monitoring, as inflows and outflows of funds are likely to be planned and discussed with the client.

Conclusions

Our overall message is that we are concerned that any additional requirements must add value demonstrably in terms of the fight against money laundering.

The industry as a whole must avoid creating an expectation (either by suggestion or through direct regulation) that firms should have in place processes to collect additional KYC information and/or implement transaction monitoring procedures that are unlikely to place any substantive barrier to money launderers or distinguish between bona fide investment activity and the process of money laundering activity.

That is not to say that firms should not be vigilant in this respect, merely that expectations should be realistic in terms of what can be done that will have a real impact.

In that light, we recommend that the FSA adopt a "wait-and-see" approach for the time being, thus allowing firms time to respond to the future development of the JMLSG guidance in light of the additional demands of the Proceeds of Crime Act 2002 and, indeed, to the new provision at Regulation 3(1)(b) of the Money Laundering Regulations 2003. The FSA may also be able to take account of developments in this area internationally.

In any event we would hope that, whatever you decide, firms would not be targeted retrospectively in relation to procedures in place prior to your regulatory policy being published.

I hope that our comments are of assistance to your deliberations on this issue. I would be very happy to discuss further any of the points we have raised should you feel that would be helpful.

Yours sincerely

David Broadway
Senior Technical Adviser

ANNEX

DISCUSSION PAPER 22 - RESPONSES TO QUESTIONS

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

The relevance of KYC information for monitoring purposes depends upon the nature of the monitoring. Certainly, for "transactional" products or services[1] there may be benefits in understanding the intended purpose of the customer in using that particular vehicle.

Such information will typically be required in any event by an investment manager, in order for them to understand the parameters that may affect their management of a client's portfolio, including the likely inflows and outflows of funds. As discussed in the covering letter, however, we do not see activity monitoring for the specific purposes of detecting money laundering as a necessary process in the context of investment management, as the addition and removal of funds will usually be effected in discussion between the client and the fund manager.

For CIS operators, we do not believe the collection of significant additional KYC information is likely to assist greatly in determining whether or not a particular customer's activity is suspicious. Indeed, we would suggest that a client's investment activity would not necessarily reflect their day-to-day circumstances. There are further complications where the business is placed through an intermediary both of whom would need to gather KYC information, but not necessarily the same - the investor is likely find it be highly intrusive if the CIS operator needs to go back to them for different information, or is unable to source it from the intermediary.

Clearly though, for higher value investments, it might be appropriate to look for political exposure or a demographic analysis of the customer (which can be often be done by reference to their place of residence) that is inconsistent with the amount concerned. Given the lack of any "normal" investment pattern - collective investment schemes are typically subject to ad hoc transactions - we believe it is only at the extremities (very short-term investment or unusually high value transactions) that monitoring will be of any real value.

In any event, there must be a question mark over the value of collecting KYC data without verifying its authenticity. It is very likely, for example, that an organised money launderer would deliberately provide KYC information that supported their planned investment activity. The burden of verifying the KYC information provided would, we believe, be prohibitive.

In addition, keeping the information up to date (with or without verification) for mass-market products would also, we believe, prove to be prohibitively onerous. Clearly, certain information is helpful once a suspicion has been raised, but we would suggest that current information collected as a part of a law enforcement investigation would be more useful.

[1] We would define these as products and services that are provided to facilitate the movement of funds from one person or place to another.

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

We would suggest that a risk-based approach is vital if the industry is not to waste valuable resources adding very little towards achieving the objective of combating financial crime.

Assessing the risk, however, cannot be done properly without *relevant* typologies to illustrate how different products and services are used for the purposes of money laundering, be that the simple investment of proceeds of crime or as part of a process of "cleaning" dirty money. It is here that law enforcement and NCIS can help by identifying and publishing a wider range of case studies - those that are currently available are largely focused on banking scenarios and complex shell structures, which do little to promote awareness or assist in the assessment of risk beyond the banking sector.

A key concern with a risk-based approach is that the final assessment of risk is ultimately a matter of subjective judgment and that the conclusions made at the outset by one person (in this case, the firm) may not concur with those made by another (law enforcement or the FSA) with the benefit of hindsight. As a result, practioners in the regulated sector will be fearful of enforcement action being taken against them for an innocent error of judgment or even a simple difference of opinion. Given this, it is key that the relevant authorities are prepared to differentiate between those who have undertaken a process earnestly put in place, but drawn a wrong or different conclusion, and those who have less regard for the money laundering risks and their mitigation.

As you know, a substantial feature of the revised 2004 JMLSG Guidance Notes will, subject to industry consultation in due course, be guidance on how to apply a risk-based approach. This will clearly be helpful in providing a single source of guidance, enabling firms to adopt at least a broadly similar approach to their peers and, hopefully, to draw similar conclusions. It would be helpful if the FSA in particular were able to indicate their clear acceptance of the JMLSG model.

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

We presume that this question is directed more at the law enforcement agencies themselves.

However, whatever the outcome of this consultation process, it needs to be understood that migrations to new systems (particularly as a result of outsourcing) and essential systems archiving will potentially interrupt the continuity of searchable data. Although the historic information will still be available in some form or another, its use for monitoring purposes will be limited. As we understand it, whilst information reported to NCIS is potentially helpful to law enforcement, who may be able to connect it with future criminal investigations, the percentage of prosecutions made as a result of SARs is extremely low. As such, this arguably does not justify great expense in the development of sophisticated monitoring and reporting in anything other than proven high-risk areas.

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

Clearly, for some higher-risk "transaction" based activities, where active monitoring may be justified, the benefit of collecting and using KYC information will be in the support it provides to that monitoring process. The IMA is not in a position to comment on the likely costs of either activity.

However, as mentioned above, we believe that the costs for CIS operators, starting from a position of not currently collecting extensive additional KYC, will be considerable. In our response to Question 1, we have set out what we believe may be a sensible approach, both in terms of KYC and monitoring, the costs of which might be sufficiently low for the business case to be supported.

We do not believe that investment managers, on the other hand, would need to go much further than they already need to do for the purposes of that activity.

We also urge the FSA to be sensitive to firms that operate in an international context, for whom the UK requirements should not be substantially different to those demanded by other EU Member States and FATF members.

Q5: Which options presented do you prefer and why?

Our overall conclusion at this stage is that the FSA should take Option 4 - make no decision now and review again in, say, 2 years.

This would give the FSA time to see how the issue is addressed by the JMLSG in their 2004 Guidance Notes, these being subject to industry and public consultation, and how firms and systems vendors in this area react to the regulatory risks in light of the Proceeds of Crime Act and wider demands of the Money Laundering Regulations 2003. It might also allow the UK to see how other countries respond to the same challenges.

Julie Allcock

Q1 = Very necessary. A lack of KYC information gives rise to a much greater risk of money laundering occurring without discovery. Where advisers know their clients well they are much less likely to be used to process money laundering transactions. The corollary to this is that if they know them too well or are dependent on the income generated from their business they may choose to ignore, or at least close their minds, to suspicions rather than report them.

However any KYC requirements introduced should respect the individuals right to privacy where appropriate. Lots of law abiding investors can have legitimate (and usually personal) reasons for not wanting to reveal the source of the funds or their net worth details. Q2 = A risk based approach may not be appropriate for smaller firms where say, 100% checking is carried out. The approach used must reflect the size of the firm, the nature of its business and the type of clients generally dealt with. The actual approach must be left to the judgement of senior management. Q3 = No comment Q4 = No comment Q5 = Option 1 with specific rules. Sadly I think only this would be effective. Many firms do not, in my experience, pay due respect to guidance. Consent = Yes
----
Remote Host: 81.174.209.116
Remote IP: 81.174.209.116
User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Referer:

.

KPMG

20 Farringdon Street
London EC4A 4PP
United Kingdom

Tel +44 (0) 20 7311 3853
Fax +44 (0) 20 7311 3630
DX 38050 Blackfriars

Private & confidential
Sarah Tracey
Financial Crime Policy Unit
Prudential Standards Division
25 The North Colonnade
Canary Wharf
London E14 5HS

Your ref

Our ref kb/jm/519

Contact Karen Briggs
020 7311 3853

13 February 2004

Dear Ms Tracey

DP22 (Reducing money laundering risk) - Know Your Customer and anti-money laundering monitoring

Further to publication of the FSA's above referenced discussion paper ('the paper'), this letter sets out KPMG's response on the questions and options set out in the body of the paper.

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

The paper refers to 'Know Your Customer' or 'KYC', as being the additional information (e.g. occupation) that a firm may obtain for anti-money laundering ("AML") risk management purposes, over and above customer name and address. With regard to the collection of KYC information it is worth noting that:

- Determined criminals or members of organised crime groups will be inclined to present forged or stolen documents in support of claimed identities.
- Requesting documentation in support of identity is more likely to deter those criminals, who in relative terms possibly pose less threat to the UK's financial systems than, for example, organised crime groups.

As a result trying to identify or assess AML risk, based on name and address verification alone, will not work. The wider KYC requirement is necessary as this encourages firms to gather the raw information with which to be able to conduct a risk assessment based on other factors, such as *inter-alia*: Current occupation, Income/salary, Source of funds, Nature of business, etc.

Without the basic building blocks of knowing who the customer is and the why and how they conduct business, a firm is generally unable to make a reasoned assessment of the potential for money laundering risk arising from individual customers. A firm's risk based approach to money laundering prevention, using KYC and monitoring might, without the availability of such basic information be otherwise flawed.

Regarding the approach to monitoring, a distinction needs to be made between monitoring carried out within the business, and monitoring carried out by a firm's control functions, eg by Compliance or Internal Audit. In some firms with a small customer base it may be possible to manage risk without reliance on information technology. But, for others and particularly the larger firms dealing in high volume activity, they will probably place some reliance on analytical tools and models to identify exceptions to the norm. The design of such tools is reliant on the availability of up-to-date statistics, customer information and other data, with which to build a benchmark in a logical model.

Transaction monitoring procedures, assessing transactions against information documented in customer profiles, assists firms' to manage money laundering and fraud risk. The frequency of such monitoring, whether for *inter-alia*, credit, environmental or AML risk assessment, is a commercial decision influenced by the nature, scope and complexity of business undertaken, the markets involved and what is known or unknown about the parties involved.

By not adopting a systematic approach to monitoring or assessing change in market forces or risk, will leave firms potentially exposed. Suitable monitoring procedures provide a trigger to identify changes in risk profile, particularly when exceptions are identified out-with a customer's known profile. Therefore, some degree of monitoring for AML purposes should be considered a necessary standard practice.

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

The extent of risk management required depends on a number of filters, such as *inter*-alia, how firms interact with their clients (eg face-to-face or non face-to-face) and assessing which financial products or relationships provide the greatest risk of involvement in money laundering.

Other filters to consider in a risk-based assessment might include:

- Whether a business relationship or service provision is direct with a customer, or if it involves a third party, such as an intermediary, agent, etc.
- The location of providing services, together with the reliability and extent of management control will influence local compliance culture and risk management oversight.
- Any susceptibility a particular service has to money laundering or financial crime. For example, different risks arise in over the counter cash based business when compared with on-line banking. In the former, customers are face-to-face, whereas in the latter they might not even be in the same country.
- The nature, style and volume of sales, dealing, etc of the services offered. This might include monitoring threshold balance, increase in volume, turnover activity or other trigger leading to an exception report for risk-review by management.

- The demographic population of the customer base and any identifiable bias towards use of typical products/services. This would aid identification of average sales, volumes, turnover, or other statistical factors where exceptions to the norm could be identified for review.
- Stratifying business relationships into risk streams of high, medium and low. This would depend on a range of factors, possibly using industry agreed/identified benchmarks, guidance provided by the FSA, or internally defined by respective firms. The frequency and extent of risk management required would vary depending on which stream is involved. Those considered low risk would require less management than for the medium to high-risk categories.
- Business relationships having regular/routine activities wholly consistent with the customer's profile and/or industry norm would be less likely to be considered medium to high risk, as long as the customer profile was accurate and maintained appropriately.
- How the business is/was introduced and/or maintained.
- How comprehensive and up-to-date the KYC is, particularly on higher risk customers. Is there transparency in asset ownership, particularly where more than one firm or regulated body is involved?
- How a firm ensures that customer risk profiles take account of change made or anticipated in the regulatory regime.
- How the firm or group incorporates a global risk management policy into the local environment, particularly situated outside the UK. And how is this monitored?
- Do relationships involve non-ordinarily resident accounts?
- Is a business activity/relationship associated with a pre-1994 account, a KYC defective relationship, or a legacy account inherited from a merger relationship?
- Have business relationships (eg signatories, controlling parties, etc) been risk assessed against UN Sanctions, OFAC and/or other lists?
- Are KYC deficient accounts monitored until deficiencies rectified or the accounts closed?
- Is customer activity consistent with a benchmark for the type of client, nature of business, 'class of customer'?
- Is the activity or customer profile of a similar style/construct to frauds or other dishonesty, which have been subject of law enforcement public notices or publications (eg as produced by HM Customs, Met Police and NCIS).
- Does activity involve any of the past or present NCCT territories in any aspect?
- Is transaction activity consistent with gate-keeping profiles (eg employment)? If not, what are the variances and are they understood?
- Are credits/debits via other jurisdictions typical of the nature of customer relationship?

- Are there average thresholds (values or numbers of transaction) for typical customers' of the same class/category, etc?

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

In 2003 the Home Office published KPMG's report "Review of the regime for handling Suspicious Activity Reports". Part 2.6 of the report includes a summary of the key recommendations. We therefore refer you to this report for more detail. We do not believe we can comment further than the findings set out in that report.

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

From our experience of working with firms, infrastructure costs for KYC AML systems and controls vary between organizations. This was borne out by the FSA's own research on the cost/benefit review of extending the CCR Review. The costs are subject to factors such as, the product range, nature of customer base and geographic location of branch networks, along with any requirements to comply with national or international regulatory, legal or other commitments, including for example, any industry derived obligations (eg The Wolfsberg Principles).

Capturing gate-keeping information at account opening is a well-established principle and recognised cost of doing business. In some cases, for example when advancing credit, this is as much a part of routine business for commercial reasons as it is for meeting compliance obligations.

Perhaps due to the lack of an agreed standard about what is required for KYC compliance, the range of costs incurred by firms is probably variable and non-standard. Compliance costs for many firms might reduce and the standard of KYC obtained would also benefit from having a recognised KYC standard when collecting and analyzing relevant customer information.

The benefits of having a defined or near standard understanding of what is required to comply with KYC requirements, include:

- Data capture costs would reduce and benefit from economies of scale rather than collecting disparate data.
- Monitoring costs might reduce through standard data capture facilitating better use of IT systems and databases for monitoring/evaluation.
- Costs of internal compliance testing would reduce.
- The production of credible, industry standard, risk based customer profiles.

Q5: Which options presented do you prefer and why?

In broad terms, we consider the regulator's role to be the development of principles rather than defining detailed individual rules, which may or may not be suited to all of the lines of business undertaken by respective firms. Firms should be encouraged to develop effective systems and controls, to include countering financial crime (SYSC 3.2.6), to have appropriate, considered policies and practices for obtaining and using KYC information, and/or for monitoring their customers' accounts.

Our view of the preferred approach would, in part, be a combination of options one and two. We also believe it important to ensure consistency in how the FSA and firms address broader financial crime risks, including fraud, which is subject of the FSA's recent Discussion Paper DP 26. We believe it important that a cohesive resolution be promulgated on the range of issues that will no doubt be identified as a result of the FSA's consultations on both DP 22 and DP 26.

Prescriptive rules will not cater for all forms of financial crime risk encountered by firms. Their adoption would either be piecemeal or an administrative acknowledgement of a rule's existence, rather than promoting the underlying principle of preventing misuse of the UK's financial systems for criminal purposes.

We support development and continuance of a risk-based system, which incorporates scaleable due diligence and financial crime measures. Those measures being identified and implemented by firms, consistent with and integrated into their business activities, rather than implemented under specific detailed rules. Identifying the appropriate measures to take will, nevertheless, require senior management in firms to undertake or commission an assessment of their perceived money laundering risk.

In our view obtaining KYC information (over and above solely name and address verification) is a necessary risk management tool, albeit that some additional costs are involved. To ensure consistency in application of what may be relied on for establishing KYC, we believe that the FSA should provide some form of written guidance on what it considers to be acceptable, or an acknowledgement that KYC standards as set out in the JMLSG Guidance Notes is the benchmark against which firms could be assessed.

In addition to furthering a risk-based approach to dealing with financial crime risk, the FSA is we believe, ideally placed to provide, encourage or facilitate a coordinated effort amongst:

- Regulated firms - To identify and promote the principles of best practice found in anti-money laundering and financial crime initiatives across industry sectors.
- The law enforcement community - Particularly with regard to typologies or guidance for regulated firms on raising awareness of what to look for when considering money laundering or other serious crimes having a financial aspect. Firms face significant obligations on KYC and monitoring requirements. They are entitled to feedback, or other information to illustrate effectiveness of the UK's regime, which relies heavily on the financial sector to provide evidence of criminal money flows and/or asset identification.
- Supervisors of regulated firms - Particularly where generic but timely feedback could be provided as part of the FSA's training services on industry or sectoral issues identified in various reports that are available.

- Legislative bodies and other influential stakeholders – Particularly with regard to financial crime issues and their effect on the financial services industry, identified by regulated firms, and where change may be required in legislation. For example, changes in the Data Protection Act to enable, if not encourage regulated firms (with adequate safeguards) to exchange intelligence on suspected criminals or their activities. Safeguards would be required to protect the innocent but also to protect the employees of firms acting in the best interests of protecting the financial markets.

In conclusion, we welcome the opportunity to contribute to the wider discussion on anti-money laundering and financial crime as it affects the UK's financial sector. Should you wish to discuss the content of KPMG's contribution to the debate please do not hesitate to contact Karen Briggs, Giles Williams or Jon McNally.

Yours sincerely

KPMG LLP

Legal & General

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

Legal & General Group Plc
Legal & General House
Kingswood
Tadworth
Surrey
KT20 6EU.

Tel: 01737 376543
E-mail: angus.halton@landg.com

30 January, 2004

Dear Daniel,

Re: FSA Discussion Paper 22: Reducing money laundering risk

I am writing in response to the above Discussion Paper on behalf of Legal & General Group Plc.

We have also participated in the response prepared by the Association of British Insurers and we share the views of the industry as a whole that are expressed in that document.

As with all other financial institutions Legal & General take the fight against the use of our products for the purpose of money laundering extremely seriously.

We support an adoption of a more risk-based approach which, if implemented successfully, will create a more effective and flexible response to the risk of money laundering. However, against this background we are concerned that many of the issues raised in this discussion paper and references to best practice remain based on an understanding of money laundering risk as it affects the banking sector. Applying banking based recommendations to other industries within the financial sector restricts the development of a risk-based approach.

We would welcome more focus on the development of a generic framework that encourages the risk-based approach rather than concentration on particular prevention techniques, the use of which should be dependant on this approach.

One significant challenge with the risk based approach is to minimise confusion and barriers to saving that may result from additional anti-money laundering requirements and the different approaches taken by firms to meeting those requirements.

Comments on the specific questions and requests for information raised in DP22 are below.

Should you require further clarification on any of the points made, please do not hesitate to contact me. I will, of course, be happy to discuss.

Yours sincerely,

Angus Halton
Compliance Director, Money Laundering Controls

Question 1 -
How necessary is the collection of KYC information and an active approach to monitoring in reducing money laundering risk and in meeting legal and regulatory obligations, in particular reporting?

The relevance of KYC information and an active approach to monitoring in meeting legal and regulatory obligations is very much dependant on the risk profiles of the products or services that may be purchased and used for money laundering. Any approach to the use of these approaches therefore needs to be proportionate in terms of the risk presented and the costs incurred.

However, we see KYC and monitoring as separate issues and so we have split the remainder of our response to this question accordingly:

<u>KYC</u>

In assessing suspicions, the most useful information is (apart from a clear explanation of why the suspicion arose):
- Age of the applicant;
- Place of residence;
- Source of the funds for the transaction;
- Sources of wealth; and
- Employment.

Whilst useful in deciding whether or not a disclosure should be made, KYC is not the only means of assessing transactions. Often the basis for reporting is information provided voluntarily by the customer which could not be requested (for example admissions of tax evasion or previous criminal record).

Of course in situations where there is regular client contact as orders are taken or transactions confirmed the use of KYC information may be vital if changes of behaviour leading to a suspicion are to be spotted. However, KYC information must always be used with care, as a money launderer may supply information that will make transactions appear more legitimate than is truly the case.

Of equal importance is an understanding of the typical profile and behavior of a customer for a particular product.

There is an inverse relationship between the amount of KYC required to assess a suspicion and the flexibility built into a particular product. KYC is less relevant in detecting and assessing unusual behavior where the product concerned fulfills a very specific purpose (for example decreasing term assurance or Stakeholder pensions). In these circumstances unusual transactions may be identified by comparison to the normal customer profile for the product.

Additionally, less KYC information is normally gathered where business is transacted on a Direct Offer or Execution Only basis. With reduced product charges and advised sales becoming increasingly uneconomic for simplified products we envisage the non-advised route becoming a more widespread method of distribution. Lack of KYC information clearly increases the risks of products distributed by this method being used for money laundering. However, making the consumer fill out longer application forms may turn them away and damage the growth of these distribution channels. We consider it important that any new regulation in this area recognises that a balance needs to be struck between increasing the information required from customers and closing the savings gap by making it as easy as possible for consumers to take out savings products.

If new KYC requirements are made for certain categories of product risk, what action would firms be required to take on their existing customer base to bring it up to the new standard? It would not be practicable for many firms who have already conducted a current customer review to go back and reconsider it in the light of new requirements. If a new standard were adopted we would suggest that existing customers be excluded from the requirement.

Active Approach to Monitoring

DP22 has been widely discussed across a number of forums (including the FSA's own workshop on the subject) and it is apparent that there is some confusion as to what is meant by monitoring. Specifically, some interpret monitoring controls to include awareness training of staff (who then 'spot' suspicious transactions in the course of their work) whilst others take the view that monitoring is a separate exercise, designed specifically to detect unusual transactions which either individuals failed to spot or could not be identified manually. A definition of monitoring would therefore give clarity to this discussion.

At paragraph 4.4 your paper concludes that a firm that does not attempt to pick up what may be unusual for its business may be exposing itself to a higher risk of money laundering (and falling short of these obligations) than a firm taking an active approach. This conclusion is a significant departure from the written requirements of the law and FSA regulations and if this is to be the FSA interpretation then it should be subject to wide consultation. The Money Laundering Regulations require firms to take "*such other procedures of internal control and communication as may be appropriate for the purposes of forestalling and preventing money laundering*". Whilst monitoring may be an appropriate anti-money laundering control for some firms, the current conversion rates (i.e. the proportion of Suspicious Activity Reports generated from the population of unusual transactions identified) experienced by firms employing transaction monitoring are low enough to suggest that they cannot (yet) be considered an appropriate control as required by law. Likewise under SYSC 3 it would be difficult to interpret such inefficient monitoring systems as appropriate controls.

Products or services which are subject to frequent transactions that can be expected to exhibit a pattern lend themselves more to transaction monitoring than products whose life cycle will typically consist of only one or two interactions between the product or service provider and the client. In these circumstances it is necessary to identify individual transaction types that may be suspicious and are worthy of investigation. Where products are subject to fewer transactions in their lifetime, and so do not establish their own pattern, staff awareness and training is a crucial component in the risk mitigation process.

In conclusion, in certain circumstances where the features of the product are suitable, an active approach to monitoring may reduce money-laundering risk. There is no evidence to indicate that the current methods of monitoring (e.g. manual, exception reporting, and automated systems) are sufficiently accurate to be classified as an appropriate control for the purpose of meeting legal and regulatory obligations.

Question 2 –
How should firms pursue a risk-based approach to anti-money laundering?

Use of an effective risk based approach would lead to the finite resources of individual firms being targeted where they can make the biggest contribution to the prevention of money laundering resulting in the following achievements:

- an increase in the quality of controls designed to prevent money laundering;
- different controls being used in different parts of the financial sector, increasing the cost to the criminal of using the proceeds of crime in the financial system; and
- a flexible approach which would allow firms to respond quickly to emerging threats.

When developing a risk based approach it is important that the risk is considered in conjunction with the product or service characteristics (product risk), the distribution method for the product or service (channel risk) and types of client who use or purchase the product or service (client risk). Each of these component elements will have risks that are consistent across firms and industries within the financial sector, but the combination of them will produce a risk assessment that is tailored to the individual firm.

The risk assessment should drive the measures taken to control risk, including increased information requirements and monitoring of higher risk rated relationships.

However, there are a number of barriers to creating an effective risk based approach.

A strength of this approach is that each individual firm will arrive at a risk assessment based on its particular combination of circumstances and therefore the approach taken may also be unique to it. It is important that whilst this approach is supported, it is recognised that the component risks that make up the assessment will be common across firms in a particular industry (for example product risk) and in some cases between industries (for example the risk presented by overseas clients). Whilst it is right that firms should be responsible for developing their own risk assessments, guidance is required from trade bodies and the FSA / Government to ensure that firms treat the component risks consistently.

One significant danger of a risk-based approach is that inconsistent approaches to risk lead to customers being required to satisfy different requirements for the same product by different firms. This would cause confusion amongst consumers and intermediaries and competition will cause the least onerous requirements to become widespread, when they may not be appropriate. Intervention by trade bodies and/or the regulator is required to ensure the consumer is presented with consistent requirements.

The accuracy of a risk assessment relies in part on the quality and amount of information considered. Currently there is very little evidential information on how the proceeds of crime are money-laundered in the financial system using anything other than banking products. The risk is therefore that a risk based approach for non-banking sectors of the financial system will be reliant on theory and supposition which may produce ineffective results. A regular dialogue between firms, the FSA and Government, such as that proposed in October 2002 in the HM Treasury paper entitled 'Combating The Financing of Terrorism: A Report on UK Action', would enable firms to keep abreast of developments and enable them to develop their systems as new risks come to light.

A risk-based approach assumes that it is acceptable to tolerate some risk and by implication, there will be some instances where cases of money laundering occur and remain undetected. Once a case is discovered it may be apparent in retrospect, that the approach taken was flawed, even though it appeared reasonable before the case came to light. Firms have to take a 'leap of faith' (in Mr Shonfeld's own words) that the regulator will recognise the difficulties in developing a risk based approach in the absence of good quality evidence of the risks (as discussed above). Some overt support from the FSA for this approach is required if firms are to adopt this approach.

Question 3 –
What type of monitoring (and reports) would be most useful to law enforcement agencies?

We consider that this is best answered by the agencies themselves. However, there is a role for regulated firms to play in discussing the types of reports that can be provided to agencies, and for them to outline to us what they would find useful. This could be accomplished using the forum proposed above.

In any case we would expect law enforcement agencies to only want reports of genuinely suspicious transactions as opposed to reports that include activity that is simply outside of the norm. A dialogue between the law enforcement agencies and regulated firms would help both sides identify what is suspicious.

Question 4 –
What are, or may be, the costs and benefits of KYC and monitoring?

There are various costs associated with KYC and monitoring. These can be summarised under the following headings:

<u>IT</u>

The degree of sophistication and complexity required for a fully integrated transaction monitoring system that would be able to detect patterns of customer behavior across different computer systems and generate automatic alerts would be considerable due to the complexity of our systems and number of legacy products. It has been estimated that the implementation of such a system would be likely to exceed £1million. In addition, there would then be operational and monitoring costs that would be incurred on an ongoing basis.

Less sophisticated systems cost much less, however they would not be able to detect patterns of behavior. Instead they would be limited to scans that look to identify specific behavior that may be suspicious or identify specific client profiles. Such a system is clearly limited in its use and great care would need to be taken to identify the events to scan for, if a large number of extraneous cases are to be avoided. A basic system such as this is still likely to exceed £100,000 to implement, and once again there would also be ongoing operational costs.

Staff

There will be a need to monitor, analyse and interpret the results of any transaction monitoring systems, if they are to add true value, and to ensure that only genuinely suspicious transactions are reported. If transactions are considered in conjunction with KYC information, which may be necessary if individuals are to be protected from a failure to disclose an offence under POCA, this will also require additional staff time in implementation, and the additional checking will increase processing times and costs. These requirements will all add to staff recruitment, training and retention costs.

Client Service

Any systems or processes developed to monitor transactions or gather KYC information will need to ensure that customer service is not affected. Otherwise there may be a reputational cost in that customers will feel the industry, or particular firms, demand too much and place too many hurdles in the way of what are to them perfectly innocent transactions. Any systems should not discourage individuals from purchasing financial services, particularly at a time when a clear 'savings gap' has been identified.

Storage

If additional KYC information is to be gathered then this will need to be stored alongside existing client information, and will need to be readily accessible. This will lead to an increase in storage costs, be they the cost of additional physical warehouse space, or the cost of increased computer storage space if the information is held as a digital image or record.

The benefits that increased use of KYC and transaction monitoring would bring are less easy to quantify. We would expect there to be fewer erroneous reports made, saving time on fruitless investigations, and if any measures taken as an industry were effective in reducing the amounts of financial crime, we would expect this to have a positive impact on the reputation of the industry.

Question 5 –
Which options presented do you prefer and why?

In order of preference we make the following comments:

Option 2

We would welcome a focus of effort in this area, in preference to setting rules and/or guidance on specific money laundering prevention techniques, the use of which should be dependant on a risk based approach.

Option 4

Specific rules and guidance on money laundering prevention techniques should be provided once the risk based approach has been implemented and greater information is available from NCIS and the Law enforcement agencies. We do not feel that creating more regulation on specific issues before this approach and the changes to NCIS are implemented is worthwhile.

Option 3

The radical review of JMLSG should concentrate on creating a structure which assists in the development of a risk based approach, for example by providing industry specific guidance on product risk categories.

Option 1

Where any additional requirements would have an impact either on customers, or on the customer experience (in particular additional requirements to provide KYC information), we believe rules should be laid that will bind all firms, and so ensure uniformity across the industry. We consider it important that product providers, intermediaries and consumers have a clear, common understanding of the requirements and this approach would make consumer education possible. We do not feel however, that new rules and regulations should come in advance of implementing an effective risk based approach.

Request at paragraph 5.16 (i)
How firms currently match up to the risk management considerations (i.e. how aware are we of our business being used in connection with money laundering, and to taking appropriate measures (and devoting adequate resources) to prevent money laundering, facilitate its detection and monitor its incidence)?

At present the lack of information from law enforcement agencies on how (and to what extent) pensions, protection and investment products are used for the purposes of money laundering makes the assessment of the effectiveness of our current anti-money laundering measures extremely difficult to assess. Rather than making informed decisions about where resources should be placed, in order to have the greatest affect, decisions have to be made based on assessments of probability.

To some extent, evidence that the risk of regulatory action will result from weaknesses in money laundering controls is greater than the evidence of underlying money laundering risk in the insurance sector. There is a danger that regulatory risk drives the allocation of resources to prevent money laundering, as there is insufficient information available to assess the underlying risk of money laundering that a firm faces.

Request at paragraph 5.16 (iii)
The actual or potential costs of an active, but risk-based, approach by firms to KYC and to monitoring.

We have commented in detail on the costs and benefits of KYC and Monitoring in our response to question 5.

Any costs incurred will be in addition to business as usual expenses, which is why we are of the opinion that any requirements must be proportionate to the risks and apply equally across business sectors to avoid the potential for firms to benefit from a lower cost base in relation to the prevention of money laundering through different interpretation of guidance. If these criteria are met then any costs should be met with a view to truly reducing financial crime. These costs will, however, inevitably be passed onto consumers, through product pricing, where possible, and where this is not possible, i.e. Stakeholder, there may need to be a degree of cross subsidy.

Request at paragraph 5.16 (iv)
Are firms are confident that they understand the FSA's regulatory requirements and what it expects of them.

We are confident that we understand the requirements as they stand.

The situation is less clear with regard to the FSA expectations. These are less well defined in the handbook and our understanding of them is formed from the various communication channels that the FSA employs (eg Conference speeches, CEO letters, final notices). In particular, various final notices have referred to failure rates on identity verification and now the length of time elapsing between receipt of a suspicion report to the MLRO and disclosure to NCIS . Until these notices are issued there has been no communication on what the FSA views as acceptable levels for these statistics. We would welcome more dialogue with the FSA on their expectations surrounding the effectiveness of money laundering controls.

It is important that if any new requirements are considered necessary they are clear in their application and that they apply equally across firms.

Liverpool Victoria

Daniel Shonfield
The Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

28th January 2004

Dear Mr Shonfield

Discussion Paper 22: Reducing Money Laundering Risk

Further to our letter dated 26th January, we would like to now add a further comment following our review of DP26 Developing the FSA's policy on fraud and dishonesty.

Option 4 of the paper states that the FSA will modify the Handbook, by bringing together and clarifying provisions on fraud risk management in the Handbook. The FSA also proposes considering replacing the ML sourcebook with a more high-level, unified approach, focusing on financial crime risk management. In view of this option, we believe that the only choice available to the FSA at this time under DP22, is option 4.

I hope that these comments are of assistance.

Yours sincerely

David Nicholls
Group Director Corporate Governance

Liverpool Victoria County Gates Bournemouth BH1 2NF

Liverpool Victoria

Daniel Shonfield
The Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

26th January 2004

Dear Mr Shonfield

Discussion Paper 22: Reducing Money Laundering Risk

The Liverpool Victoria Friendly Society was founded in 1843 and is today the largest friendly society in the United Kingdom, with over 2 million members and customers, and assets of around £6.5 billion. Subsidiaries of the Friendly Society include an IFA, a Bank, a Portfolio Manager, a Life Company and a General Insurance Company.

The responses to the questions below take into consideration the activities of all the ~~regulated~~ companies ~~referred~~ to above.

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

   Any KYC information provided by the customer that cannot be easily independently verified is of no use whatsoever as it would always appear to justify the customer's position and the business relationship entered into. As a result obtaining additional KYC information will probably have little impact on a firm's legal and regulatory obligations.

   Indeed, it might even have a negative effect on the reporting of suspicious transactions as some transactions might well have been deemed suspicious if it was not for the additional unverified KYC information obtained which would seem to justify the transaction.

   Automated monitoring systems are commonplace in the banking sector and successfully highlight transactions that are unusual in nature in line with customer and product usage experience.

   Such systems could also benefit other sectors of the firm where there are large numbers of regular transactions and where an individual customer's transactions can vary significantly. However, a blanket approach to monitoring across the financial services industry is not appropriate – requirements must be linked to the type of product and service and its perceived risk of being used by money launderers.

2. *How should firms pursue a risk based approach to anti money laundering?*

   As part of the overall risk assessment exercise, a firm should assess all the potential money laundering risks relating to its products and services and distribution channels. The firm should then put in appropriate controls to mitigate these risks. This is an on-going process to ensure that the risk assessments and the controls remain appropriate bearing in mind internal and external factors which may affect them.

   It must be recognised that in the large majority of cases the risk assessments and associated controls are determined with the best intentions and that they are personal. Enforcement action should only be contemplated where it can be determined that the assessments and controls were inadequate as a result of negligence or having poor regard to their responsibilities.

4. *What are, or may be, the costs and benefits of KYC and monitoring?*

   It is difficult to assess what the costs would be without knowing the detail of the requirements for the various sectors of the financial services industry. The additional acquisition and maintenance costs as a result of any further KYC and monitoring requirements must be taken into account when determining the levels of any charge caps that may be applicable in the post Sandler environment.

   We are all working towards reducing the opportunities for money laundering and appropriate and effective KYC information and transaction monitoring would assist progress towards this goal.

5. *Which options presented do you prefer and why?*

   Option 4 is our preferred option for all the reasons contained in the paper. However we would be supportive of the issue of guidance to promote better money laundering risk management, as outlined in option 2, in the interim period.

I hope that these comments are of assistance.

Yours sincerely

David Nicholls
Group Director Corporate Governance

LIBA

LONDON INVESTMENT BANKING ASSOCIATION
6 Frederick's Place, London, EC2R 8BT
Tel: 020 7796 3606 Fax: 020 7796 4345
E-mail: liba@liba.org.uk Website: www.liba.org.uk

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

Our ref: PJM/COM 52

30th January 2004

Dear Mr Shonfeld

Response to DP 22 Reducing money laundering risk

LIBA is the principal trade association in the United Kingdom for firms active in the investment banking and securities industry. The Association represents the interests of its Members on all aspects of their business and promotes their views to the authorities in the United Kingdom, the European Union and elsewhere.

Background
In the past few years unprecedented attention has been focused nationally and internationally on anti-money laundering practice and the associated laws, regulations and rules that surround it. This has resulted in significant changes to anti-money laundering requirements in most, if not all, jurisdictions in which our Members transact business. However, despite the genuine efforts of the FATF and many of the regulatory authorities, especially the FSA, there remain differing standards across jurisdictions making it difficult for international groups to implement universal anti-money laundering practices.

We would encourage the FSA to engage other regulators internationally in this debate so as to obtain greater consistency in anti-money laundering requirements. Without this consistency business is potentially adversely effected and it permits regulatory arbitrage by firms and clients, creating opportunities for money laundering. There is a danger that clients will gravitate to firms and countries with lesser standards.

There have been a number of significant changes to the UK's anti-money laundering laws and regulations to reflect the developing international environment and dynamic national good practices. For example, FATF's revision of its Forty Recommendations and issuing eight Special Recommendations; implementation of the Second EU Money Laundering Directive; the Proceeds of Crime Act 2002; the two sets of Money Laundering Regulations; new US requirements aimed at tightening up customer identification requirements; amendments to the JMLSG Guidance Notes 2001 to reflect the new regulatory requirements and developing good industry practices. These have had to be absorbed and acted upon by our Members. In addition the rewriting of the JMLSG Guidance Notes is taking place at the moment and there are proposals for a Third EU Money Laundering Directive and further initiatives likely from FATF. Also the FSA has suggested in DP 26: "Developing our policy on fraud and dishonesty", that it is "considering the case for replacing the money laundering sourcebook with a more high-level, unified and succinct approach" focusing on financial crime risk management, including both money laundering and fraud (paragraph 7.13). Our Members are conscious that there is much in the pipeline and this needs to be considered when or if changes are being contemplated.

Monitoring
We have commented on the important issue of *monitoring* in our detailed answers to the questions posed in the DP. The checking of a firm's internal procedures is necessary and, for example, provides comfort on compliance with Regulations, ML sourcebook and its own procedures. As a general comment we do not consider that monitoring should be required to go beyond this and have some concern that DP 22 might be suggesting otherwise. It seems that the industry may be being asked to install monitoring processes that are designed to "catch the money launderers". We do not consider this a job for the industry. We should not be regarded as an extension of the police forces. The law does not require firms to monitor their clients in the way that a police force might undertake such a task. We consider the law correct in not including such a requirement and ask the FSA to consider this before deciding whether additional rules and guidance are necessary.

The retail banking industry appears to have a more certain view of what it is required to do in relation to monitoring of clients than other sectors. This may be because of its position at the front end of the money laundering process. Some clarification of this situation may be aided by guidance.

The FSA should maintain a watch over developments taking place in other countries. Switzerland, for example, has introduced monitoring requirements that come into effect in July 2004 and perhaps useful lessons can be learnt from the Swiss experience
.

The Four Options
DP 22 asks the industry to reflect on four options posing the question "Which options presented do you prefer and why?" We have considered these options in the light of current and future requirements being imposed on the industry and the significant costs associated with them. **We do not see any one option as an optimal choice.** We strongly recommend that the FSA keep the current situation under review (Option 4) especially by continuing its engagement with the industry. This review should be on going and continuous, reflecting the dynamic nature of anti-money laundering practices. In addition there may be need to clarify the FSA's position on a number of issues by the introduction of some guidance on money laundering risk management (Option 2) and also on its interpretation of a risk-based approach. It may be that this can be achieved through industry guidance so we recommend that the FSA work closely with the JMLSG and others that produce industry guidance to ensure a joined up view is conveyed.

We do not see a need, nor do we consider it appropriate, at this time to make significant changes to the FSA ML sourcebook (Option 1). This route should only be taken if there are clear deficiencies in the ML sourcebook or if the FSA considers it necessary to strengthen the rules in order to assist in the enforcement of anti-money laundering requirements. Recent FSA disciplinary cases have suggested that neither course of action is necessary. The current ML sourcebook appears to address the key issues and provides the FSA with sufficient flexibility to accommodate future changes to legislation and good industry practices.

The future for industry-led guidance

The FSA has recently stated its intention to reduce the number of rules, amount of prescription and size of the Handbook. The statement in DP 26 quoted above, regarding the replacement of the ML sourcebook, may be a part of this. We see the working relationship that has developed between the FSA and the JMLSG in particular as significant and important, it benefits both the industry and the regulator. This kind of co-operation should continue. However, we are disappointed by the FSA's lack of a proper endorsement of industry guidance in general and the JMLSG Guidance Notes in particular (current recognition is contained in ML 3.1.4G).

In the future we see the necessity for the FSA to be prepared to endorse industry codes and guidance if it is intended that the Handbook should meet the FSA's stated objective. We see industry codes and guidance as necessary and an integral part of this development and encourage the FSA to consider taking this opportunity to create its policy on this by using the JMLSG Guidance Notes, that are carefully constructed and consulted upon, as the pilot. Perhaps this could be achieved through an *evidential provision* to indicate that compliance with the Guidance Notes would constitute compliance with the ML rules. However, such Guidance Notes should not be looked at by the FSA's staff as if they were rules, this gives rise to difficulties. We comment below on the need for the FSA's internal staff training to cover this.

We would be pleased to discuss our views on this with you if it would help to develop your thinking in this policy area.

Yours sincerely

Paul Martin
Director

We address the questions set out in DP 22 in this section of our response.

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

Collection of KYC information

The collection of KYC information plays a part in the detection of money laundering and is of particular relevance to investigating authorities. KYC information is also important to a firm's business generally. It assists a firm to understand its clients both individually and collectively, adding to the total knowledge it possesses about its business. The information gathered can be used in the planning of the future direction of a firm's business activities. It is also important in the planning of a firm's administration processes. It may also provide an insight into the interaction of a firm's employees with its clients.

We concur with DP 22's statement that: (1) KYC serves to help firms to manage effectively their money laundering risks, by reducing the likelihood that they will take on a money launderer as a new client and also increases the likelihood that they will detect the use of their products and services for money laundering and (2) KYC information assists firms in meeting their reporting obligations under the Proceeds of Crime Act 2002.

Monitoring

Monitoring is a process that may assist in identifying money laundering and transactions that may not be straightforward, for example, fraudulent transactions. Monitoring includes the observation processes (often included in training programmes) adopted by employees when carrying out a firm's business on behalf of clients. It is not solely the formal automated and manual monitoring procedures that firms have in place. Monitoring all transactions is undesirable too, as it makes it easier for launderers to circumvent notice where the business being transacted is consistently dishonest.

Monitoring aids in highlighting those activities that are unusual and which may therefore be suspicious. Such monitoring may take the form of reference to specific activity on a client's account, or by comparing the client's activity with the activity on the part of similar, peer group, clients.

Monitoring of inactive or dormant client accounts is also required to be able to identify future, possibly unnoticed, reactivation and unauthorised use.

Meeting legal and regulatory obligations

The degree of gathering KYC information and conducting monitoring exercises will vary with the size of the business, the nature of the client base, the level of direct involvement with the clients by senior management and the activities being transacted. This is especially so in investment banking business where there are varied types of business being undertaken. We do not think that firms should be required to adopt a specified approach to these activities. Firms should be undertaking KYC information collection and monitoring to assist them in meeting their money laundering risk management and reporting obligations.

We consider that the gathering of KYC information and having active monitoring systems aid in the recognition of money laundering activities and managing the risk to the firm. We do not consider that these processes actually reduce money laundering. We consider that money launderers that might use investment banks are well aware of the processes used to deter their activities. They therefore ensure that transactions entered into pass scrutiny. We agree that the knowledge by the professional money launderer of the existence of KYC information gathering and monitoring processes does probably cause them inconvenience and may deter some.

The significant increase in the supervision by the FSA in relation to money laundering regulation has increased the collection of KYC and monitoring generally. This has resulted in a significant increase in the reporting of transactions to NCIS. This is helping firms to meet their legal and regulatory obligations, particularly reporting.

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

As a general comment we consider that for a risk-based approach to be accepted by the industry the FSA will need to educate and ensure that its supervision staff understand what such an approach means and the various ways in which it can be achieved. There remains a concern within the industry that FSA is maintaining the "tick box" approach to the supervision of firms' anti-money laundering procedures. Consequently firms are reluctant to use their own initiatives to implement a risk-based approach in this area. Clearly this is an important issue and needs to be addressed promptly to overcome the perception, real or otherwise. We have observed that in practice a risk-based approach has created uncertainty and unease and wide differences of implementation processes.

A risk-based approach to money laundering prevention should serve to balance the costs associated with the necessary internal controls and reporting requirements, with the assessment of the threat of the firm being used in connection with money laundering and the needs of its clients, in particular the level of acceptable enquiries into their business affairs.

A risk-based approach should acknowledge that the money laundering threat to a firm differs across jurisdictions, products, services, delivery channels and clients. It should permit management to differentiate between their clients in a manner that matches the risk in those clients' business. It must also match the costs and benefits of the controls implemented to produce a cost effective system when viewed against the assessed risks.

There must be recognition by firms and regulators that a risk-based approach carries its own risks. It is not a zero failure system as has been pointed out by the FSA in its pronouncements on regulation generally. Such a system will inevitably result in some money laundering going undetected. It would be reasonable for the FSA to acknowledge, that provided a firm can demonstrate that its systems were applied robustly and proportionately in a particular case, it will not seek to question a firm's application of a risk-based approach. However, in applying a risk-based approach, a firm must have carried out in all cases the basic identity checks and the assessed necessary monitoring.

There needs to be an understanding that clients assessed as posing a higher risk of money laundering are not necessarily money launderers. Nor are those assessed as low risk not money launderers. Staff should be trained to be vigilant so as to make use of their experience and common sense when applying a firm's risk-based processes. In addition they will need to document their conclusions when a case is picked out.

A risk-based approach to anti-money laundering needs to start with the identification and assessment of the risk that has to be managed. It is likely that the firm will have to take into account the risk it faces in relation to wider financial crime. All relevant departments must therefore be involved in the identification and assessment process. In the case of the investment banking industry where there already exists a reasonably well developed risk-based approach to money laundering it will be a matter of revisiting existing procedures with a view to further enhancements. There is greater concentration on the knowledge of the clients' businesses rather than on products, services and delivery channels referred to below.

There needs to be clear delegation of responsibilities by the Board for carrying out the work. Management will need to ask itself a number of searching questions in assessing the likely use of the firm in connection with money laundering. For example:

- What is the threat to the firm being used in connection with money laundering?
- How could money be laundered through the firm?
- What risk is posed by the firm's clients?
- What risk is posed by the firm's products and services?
- What risk is posed by the firm's delivery channels?
- What countermeasures can the firm employ and to what extent to manage these risks most effectively?
- How will the firm know that its countermeasures are working effectively or that they need to be enhanced or modified?

All this will need carefully documenting and will form the basis for the high level controls framework for money laundering prevention. It will assist the firm's development of a policy statement regarding money laundering prevention. In addition the overall assessment of the risk to the firm from money laundering will be an aid to the firm's prudential risk assessment requirement.

This may necessitate carrying out an assessment of each product line, service and delivery channel and to decide which would be most likely to be used in connection with money laundering. In addition the firm's various client "take-on" procedures must be assessed for weaknesses that could be exploited by money launderers. Assessments need to be made of how clients are introduced and the countries where they reside and do business for their likely involvement in money laundering. This assessment will enable the firm to develop graduated client acceptance policies and procedures that require more due diligence for higher risk clients and minimum levels of identification. It should also enable the firm to identify characteristics tending to indicate lower and higher risk clients.

Monitoring systems need to be assessed and then concentrated onto those business areas most likely to be vulnerable to use in connection with money laundering.

In addition an assessment of the firm's reporting and reports will reveal patterns and products, services and client types that will be useful in the application of a risk-based approach.

A firm will need to keep its risk assessment up to date.

Finally it must be recognised that a risk-based approach may not be appropriate in all cases. A firm with a limited client base or product range where the risk is assessed as high may carry out more systematic, in depth checks for all its clients as a practical way of addressing the money laundering threat it faces.

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

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

- Where they have knowledge that a person is engaged in money laundering, or
- Where they suspect that a person is engaged in money laundering, or
- Where they have reasonable grounds for knowing or suspecting that a person is engaged in money laundering.

Firms therefore have an obligation to have procedures in place to enable them to fulfil this reporting requirement. We do not consider that monitoring systems should be required to be designed to catch the money launderers. The purpose must be to ensure compliance with the relevant legal and regulatory requirements. The industry should not be asked to be an extension of the police forces. We are all in danger of pursuing this goal unintentionally.

We do not consider it appropriate to refer to types of monitoring as the procedures followed by a particular firm will be dependent upon a number of factors including the size and nature of its business and the complexity and volume of the transactions or activity. For example in the retail banking sector, where there are large numbers of personal accounts and transactions to check, it is common for automated monitoring systems to be employed. Such systems will not be appropriate for all businesses and many firms will be unable to afford such sophisticated monitoring. Well planned and appropriate targeted manual monitoring procedures are effective. We must accept that we conduct business in a world of limited resources and that our monitoring systems will inevitably reflect that limitation.

We expect that the law enforcement agencies would like to see firms focus their monitoring on those areas of their business that are likely to produce significant results. In order for this to happen it is necessary for these agencies to provide incident profiles to the industry. These profiles will enable the industry to monitor likely clients, transactions and business. We understand that money launderers change their laundering habits to meet circumstances and also to reduce detection. The agencies need to have a mechanism in place to keep the industry up to date with this and so make the efforts of many firms more fruitful.

Appropriate "know your customer" procedures provide the basis for recognising unusual and suspicious transactions. The key to recognising suspicions is knowing enough about the client and his normal expected activities to recognise when a transaction or instruction or series of transactions or instructions is unusual. Any monitoring processes need to take account of this.

Reporting of transactions has to be made in the prescribed manner. Firms should provide additional supplementary information where they possess it and it is useful. This reporting has to take account of any Data Protection Act matters. We are sure the agencies would prefer that firms apply a degree of discretion when reporting transactions and have a review process to ensure that quality reporting takes place. However the firms are conscious of the legal obligations imposed upon them and therefore are advised by lawyers not to apply discretion when reporting. This is an area where guidance from the authorities could be helpful and so reduce the increasing number of defensive reports.

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

The costs associated with effective anti-money laundering management will likely be considerable for any firm, no matter what its size or business activities. These costs do not just include the time spent and the systems that have to be created and implemented. Account has to be taken of the on-going effort that has to be put into maintaining the momentum and ensuring that controls are up to date, reflecting management's assessment of the risks to the firm in connection with money laundering. Firms have difficulty in providing actual costs other than budgets for departments and projects.

The task of collecting KYC information involves considerable staff time and therefore inevitably costs. There is information that is required to be collected as part of the client identification process, part of KYC, that may not be necessary for normal business purposes. We consider that there is too much emphasis placed on the client identification procedures as if it were the answer to stopping launderers. The gathering of this information to the standards now expected by all authorities is very costly for all firms. It is people intensive, requires careful recording and storage facilities which will enable it to be readily retrievable. KYC information needs to be collected by all business areas and across all products and services supplied to clients. There really needs to be a facility to record all available information centrally and for it to be accessible to all business areas so that all associations and business activities can readily be known to all sectors of the business. Such a central data register would assist staff to assess whether the business is unusual in any way and therefore reportable.

Few firms have central databases containing "entire knowledge" of clients with their connections. Building such databases is a costly exercise and takes considerable human resources. With increased globalisation, the international firms are committing large sums and resources to providing these systems.

The benefit of these systems is that they are not just being built for money laundering purposes. The information is of general use to the business as a whole and can be compared with that obtained by high street retailers through point of sale systems. Such systems help plan the future needs of the business.

However, the systems must be seen as long term projects that will take years to develop fully.

Such sophisticated systems can also feed into automated monitoring systems, thereby providing client profiles and creating more accurate monitoring processing.

Whatever form of KYC and monitoring is installed - automated or manual - the costs are considerable and the benefits not always seen by the firms.

Which options presented do you prefer and why?

DP 22 sets out four options. We have considered these options and do not see any one option as optimal. Option 3 may be attractive as there have been so many changes and new requirements to come to terms with that time is needed for firms to adjust to them all. The latest version of the JMLSG Guidance Notes reflect these changes and current good practices and will need to be reviewed and implemented by firms as needed.

We do not consider Option 4 on its own to be a solution. We do consider that the FSA and industry will need to continue together to review the continuing developments in the money laundering field. This should be a continuing review and say in two years time culminate in a report or another discussion paper.

We do not consider that Option 1 is desirable at present. We have stated above that we consider it appropriate for FSA to monitor current developments and in two years time consider the position which should then entail consideration of including in the Handbook specific rules and/or guidance on KYC and/or monitoring. We understand that more international rules and regulations are being promulgated and will produce the need to develop further procedures. These should be reviewed and the Handbook developed as necessary.

We have considered Option 2. It may be appropriate for the FSA to give guidance on its view of a risk-based approach to the management of money laundering risk. We do not consider it necessary to have guidance on documentary policies for managing money laundering risk. There are already many policy documents that suggest this process and FSA's contribution to this is not necessary.

We therefore consider that no one Option is right and that a combination of Options 2 and 4 may be appropriate. We are aware that the FSA has developed a working relationship with the JMLSG and that the Guidance Notes can be developed in co-operation to reflect both the industry's good practices and FSA's views of procedures.

FSA asked for comments on whether firms are confident that they understand its regulatory requirements and what it expects of them.

We do not consider that the FSA has issued a clear enough policy on its regulatory requirements and what it expects of firms. Firms generally are concerned that the FSA is seeking for them to become the extension of the police forces that we mentioned above. Firms are not generally equipped to undertake such a role and do not see it as a role that they should be asked to perform.

The FSA also sent out a confused message when it sought the co-operation of the industry to undertake a retrospective review of the identity of all clients when the law did not require such reviews. The industry perceived this to be a policy more to protect FSA than to reduce the money laundering threat. It would also be expensive and in many commentators views unnecessary. The FSA had to withdraw from what was to have been a compulsory requirement for firms to undertake such a review. This followed the publication of an independent cost benefit analysis. However, the FSA's retraction statement still appeared to be requiring firms to undertake such an exercise. This has created difficulties within firms and demonstrates just how carefully matters of this nature need to be handled.

The industry accepts that firms should have controls in place to assist with the prevention of their use in money laundering. The major financial sector businesses have spent large sums on enhancing their procedures. However there is a need to ensure that there is a clear understanding of FSA's expectations of a risk-based approach to anti-money laundering procedures. We pointed out in our commentary above that there seems to be a difference between the policy makers and the supervision side of FSA and this needs to be corrected.

Financial Services Authority

Reducing Money Laundering Risk
Know Your Customer and anti-money laundering monitoring

Comments on Discussion Paper 22
Submitted by Mantas, Inc.

Submitted January 2004

Fairfax, Virginia 22033

1 Executive Summary

Mantas wishes to make the following key points in response to FSA DP22:

i. **The introduction of an AML monitoring standard, meeting regulatory requirements, would significantly improve AML controls among regulated firms**

Mantas sees benefits from both Option 2 and Option 3 as presented in the Discussion Paper, but believes that in order for the industry to really benefit from anti-money laundering controls, a monitoring standard needs to be put in place, which all regulated firms would need to meet in order to satisfy existing and future regulatory requirements.

ii. **The importance of adequate KYC and AML monitoring is paramount to fighting financial crime**:

Effective, comprehensive KYC and AML monitoring are necessary components in each firm's ability to contribute to the fight against money laundering, terrorist financing, and financial crime, and for the firm to meet its legal and regulatory obligations. Shortcuts and half measures are not sufficient; firms must take an active approach.

iii. **Effective KYC and AML programs underscore a risk-based approach to fighting money laundering:**

An effective and systematic KYC and AML monitoring program can support the successful execution of a risk-based approach as advocated by the FSA, as well as improve the quality of reports and leads provided to law enforcement.

iv. **Automated KYC and AML Monitoring programs offer benefits outside the scope of AML controls:**

The business realities of many firms necessitate an automated approach to KYC and AML programs – whether this automation is developed internally or involves a third party product or tool. Such products and systems can involve significant investment in money and resources. However, they also offer potential ancillary benefits.

v. **The FSA should recognise and encourage firms at the forefront of implementing effective AML controls:**

The FSA should consider the possibility of some form of incentive, through compensation or recognition, for firms who are leading the industry through their implementation of sophisticated AML systems and programs.

2 Introduction

Based in the US, and operating globally, Mantas, Inc. provides behaviour detection technology to financial services firms, through which behaviour in every transaction across an enterprise is analysed. This allows companies a comprehensive solution for avoiding risk and meeting regulatory requirements. Behaviour detection technology allows companies to uncover wrongdoing by finding suspicious patterns of behaviour hidden within voluminous data.

Mantas is used to deploy technology for anti-money laundering compliance, broker surveillance, best execution and trading compliance, fraud detection, and other purposes, providing Best Practices for some of the world's largest financial services institutions.

Mantas appreciates the opportunity to participate in the debate generated by the Financial Services Authority's Discussion Paper 22, *"Reducing Money Laundering Risk: Know Your Customer and anti-money laundering monitoring"*. Mantas share with the FSA, as well as with our clients and colleagues in the financial services industry, an appreciation of the importance of public confidence and trust in the financial services industry. In the areas of money laundering and financial crime, the potential risk to firms' reputations is particularly acute. Mantas' success is dependent on our ability to supply quality products, participate in relevant industry issues, and support our clients in their efforts to develop and share best practices.

Mantas have chosen to submit comments because we believe that we have a valuable perspective to share in the areas of effective Know Your Customer (KYC) and anti-money laundering programs. The positions offered are based on our perspective as an AML solutions vendor familiar with the technology available to financial services firms, as well as our experience working with a variety of financial institutions in their efforts to implement progressive and effective anti-money laundering programs.

Our submission to DP22 consists of a few notes addressing the specific topics of Know Your Customer (KYC) and anti-money laundering monitoring, followed by more specific responses to the FSA's questions.

3 Know Your Customer (KYC)

An effective, comprehensive Know Your Customer (KYC) program is a valuable component in each financial institution's ability to contribute to the fight against money laundering, terrorist financing, and financial crime, and for firms to meet their legal and regulatory obligations. Careful vetting of new customers, as well as systematic and regular updates of existing customer information, help the financial institution serve in its role as a careful gatekeeper against terrorists, fraudsters, and criminals.

Shortcuts and half measures are not sufficient; firms must take an active but appropriate approach in obtaining and utilizing pertinent information about their customers. Effective KYC and Customer Information programs are viewed as good practice by international bodies such as FATF and the Basel Committee, and are mandated in a number of countries such as the United States (Section 326 of the USA PATRIOT Act). The expectation is that firms will collect and use KYC information as appropriate and will take an active approach to monitoring. An effective program will ensure the protection of the institution. It also will assist firms in understanding their clients in a more thorough and complete manner.

In general, financial institutions already have extensive data on their clients. This data can and should be used in a thorough, but appropriate, manner. If the firm better leverages the data it already collects through various sources, it can achieve the goals of an effective KYC program without adding policies or procedures that its clients find to be intrusive or demeaning.

4 Anti-Money Laundering Monitoring

An effective, comprehensive AML monitoring program is a necessary component in each financial institution's ability to contribute to the fight against money laundering, terrorist financing, and financial crime. It is also necessary for firms to meet their legal and regulatory obligations. The business realities of many firms necessitate an automated approach to their AML monitoring programs. The number of accounts and clients is only one consideration. So many of the products and services offered today involve convenient, remote access points and channels that can aid potential money launderers and fraudsters as they attempt to avoid detection. This provision of convenience and ease of access, particularly through online means, also place customers at increased risk of fraud.

The implementation of a more sophisticated, automated approach may be achieved through internal development, as well as through one or more third party products or tools. Mantas' expertise in providing AML systems to major financial institutions has shown us that automated systems help the firm focus its valuable resources and expertise on value-added activities *(see Q1 below).* Rather than sampling, reviewing reports, and hunting for contextual information, these analysts and investigators are able to devote more of their time to actual investigations and the development of meaningful, actionable cases. This, in turn, can help improve the quality of reports and leads provided to law enforcement.

An effective and systematic KYC and AML monitoring program can support the successful execution of a risk-based approach as advocated by the FSA *(see Q2 below)*. The use of an automated product or system can involve significant investment in money and resources. However, it can also offer potential ancillary benefits, including a better understanding of customers and their needs and an enhanced ability to detect and prevent fraudulent activity *(see Q4 below)*.

5 Responses to Options and Questions

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

An effective, comprehensive Know Your Customer (KYC) and AML monitoring program is a valuable component in each financial institution's ability to contribute to the fight against money laundering, terrorist financing, and financial crime, and for firms to meet their legal and regulatory obligations. Careful vetting of new customers, as well as systematic and regular updates of existing customer information, help financial institutions serve in their de facto role of careful gatekeeper against terrorists, fraudsters, and criminals.

Effective KYC and AML programs are viewed as good practice by international bodies such as FATF, and are mandated in a growing number of countries. The FSA's consideration of further refining and institutionalizing such programs is certainly reasonable given the broad-based emphasis on these areas.

For some firms, an active approach to KYC and, in particular, to AML monitoring, will necessitate the implementation of an automated system to support the firms' analytical and investigative resources. Mantas believes that a monitoring system alone is not the only component; an effective program includes training, senior management support, and ongoing knowledge of business and industry imperatives that impact the firm's vulnerability to money laundering and financial crime. However, an automated system helps the firm focus its valuable resources and expertise on value-added activities. It can also help to enhance the quality of suspicious activity reports and leads provided to law enforcement.

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

At the FSA conference regarding Discussion Paper 22, participants voiced concerns about their ability to correctly interpret the meaning of "risk-based approach" as it pertains to each specific firm. This is not a problem isolated to the U. K. In other countries, regulations and guidelines that mandate a risk-based approach are similarly vague. The reality is that each firm will be judged by its regulator during periodic or special audits and reviews. Firms are concerned that they will be held accountable in such reviews for specific program elements that have not been articulated adequately in the existing regulations or guidelines, and that their approach will not pass muster with their reviewers.

Specific to this issue, our experience at Mantas has shown us that a systematic and robust monitoring program, such as that which can be achieved through the use of an automated system, helps to support an effective, risk-based approach. An automated system helps the firm develop and refine its risk assessments, and helps justify the approach the firm takes in managing its risk.

For example, the process of implementing a system serves as a catalyst for researching, evaluating, and making decisions about the type of monitoring required. This process exposes certain types of data and information, often for the first time. Once it has implemented the monitoring system, the firm can derive actual metrics on alerts or exceptions, the resulting cases or investigations, and the suspicious activity reports submitted to law enforcement. This type of analysis enables the firm to further refine its monitoring to constantly improve and adapt as trends and business or regulatory drivers evolve. It also indicates to reviewers that the firm is focusing on the right areas and its specific risk-based approach is sound.

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

Because of the pressure on firms to submit suspicious activity reports, there has been a focus on quantity, not quality. This exacerbates the problem of NCIS and other agencies' inability to thoroughly process and pursue the leads provided in these reports. As firms work to improve their overall KYC and monitoring programs, they can produce more actionable output and therefore more targeted, meaningful cases. More targeted alerts and cases contribute to a higher quality of SAR or STR. Fewer but more actionable SAR's / STR's would help address the key issue identified in the KPMG report on the U.K. SAR Regime – the fact that huge numbers of reports are generated, and NCIS and other law enforcement agencies can't possibly investigate all of them.

Mantas believes that modern approaches to establishing effective AML controls, though automated monitoring systems and complementary training, support and expertise, can be implemented to allow firms to concentrate on the quality rather than quantity of SARs.

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

The FSA have indicated its desire for a “proportionate” approach. Based on the discussions at the FSA meeting regarding DP22, both the FSA and regulated firms understand that proportionate does not mean “cheap”. The implementation of a robust KYC and monitoring program involves significant time, money and resources. This can be a difficult sell to senior management, because AML compliance typically is considered a sunk cost without any direct return on investment. Mantas’ experience has indicated that the firms who are leaders in this area have reframed the issue to one of overall risk management. They also have a long-term vision of how they will leverage the ancillary benefits that such programs can offer.

The implementation of an automated approach to monitoring can involve a significant investment. However, it can also offer potential ancillary benefits, such as an increase in the productivity and effectiveness of analysts and investigators. Another important benefit derives from the wealth of data that is collected for monitoring. This same data can be leveraged to help the firm develop a better understanding of its customers and their needs. It also can contribute directly to enhancements in fraud detection and prevention, a core component of the firm’s overall risk management program. Making optimal use of the firm’s data can help balance the need for information with the potential for intrusiveness that would be objectionable to customers.

Despite these potential benefits, Mantas suggest that the FSA consider the possibility of some form of incentive for firms who are leading the industry through their implementation of sophisticated AML systems and programs. This could take the form of compensation – such as tax breaks, although we understand that this would fall outside the FSA’s remit - or other type of reward or recognition. This would add the power of the carrot to the already utilized (or threatened) power of the stick – a very potent combination in a market economy

Q5: Which options presented do you prefer and why?

Mantas sees benefits from both Option 2 and Option 3. Option 2 has merits such as better high level guidance from the FSA that might help alleviate regulated firms’ concerns about a risk-based approach and what precisely that means. Option 2 is also more consistent with other countries (such as the United States) that have regulatory obligations for KYC and monitoring. The opportunity for the FSA to provide more specific guidance should always be considered as a viable alternative, particularly given the FSA’s approach of collaboration and consultation with industry and law enforcement. However, there exists concern within the industry that adding additional regulatory guidelines at this time may be excessive.

Option 3 would provide an opportunity for the firms to get in order their respective KYC and AML monitoring programs relative to the updated Guidance Notes. Retaining the reference to, and reliance on, these notes would provide a consistent environment in which firms could make significant progress in their AML regimes. The FSA can leverage the review process to make clear (through supervisory and enforcement action) the obligation firms have with respect to KYC and monitoring. However, we believe that reliance on the notes alone may not be sufficient, and would suggest that the FSA consider the publication of money laundering, terrorist financing, and financial crime typologies, methodologies, and cases, which would provide enormous benefit to regulated firms.

However, Mantas believes that the one measure that would be of real benefit to the industry is the introduction of a monitoring standard. This would require firms to put in place technology meeting certain requirements that would satisfy existing and future regulatory obligations. A standard could be developed via a technology steering committee that would coordinate consultation with all interested parties, from regulated firms to AML consultants and suppliers of automated systems. Such a move would ensure greater detection of money laundering activity, and a more qualitative basis for suspicious activity reporting without increasing the regulatory burden on financial institutions.

Mantas believe that such an approach will support the FSA's stated goals pertaining to financial crime, in particular its efforts to raise industry AML standards, achieve higher quality reports to law enforcement, and ensure proportionate costs to the financial services industry. This will enhance efforts to detect and prevent financial crime and, in turn, reflect positively on the industry's reputation and ensure public understanding of the advances being made.

[redacted]

MARKS & SPENCER | MONEY

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

28th January 2004

Dear Mr Shonfeld

<u>DP 22 - Reducing Money Laundering Risk – Know Your Customer and Anti-Money Laundering Monitoring</u>

In response to Discussion Paper 22 and the issues raised within it, we write with our response as follows:-

<u>Question 1</u>

The collection of KYC information is a vital tool to combat the risk of institutions being used as a vehicle for money laundering, and to guard against fraudulent activity. It is essential for financial institutions to satisfy themselves with regard to the true identity of the individual/entity they are entering into a business relationship with, and to understand why the customer wishes to open the account.

It is also imperative to conduct KYC checks from a regulatory perspective to avoid the risk of fine, and loss of reputation.

An active approach to monitoring enables firms to maintain an understanding of the customer's behavioural patterns, to assess whether a specific transaction is suspicious, illogical, and warrants reporting to NCIS.

<u>Question 2</u>

A risk-based approach to anti-money laundering should be implemented taking into account the product types on offer, the type of customer and the volumes of transactions/investments involved. Procedures implemented should also be proportionate to the costs involved. Where no major risk is identified, high level system changes would not be justified where costs

Marks & Spencer Money, Kings Meadow, Chester CH99 9FB. Tel: 0845 900 0900. Fax: 0845 300 0326. www.marksandspencer.com/money. See reverse for important information.

outweigh the benefit and risk. Where the product is deemed to be low risk (ie. no third party facilities allowed), the requirement to conduct id checks should be less onerous than for higher risk products allowing third party facilities. In such cases, a more thorough ongoing monitoring programme should also be implemented.

Question 3

Where the risk of money laundering is greater, comprehensive KYC information is beneficial to LEAs in building up an accurate picture to determine whether the case warrants further investigation.

Similarly, detailed record keeping of the customer's transactional history (application forms, transaction statements and communication logs), would also benefit LEAs in their investigation.

Question 4

1. The costs of adequate KYC checks and monitoring procedures include obtaining documentary evidence, conducting electronic checks, record keeping, training of staff, ongoing monitoring (manual or electronic), systems changes/upgrades, updating of KYC information and the drafting and implementation of procedures and policies.

2. The benefits of robust KYC and monitoring practices include the ability to establish the true identity of individual/entity concerned, protection against the risk of money laundering, fraud, other financial crime and profit loss, and protection against the risk of a fine from FSA.

Question 5

Having taken into account the issues raised in DP22, and having considered the 4 suggested options, Marks & Spencer Money would prefer to see a combination of Options 1 and 4 adopted.

We would favour specific rules on KYC and monitoring, set out in very clear terms adopting a risk based approach to be applied dependent on product type and customer.

Regulated firms would benefit from specific rules to provide a concise, defined framework for anti-money laundering KYC and monitoring measures. Enforceable requirements would bestow clarity on rules and guidance, which at times can be ambiguous to interpret. A clear, practical interpretation of these Rules should be defined within the Guidance Notes. We believe this approach would be particularly beneficial, especially in light of the recent fines meted out by the FSA to institutions for failures and weaknesses in KYC/monitoring procedures.

Customers would also benefit from a consistent approach across the industry, reducing confusion and increasing awareness of firms' expectations, and promoting a level playing field in terms of required checks for similar types of products.

However, we believe firms should be given the time to implement and embed the new obligations imposed on firms by the Money Laundering Regulations 2003 and also POCA. Defining specific FSA Rules in 2 years time would give the FSA the benefit of experience of the practical implications of these regulations and legislation.

Yours sincerely

Wendy Gee
Money Laundering Assistant

Regulatory Compliance

National Australia Group
Europe Limited
European Office
The Athenaeum
3rd Floor
8 Nelson Mandela Place
Glasgow
G2 1BN

Telephone 0141 223 5968
Facsimile 0141 223 1044

Date : 09 June 2004

The Financial Services Authority
Individual Vetting and Approval
25 The North Colonnade
Canary Wharf
LONDON
E14 5HS

Dear Sir/Madam

National Australia Group Europe:- Response to FSA DP22

Please find enclosed the response from National Australia Group Europe Ltd to FSA DP22 on behalf of its regulated and authorised subsidiaries.

I hope this is of use in developing the FSA's thinking in this important area.

Yours sincerely

Chris Terry
Policy Manager

DP 22:- Reducing Money Laundering Risk - Know your

customer (KYC) and anti-money laundering monitoring.

We welcome the opportunity to provide comment on the above paper. The paper itself is as timely as it is thought provoking. To keep our response concise we have focussed on the five key questions posed. We have also input to the British Banking Association (BBA) submission and would generally endorse the comments made in that submission.

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

There is little doubt that collection of KYC is, at its simplest, good basic banking practice and is an essential part of a robust and effective transaction-monitoring regime. We support the principle of a risk based approach promulgated in the paper and as such, in our view, there is not a requirement for a specific rule on collection of KYC at this time. Institutions should be taking a risk based approach, in line with their market, product and customer risk profile.

The danger is that the more rules based and prescriptive the regime becomes, the less likely we will be able to take a risk based approach in reality. It is also important to recognise that KYC is just one element of a successful anti-money laundering strategy.

While automated transaction monitoring systems are not a mandatory requirement at this stage, they will become more and more important going forward for firms of all sizes as we seek to ensure that our products and systems are not abused for money laundering purposes.

However, to put the overall impact of these systems in context, we would anticipate that the overwhelming majority of Suspicious Activity Reports (SARs) disclosed will still originate from our staff at the customer interface.

2. **How should firms pursue a risk-based approach to anti-money laundering ?**

The approach set out in section 2 of the paper is appropriate and provides a good summary. Understanding the risk profile of your customers, products, services and processes is critical. It is also important to have good dialogue with relevant Law Enforcement Agencies (LEAs) to enhance your understanding of the risks, and which products and services are more susceptible to money laundering activity and how criminals would typically use such products.

The approach also needs to be flexible as the risk profile of both customers and products will change during the course of their respective life cycles.

Sharing best practice and regular dialogue with other institutions would also be important, it is difficult to see how we as an industry can be successful without working very closely together. There will still however remain a need for flexibility to ensure that systems and processes that firms implement are tailored to their own risk profile and also to ensure that new learnings consistently emerge.

It is important that action is taken to provide institutions with the confidence that a risk based approach will not fall foul of the Proceeds of Crime Act 2002 (POCA) and in particular the “reasonable grounds” issue.

3. What type of monitoring (and reports) would be most useful to law enforcement agencies (LEAs)?

While primarily a question that would be best answered by the LEAs themselves, the critical things are timeliness and appropriateness. Clearly a high volume of poor quality submissions (defensive reporting) would be counter-productive and there is a need to provide greater clarity around the implications of POCA 2002 or this may become an inevitable outcome.

It is essential that the LEAs also work with and provide regular feedback to financial institutions on the quality and appropriateness of their disclosures and also on emerging typologies and risk areas, to in turn allow the institutions to pro-actively manage the risks and enhance detection and conversion rates.

4. What are, or may be, the costs and benefits of KYC and monitoring?

The key cost elements are highlighted within the Discussion Paper. There is no doubt that these are significant and it is important that we start to see a better outcome emerging (in terms of reduction in financial crime) for the investment and effort that is being put into these activities.

It is concerning that while the estimates of Money Laundering in the UK are from £25bn per annum upwards that relatively little is being recovered via The Asset Recovery Agency and few successful prosecutions are made. It serves to highlight just how difficult it is for such criminal activity to be identified.

To be successful then there needs to be a much more integrated approach including better access to some key verification databases eg, passport office, driving licence, national insurance etc. This would be further strengthened via the introduction of a robust National Identity Card scheme into the UK.

Perhaps we also need to be considering a much more focussed approach around targeting known and suspected criminals and terrorists. Clearly that would have major implications for all stakeholders and would require significant further discussion and consideration. The issues surrounding such an approach are quite far reaching however in terms of reducing financial crime all evidence suggest that this is a proven strategy.

It is critical that the Government, FSA, LEAs and the industry work together on this in a fully integrated manner if we are to make a real and genuine breakthrough in the fight against financial crime.

The benefits of KYC and monitoring are quite simply that it allows us to improve our understanding of our customers and in turn better manage our risks as well as providing revenue growth opportunities. Additional product sales can be achieved through clear identification of customer needs while on the other hand implementing effective processes for collecting KYC and monitoring accounts helps us to mitigate significantly our legal, regulatory and reputational risks.

It is fair to say that both the costs and the benefits are extremely difficult to calculate. However it is also fair to note that a risk based approach is not a soft option but could actually be a more costly methodology dependent on any institutions operating environment.

We need to be very cognisant that we do not simply add another layer of cost without taking some away, and this needs to be linked to a real focus on high value added activity.

5. Which options presented do you prefer and why?

After considerable discussion our view is that a derivative of Option 3 is preferable, i.e. "leave ML unchanged; rely on the JMLSG Guidance Notes". However we would caveat this to the extent that we believe the guidance notes need to provide greater clarity in certain areas.

In particular we would like to see the Customer Identification and address verification separated from the wider KYC. ID and address verification is pretty basic and we should be seeking to develop and publicise a core industry wide standard, while also at the same time increasing access to key databases mentioned above.

While the other aspects of KYC and Monitoring require the industry to work together there is a need for flexibility as potential competitive advantage can be gained as to how well these are integrated into each firm's overarching risk framework, sales processes and customer management systems.

At this stage there is too much fluidity in the market place with regard to both current and emerging regulation, and the pace of change which has seen new channels (non face to face), new monitoring and EID technologies emerge. It would be prudent to see how these develop before considering further rules and regulation.

In summary the focus needs to be on developing and enhancing a completely integrated approach across all stakeholders if the goal of reducing financial crime is to be achieved. This needs to be supported by a strong and continuous message from the FSA/ Government educating the public on the rationale and benefits of the anti-money laundering regime.

Nationwide

Our Ref: RJ/dj

28 January 2004

Legal Compliance (Consumer Affairs)
2nd Floor East
Kingsbridge Point
Princes Street
Swindon
SN38 1ND

Tel No. 01793 732656
Fax No. 01793 732279

Mr D Shonfeld
Financial Services Authority
Financial Crime Policy Unit
Prudential Standards Division
25 The North Colonnade
Canary Wharf
London
E14 5HS

Dear Daniel

FSA DISCUSSION PAPER 22

Nationwide welcomes the opportunity to respond to Discussion Paper 22.

1. GENERAL COMMENT

We recognise that we have a social and moral responsibility, as well as a regulatory duty, to deter and detect money laundering activity.

Financial firms such as Nationwide bring many positive benefits to individuals and the wider community by providing comprehensive services, good products and financial soundness that gives customers confidence that the decisions that they make today can be relied upon for the future. If firms were to adopt a lax approach to anti-money laundering, we believe that this would seriously undermine the provision of financial services within the United Kingdom. We have therefore approached our response to Discussion Paper 22 in the spirit of wishing to serve our customers' best interests, as well as meet our strict regulatory duty.

It seems to us that there are three elements in anti-money laundering that are important. Firstly, the identification of the customer. Secondly obtaining sufficient information about the customer at outset to determine what would constitute normal patterns of activity for that customer and thirdly, the monitoring of that customer's activity to determine if suspicious activity is occurring.

(a) Initial Identification

We recognise that this is a very important part of anti-money laundering. It is also, however, very problematic in that:

- An astute criminal will be able to obtain false documentation with little effort and at small cost.
- The bona fide customer may find it difficult to produce the appropriate identification.

You are aware that within Nationwide we plan to introduce an automated identification system throughout the Group during 2004. In approximately 85% of new customer enquiries, we envisage that there will be no need for paper identification at all. In the remaining 15% of cases, paper identification will be required and a note taken of this electronically during the account opening process.

Although ID is very important, within Nationwide we believe this is intrinsically the weakest part of any anti-money laundering programme. Virtually anyone, but especially criminals, can easily overcome the ID hurdle. Hence, our view is that Know Your Customer (KYC) as defined in Discussion Paper 22 and subsequent transaction monitoring are of paramount importance in an effective anti-money laundering regime.

(b) <u>Know Your Customer</u>

We agree that it is important to obtain as much information from the customer at outset that helps establish a picture of how the service or product being supplied is going to be used by that customer. However, it is only important to get this information **if you intend to use it**. In other words, the mere collection of such information is of no use whatsoever if you do not subsequently match the **actual transactions** against the **anticipated** pattern of activity.

(c) <u>Transactional Monitoring</u>

A significant proportion of many firms' businesses are on the basis of "non face-to-face" transactions. Indeed, in many cases the firm will never see the customer at all. The increasing use of internet banking, postal banking, telephone banking, cash withdrawal and cash deposit via ATMs are all meeting a customer need to be in control of their finances 24 hours a day, 7 days a week and every week of the year. In these circumstances, we fail to see how any firm involved in any of these activities could claim to have an effective anti-money laundering programme without having some form of transactional monitoring in place. Moreover, even in a face-to-face situation within, for example, a retail branch network, we recognise that staff will be unable (despite appropriate testing and training) to spot all suspicious transactions that they could because they only see part of the picture. It may be that a money launderer visits the branch on a number of occasions, but on each occasion would deal with a different member of staff, yet each transaction in itself would appear to be above board. A "bird's eye" view is needed and we believe the only way of achieving this is via transactional monitoring.

2. RESPONSES TO SPECIFIC QUESTIONS

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

It is important that comprehensive KYC is gained at the outset of the relationship as this will help to "benchmark" subsequent transactions.

We believe that there should be a consistent, industry standard within the United Kingdom in relation to KYC. This is because there may be a feeling amongst some financial firms that to introduce new requirements unilaterally will impose a heavier burden upon their prospective new customers than that same customer would have to bear should they go to a different provider. For example, while firms may currently be asking details of employment and income in relation to an account that is currently credit scored, perhaps the same questions with regard to employment and income ought to be asked for non-credit scored accounts, such as savings accounts. However, as it is not a regulatory requirement to do so, some firms may believe that it would be too intrusive to ask these additional questions when other firms are not asking them.

There is obviously a strong link to reporting, in that in determining whether an unusual transaction is in fact suspicious, it is beneficial to know as much about the customer as is possible.

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

In our "General Comments" we describe three fundamentals of a good anti-money laundering programme, namely ID, KYC and transactional monitoring.

Although some products might be regarded as more high risk than others, we believe there has to be recognition that most products are capable of being used for money laundering purposes. A monitoring system therefore ought to be in place to look at unusual transactions across all product types, such as current bank accounts, savings accounts, mortgages, personal loans, credit cards and unit-linked policies. For large firms with a Treasury function, monitoring should also take place.

Money launderers are sometimes very sophisticated people and will often try to launder money via a whole range of products. Transactional monitoring is therefore very important.

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

We believe it is up to law enforcement to inform us of their exact standards and requirements.

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

KYC Costs

Costs include:
- System changes to accommodate collection and updating of KYC.
- Staff training.
- Changes to application forms/brochure ware.
- Changes to business processes.
- Possible loss of new business (unless KYC requirements are prescribed and are consistent across the financial services industry).

KYC Benefits

- Better quality unusual transactions.
- Reduction in investigation time.
- Reduction in fraud.
- A better and more consistent customer experience.

Transaction Monitoring Costs

- Significant investment in technology development.
- Staff training in the use of new technology.
- System support and maintenance costs.

Transaction Monitoring Benefits

- Good quality unusual alerts.
- Able to keep track of all account activity, across all products and all distribution channels. This is of particular importance in relation to non face-to-face transactions, such as Internet banking, postal banking and the use of ATMs.
- Such systems maintain customer confidence that firms take their anti-money laundering responsibilities seriously.
- On a wider front, the use of such systems maintain overall market confidence.
- Once criminals are aware that firms are monitoring transactions in a vigilant manner, then they will find it harder to launder dirty money.
- Increased and better quality notifications to NCIS will result in more criminals being held accountable for their crimes.

Overall, Nationwide believes that we have a social and moral responsibility, as well as a legal responsibility in relation to deterring and detecting money laundering activity. While there is a cost to putting in place enhanced KYC and automated transaction monitoring, we believe this should be viewed as an investment, not a burden.

Q5: Which options presented do you prefer and why?

Nationwide prefers option 1, that is to include in the Handbook specific rules and/or guidance on KYC and/or monitoring.

The main reason for this is that money launderers take the line of "least resistance". If it is perceived that some firms are tougher with their anti-money laundering procedures than others, then criminals will gravitate towards the weakest link in the anti-money laundering chain. Hence, companies with "lighter" questions in terms of KYC and having no meaningful transactional monitoring in place, will attract more money launderers and other criminals.

I trust that our response will be of assistance to you. I have made the offer in the past, but again would like to say that if you would like to visit us in Swindon to see our own transactional monitoring system at work, then I will be pleased to facilitate this.

Yours sincerely

Russell Johnston
Head of Legal Compliance (Consumer Affairs)

DP22/FSA/DE
29 January 2004

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

Dear Mr Shonfeld

Discussion Paper 22: Reducing Money Laundering Risk

Thank you for the opportunity to provide comments on the paper. Comments and views from Northern Rock plc are as follows:

The FSA's Options

In relation to KYC and monitoring, the FSA's main options (not mutually exclusive) are as follows:

Option 1 – include in the Handbook specific rules and/or guidance on KYC and/or monitoring

Comments: It may be difficult to apply the same specific rules to every regulated firm. From October 2004 it is likely that the FSA will have an additional 30,000 firms to the 12,000 that are currently regulated. As stated in other parts of the paper, the collection and use of KYC and the approach to monitoring will vary between firms and products. Firms are encouraged to take a risk-based approach with KYC and monitoring. Existing rules within the handbook already commit firms to take a risk-based approach to managing risks and implementing appropriate systems of control.

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

Comments: High level rules could overcome some of the difficulties that specific rules could impose. However, as a regulated firm we are already subject to high-level obligations to take reasonable care to set up and maintain effective systems and controls for countering the risk of being used for a purpose connected with financial crime. Therefore, it is probably unnecessary to apply new high level rules.

Option 3 – leave ML unchanged; rely on the JMLSG guidance

Comments: The JMLSG Guidance Notes are a key driver for financial firms' compliance with the regulations and FSA rules. They provide guidance on the practical application of best industry practice for anti-money laundering policies, procedures and controls. The recent formation of the Money Laundering Advisory Committee (MLAC) and the recently extended membership of the JMLSG across a wider sector of the industry make this a preferred choice. All appropriate stakeholders provide input to the guidance notes: including Government, FSA, law enforcement, trade bodies, expert consultants and individual representatives. Although compliance with industry guidance does not necessarily mean compliance with the law or the FSA rules, it provides firms with the comfort that compliance with the guidance will be taken into account in any assessment for compliance with the law and FSA rules.

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

Comments. This is the preferred option in addition to option 3 because of a number of forthcoming initiatives that could have an impact on current rules or proposed rule changes:

- There are discussions already underway regarding a 3rd Money Laundering Directive.
- Some member states have not yet implemented the requirements of the 2nd Directive.
- The FATF has only recently published its updated 40 recommendations. It is considering other initiatives in relation to KYC and pro-active monitoring.
- HM Treasury is planning to publish an UK Anti-Money Laundering Strategy.

It may be worth monitoring the development of these initiatives and feeding into them. The position could then be reviewed at a later date as to whether rules should be changed.

<u>The FSA's Questions</u>

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

<u>KYC</u>

The collection of appropriate KYC is necessary for high-risk products such as business banking facilities and private banking facilities. The KYC information could be validated at the outset and also on an ongoing basis. It is likely that customers would see this as a normal requirement because of the nature of these products.

The value of KYC information for low risk products is difficult to assess for a number of reasons:

- There will probably be more adverse customer reaction if KYC information is collected for simple low risk products.
- The information would be of little value if it were not validated. Honest people would provide genuine information, whilst criminals could provide information that would be appropriate to how they would plan to use the account thereby avoiding raising suspicions. If the information were validated it would add to the costs of providing low risk products.
- The information may become out-of-date in relation to the operation of the account and therefore could result in many 'false positives'.
- As stated in the paper, many customers have products with different firms. It would be difficult to identify whether a customer's operation of a single account with one firm was unusual in relation to the KYC information when the operation of accounts in other firms would be unknown.
- The nature of the business that the customer normally expects to conduct on low risk products could be established but it would be difficult to be alert to transactions that are abnormal on individual accounts.

<u>Monitoring</u>

It is unlikely that a firm could discharge its current regulatory obligations without some form of automated monitoring. The number of bank accounts has increased and there is much more non face-to-face banking which has increased the risk that unusual activity could be left undetected. Staff vigilance alone could not identify all unusual activity, particularly for non face-to-face business.

Individual high-risk accounts could be 'flagged' so that each transaction could be scrutinised either at the time of processing or immediately afterwards. However, this may only be practicable depending on the number of accounts or products deemed high risk.

It would seem impracticable, particularly for low risk products, to ensure that transactions on every individual account are consistent with the firm's knowledge of the customer. With the growth in non face-to-face products firms are less likely to 'know their customers'. Automated monitoring systems would be required to identify unusual activity on accounts. These would then have to be reviewed to determine if there were any suspicions.

Automated monitoring systems would assist firms to comply with Proceeds of Crime Act (POCA). Although it would still not remove the ongoing requirement for staff to report where they ought to have had knowledge or suspicion, monitoring systems would identify unusual activity that ought to be reviewed as potentially suspicious.

It is known that some countries, for example Switzerland, have imposed a legal requirement for relevant firms to implement automated monitoring systems.

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

Offering firms the flexibility of taking a risk-based approach is helpful but there should also be basic benchmarks or minimum common standards of ‘must do’ or ‘don’t do’.

The FSA could agree with stakeholders a range of product types as being low risk or high risk. This would assist firms via their trade bodies to develop a ‘common’ risk-based approach particularly in relation to KYC and monitoring.

An alternative could be that FSA supervisor teams review a firm’s risk assessment of its products. Product types could be agreed as low or high risk. This would help firms make informed decisions about KYC and monitoring requirements for particular types of products.

For verification of identity it would be helpful if the requirements were consistent whether the business is face-to-face or non face-to-face. The identity requirements could be related to product type being deemed either high risk or low risk. As more firms move towards electronic verification products, it may be considered that the verification of individuals could be consistent no matter the product type.

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

Funds going to or from high-risk jurisdictions could be made compulsorily reportable. The list of such jurisdictions should be fluid so that it can be regularly revised. This would disrupt criminals and minimise the opportunity for them to change sending/receiving jurisdictions to avoid the reporting system.

Automated monitoring systems could be used to produce exception reports using rules based on money laundering typologies. Experience and expertise from law-enforcement agencies would also provide valuable guidance on rules that could be implemented. Currently, anecdotal evidence indicates that firms currently using these systems were developing the rules based on their own experience on money laundering and fraud.

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

The main costs of obtaining and storing additional KYC and implementing a monitoring system would probably relate to the development of a firm’s IT systems and additional storage capacity. For monitoring, the costs would also include either the purchase or development of a monitoring system. There would be additional staff costs associated with the reports from the monitoring system.

The benefits could include additional fraud reduction as a spin-off from additional KYC and monitoring. This may offset some of the costs of such systems. There would also be the benefit of more reports/intelligence to further detect and prosecute financial crime. Some of the major intangible benefits would be the reduction in the social and personal impact of crime and possibly the prevention of terrorist acts.

Q5. Which options presented do you prefer and why?

Options 3 and 4 are the preferred options. They allow the opportunity for revised industry guidance to work which has had input from all major stakeholders. They will also enable the UK to continue a lead in the fight against financial crime while not putting UK industry at a competitive disadvantage. More UK firms are looking to implement technology for verification of identity and ongoing monitoring.

These should be studied to see how effective they are before introducing further rules. Also as previously mentioned, there are a number of national and international initiatives that are currently being developed. These initiatives should be given time to be debated to see whether there is a requirement to amend the rules as a result of them rather than change the rules before the initiatives are developed and possibly implemented. Otherwise the rules may have to be changed again.

Please contact Derek Edgar, Senior Compliance Manager, if you need any further information or if you would like him to expand on any of the points noted above. He can be contacted directly on 0191 279 4601.

Yours sincerely

Austin Muscatelli
Operational Director (Group Legal & Compliance)

Patients’ Aid Association
Paycare House
George Street
Wolverhampton
WV2 4DX
Tel: 01902 371000

Discussion Paper 22 – Reducing money laundering risk

Introduction

Patients’ Aid Association is a not for profit organisation and a mutual provider of healthcare cash plans to approximately 60,000 policyholders. Our healthcare cash plans are low cost policies with premium rates ranging from as little as £0.75 per week. Benefits consist of cash payments, up to an annual limit, towards a range of medical expenses. Dental and optical treatments, complementary treatments and specialist consultations are just some of the benefits available. The average claim value is between £60 and £70, with most policyholders claiming once or twice a year.

Paycare, the healthcare cash plan underwritten by Patients’ Aid Association, is mainly sold through the workplace, although it is also available direct to individuals. Employers collect premium payments by payroll deduction, pay the premium themselves as part of the employees’ benefit package or operate a combination of the two. In the case of an employer-paid scheme, it is important to note that the Paycare plan is not sold as a group policy. The employer buys an individual policy for each employee.

Comments

Our comments are made in the light of our experiences as a provider of healthcare cash plans, and are therefore particularly relevant to simple, low-value (and consequently relatively low risk) financial products.

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

Collection of information and active monitoring are both necessary, but the amount and type should be relative to (a) relevance to the business, (b) degree of risk and (c) feasibility of/need for keeping the information up to date.

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

Firms should identify and assess the potential money laundering risks arising from their particular business and introduce measures to mitigate the material risks. They should assess the risk at the beginning of the relationship with a customer, and then monitor key factors during the course of the relationship, giving particular attention to exceptional and/or unusual or suspicious transactions or occurrences.

Patients' Aid Association
Paycare House
George Street
Wolverhampton
WV2 4DX
Tel: 01902 371000

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

Monitoring of the value, volume and nature of transactions to identify those that the firm itself considers to be unusual or suspicious for that particular customer or type of business. Reporting to agencies after internal review and investigation by the firm, which is probably best placed to identify what is truly suspicious rather than just out of the ordinary.

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

There may well be increased costs of data collection, storage, maintenance and monitoring, especially where there is a need for automated systems.

The benefits should be a limitation of opportunities for crime in the market as a whole, and reduction of the risk of loss (financial, legal or reputation) for individual firms, as well as increased confidence in the UK financial services market.

As stated in the paper, the wider benefits depend significantly upon SAR's making a marked contribution in practice to the fight against crime and terrorism.

Q5 **Which options presented do you prefer and why?**

Option 2 – high level rather than specific rules and/or guidance would give a clear indication of the importance of money laundering as an issue, but would leave firms with the ability to make their own judgments as to the best way to achieve compliance within their particular business.

In view of the diversity and complexity of the financial services sector as a whole, we cannot see how it would be possible to introduce too many specific rules, as we do not believe it is possible to achieve "one size fits all" rules in relation to money laundering.

From: Risk Values: Nigelmc
Sent: 13 February 2004 11:27
To: DP22
Subject: KYC in difficult environments

Dear Mr Shonfield

I am aware that the period for comment on DP22 has closed. However, I would like to make reference to one specific issue: that of KYC at the beginning of a relationship, and in its early stages, before a transaction pattern has been created and would be grateful if you would consider this note.

It is established that the early days, weeks and months of an account are high risk because at that time the only financial data available is that which has been provided by the applicant, and which may or may not have had rigorous verification.

We know that in many businesses, notwithstanding both Rules and accepted good practice, that verification tends to focus on the identity of the person rather than on his finances. This is especially so in organisations of limited resources or where the business is likely to be short term and, in absolute terms, generate relatively small profit. Simply, the cost of extensive verification is expected to greatly erode and perhaps even exceed the profit to be made from some business activities affected by the Money Laundering Regulations 2003, a significant proportion of which are regulated by the FSA.

The danger of focussing on the financial information provided by the applicant for business is that in the case of a money launderer, it is likely that at least a part of that is fictitious yet verification will have been anticipated and provided for. The result is that the verification is also fictional.

Further, for FSA regulated businesses operating in overseas markets where there is very limited information as to the applicant for business - especially true in developing markets such as Africa. Identification is difficult and in many cases there is no verifiable financial history.

A further issue that exercises my mind is that criteria setting may, and we know from experience has in a number of cases, result in either deliberate or inadvertent prejudice. This is especially so in the case of postcode profiling, for example.

Shortly after 11 September 2001, I began to think about this problem from a completely different angle. I wondered if we could find some way of avoiding the difficulties of both potentially or inherently prejudicial criteria and pay less, not more, attention to the financial history at the commencement of the relationship.

By turning the established theories on their head, I realised that we were, to a degree, missing the point.

The fundamental question that we were failing to ask was "does this person indicate a propensity to commit a financial crime using the service he is applying for?"

Having identified this issue, I approached researchers in consumer attitudes. Pat Dade has more than 30 years experience in analysing consumer attitudes. His co-analyst Les Higgins has been involved in similar work for many years, too. They have a massive amount of background data against which they apply principles developed by leading psycohologists over a period of some 50 years, and refined by Dade and Higgins.

Over the past fifteen years or so, they have undertaken a number of projects for financial institutions aimed at identifying the type of people that are likely to purchase particular financial products. This has led to far more accurate marketing than the previous method of looking to see which customers have certain spending or saving patterns.

We examined the characteristics of financial criminals against both the established psychology and background data. And we found that there are characteristics that can be identified with a very simple questionnaire: and importantly, the questionnaire is very much the sort of "lifestyle" questionnaire that people are used to filling in when they apply for a wide range of financial services.

Each response is analysed against data that is hundreds of thousands of responses collected in many countries over an extended period. This same background data is used ultra-reliably to predict consumer attitudes to, amongst other things, the sale of financial products. We are therefore certain that the data is valid.

The resulting product is Risk Values. It is a short,simple point of sale (or subsequently by embedding in customer surveys) questionnaire that assesses the applicant's propensity to commit financial crime against or using the institution.

The responses are divided into five categories. 1 is unlikely to commit financial crime, 5 is one of approximately 0.44% of the population who are very likely to commit such an offence.

We say that Risk Values should not be used as a reason to accept or decline a customer but that it is a guide as to how closely that account should be monitored.

We developed Risk Values to be affordable in the developing world, and therefore it is a tiny program, it will run on even a 486pc with 8Mb Ram and it fits on a floppy disk.

We have been very open about the development of Risk Values and details of its development and the basis upon which it works are set out on the Risk Values website at www.riskvalues.com

Given that there is at least a tacit suggestion in the Joint Money Laundering Steering Group Guidance Notes (current issue) that it is permissible to open and run an account pending verification (a view with which I am directly opposed), Risk Values can provide a valuable and effective means of ensuring that accounts that require it are monitored most closely whilst those that are very low risk may be subject to a lesser monitoring.

For businesses for which transaction monitoring software is unaffordable, and for those for which it is unsuitable as well as for those who have it but there is not yet sufficient financial data to assess the customer's pattern of transactions, Risk Values can be a very valualbe addition to the business's armoury.

Regards

Nigel Morris-Cotterill
Risk Values Limited
Part of The Anti Money Laundering Network. www.antimoneylaundering.net 0207 107 9512 (London)
+6 03 2412 7588 (Malaysia)
+6 019 394 9310 (Malaysia Handphone)

===========================

.

Royal Sun Alliance

Response to Discussion Paper 22

Reducing money laundering risk - Know Your Customer and anti-money laundering monitoring

Question		Response
1	How necessary is the collection of KYC information and an active approach to monitoring in reducing money laundering risk and in meeting legal and regulatory obligations, in particular reporting?	We agree that the collection of appropriate identification evidence is vital to reduce the risk that a firm transacts business with a money launderer. While we set out below a couple of specific cases where stricter identification requirements than those which currently apply might be justifiable, we stress that an additional burden should only ever be imposed after a meticulous comparison of the cost of doing so against the risks of not. For us as an insurer, the risks are less than those facing the banks and the risks for general insurance business lower than for life and pensions. However, there are areas within the insurance sector where the risks are such that KYC might be appropriate. For example, additional KYC information could be required for large premium investment products, particularly those which have the greater degree of flexibility characteristic of bank accounts - for example, those which may be capable of: ∉ receiving frequent and sizeable additional premiums; ∉ providing regular investment income; ∉ providing regular withdrawals;

		∉ partial surrender; and ∉ regular switching between funds and access across products. Investment bonds can have these features and may be further susceptible to laundering as they are likely to be subject to cancellation rights. Compared to these, general insurance products present much lower risk and will often involve relatively low premiums. Turning from a specific product to a generic customer perspective, additional KYC information could also be obtained for existing customers with known connections with countries who do not co-operate with the internationally agreed money laundering guidelines. Prospective customers could similarly be vetted for such connections on application. This will be more relevant for global commercial lines operations than for UK private retail customers. However, given that transactions involving certain countries on the Financial Action Task Force NCCT list should be presumed (in the absence of persuasive evidence to the contrary) to involve laundering, FSA could in our view reasonably introduce a specific requirement that all regulated business be checked for connections with those countries, rather than leave this to individual firms' risk assessments. FATF and HM Treasury have clearly already assessed the risk as particularly high, so it seems inconsistent to allow firms the opportunity to reach a different view (unless of course they can demonstrate that they do not and will not have customers with those territorial connections). Whilst FSA is correct in saying that some of the KYC information referred to at paragraph 3.7 of DP22 may already be collected as part of a firm's normal processes (underwriting, claims and marketing in the insurance context), it should not use this per se as a cost justification for introducing prescriptive KYC requirements.

		It must bear in mind that this data is used for assessing commercial rather than laundering risk and that significant and potentially disproportionate costs may be entailed in extracting it and converting it into useful management information for KYC purposes. In our view, existing commercial procedures and controls in the insurance sector when coupled with the current regulatory requirements should generally be sufficient for “out-of-character” transactions or events to be identified as they occur and for internal suspicion reports to be made and escalated to NCIS accordingly. Underwriting checks go some way towards preventing the risk arising in the first place and fraud controls correspondingly reduce it at claims stage. Regular monitoring of these procedures and controls to assess whether they are being properly applied in practice should of course be fundamental to any anti-money laundering compliance plan.
2	How should firms pursue a risk-based approach to anti-money laundering?	As set out in paragraph 2.9 of DP22. For an insurer, by ∉ **identification and assessment** of the risks posed by: ∉ the classes of business the firm conducts; ∉ the specific types of product it offers; ∉ the distribution lines it uses; ∉ the customer types it deals with; ∉ its individual customers through the use of client-specific KYC details at each transactional stage – whether the underwriting of new business;

ROYAL & SUNALLIANCE

		the processing of ongoing transactions during the life of a product (eg increments, switches, income payments, withdrawals and part surrenders); or paying claims leading to the termination of the contract (including the exercise of cancellation rights, pro rata premium refunds, full surrenders, death and maturity). ∉ **mitigation** of the risks identified through: ∉ compliance with the statutory and regulatory controls (eg for identification; internal and external reporting; training and awareness; use of international findings) which are imposed on it for that very purpose; ∉ the consistent implementation and application of underwriting, claims and risk control best practices; ∉ the effective provision of guidance in the form of training materials and in answer to ad hoc technical queries. ∉ **monitoring, reviewing, updating** as necessary and **documenting** the systems and procedures established as a result of the risk assessment and mitigation process set out above. The support, commitment and close involvement of **approved persons** and **senior management** are essential to the success of such an approach: ensuring that they are made fully and explicitly aware of their personal responsibilities and presenting them with high quality management information are vital ingredients in this regard.
3	What type of monitoring (and reports) would be most useful to law enforcement agencies?	The agencies themselves should be in the best position to answer this question but in our view it has to be risk-based as it is the quality of monitoring and reporting, not the quantity, that should count.

		There is a real danger in the current cautious climate that firms' monitoring will not be sufficiently risk-focused. As a result, enforcement agencies could become so overwhelmed with reports that they will not be able to see the wood for the trees and will be unable to perform their functions efficiently or effectively. Automated monitoring systems have their place, particularly for banks and firms dealing with high-volume transactions but they should be there to assist firms in making the qualitative judgement required in deciding whether to refer matters on to NCIS – and not act as a substitute for that judgement. We therefore think that it is crucial that NCIS and the other agencies provide feedback to firms, their trade bodies and the FSA as to what they want to see and the form in which they get it. This feedback could subsequently be incorporated as guidance in the JMLSG Guidance Notes.
4	What are, or may be, the costs and benefits of KYC and monitoring?	Please see our comments on costs in response to other questions. The benefits depend on the level of risk prevented as a result of the measures. Where there is low risk, as, for example, with a life operation closed to new business, additional requirements may accordingly be disproportionately costly. So if FSA is considering bolstering the requirements, it should be careful not to adopt a one-size-fits-all approach but tailor any new provisions according to the risks which different types of firm and different types of business may pose to its financial crime statutory objective. Its cost-benefit analysis must therefore be comprehensive and stand up to close scrutiny. We are aware that the ABI has been conducting its own research into money laundering risk by product category and this might be something which FSA could usefully take into account in its own deliberations.

5	Which options presented do you prefer and why?	None of the options as described in the paper appears unacceptable to us. It is clear that, even under Option 1, FSA still very much has in mind a risk-based approach which we welcome. And while there may be scope for some specific new requirements to cover particular issues (as mentioned elsewhere in our response), we feel that it is unnecessary to introduce general KYC and monitoring rules to the effect proposed across the board. Similarly, we consider that there are sufficient existing high-level provisions in SYSC, ML and IPRU for Option 2 also to be unnecessary. Option 3 is attractive in that it directs firms to where the most practical and detailed industry guidance can be found. Indeed, it seems to us that there is a case for incorporation of the JMLSG guidance into FSA's Sourcebook (in the same way as the Guidance Notes incorporate the Sourcebook as an appendix) but perhaps this is not permitted under FSMA 2000 or the mechanics are so complicated as to preclude it. Our point is that there are several different sources of legislation and regulation in this area and it would be ideal for it to be consolidated in one work of reference. Any move towards that objective and to reducing duplication and the scope for conflict and inconsistency between the different sets of provisions would be welcomed. There seems little benefit, for example, in FSA's translation of the requirements of the Money Laundering Regulations into its own Sourcebook. Quite apart from the danger that something will be lost in that translation or given a different meaning, it seems an unnecessary duplication, given that the Regulations apply come what may – a simple cross-reference or verbatim replication would in our view have been better.

		However, on balance, we favour Option 4 in order to allow FSA the opportunity to give proper and detailed consideration to: ∉ the effects of the recent legislation in this area (the Proceeds of Crime Act 2002 and Money Laundering Regulations 2003 in particular), given that the full ramifications (for example, extensive fraud reporting to NCIS) are only just beginning to sink in; ∉ the industry's risk assessment initiative currently being conducted through the ABI; ∉ its own further experience of monitoring its membership in their different risk and business categories; ∉ the preferences of the law enforcement agencies; ∉ any restructuring of NCIS following the KPMG report; and ∉ the development of monitoring tools, perhaps tailored to the needs of individual firms. In our view, it is only in the light of such factors that FSA can prepare the robust and comprehensive cost-benefit analysis which is the pre-requisite to effective regulation. We feel that, at present, the state of flux in this area is not conducive to the production of a cost-benefit analysis which would bear scrutiny – or at least which would be likely to bear scrutiny for anything but the short-term.

Schroder Investment Management Limited
31 Gresham Street, London EC2V 7QA

Tel: 020 7658 6000   Fax: 020 7658 6965
www.schroders.com

Schroders 2004
200 years of forward thinking

28 January 2004

Mr D Shonfield
Financial Crime and Policy Unit
Prudential Standards Division
Financial Services Authority
25 The North Colonnade
Canary Wharf
London

E14 5HS

Dear Mr Shonfield,

Discussion Paper 22: Reducing Money Laundering Risk
Know your customer and anti-money laundering monitoring

Thank you for giving us the opportunity to comment on this Discussion Paper. Schroders is a global independent asset management group, managing investments of £95.5 billion (as at 31/10/03). Our clients are institutions, corporations, intermediaries and private investors around the globe.

This response serves to reply on behalf of our institutional, retail and private banking divisions, all of which have different risk profiles, and therefore different requirements, in respect of KYC and monitoring. We have covered the issues faced by all three sectors in our answers to the detailed questions set by the FSA which we duly attach.

Overall, Schroders have come to the conclusion that we would recommend the FSA does nothing at this stage and review the situation again at a later stage. Our reasons for this decision are detailed in the attached.

We hope that our comments and suggestions are useful in helping the FSA reach a decision on this matter and we would be happy to discuss further any of the issues we have raised in our response.

Yours sincerely

Vicky Wand (Mrs.)
Compliance Manager

Discussion Paper 22: Response to Questions

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

It has become apparent that the verification of a client's identity may not be the most effective way to manage the risk of money laundering within a firm. Whilst it is appreciated that this is a vital part of the audit trail for law enforcement, and firms must be able to support the process by providing documentary evidence on request, further consideration needs to be given by firms on how money laundering can be identified.

A certain amount of monitoring is required to fulfil both legal and regulatory obligations. However, the level and methodology of transaction monitoring should be left for firms to decide depending on what is proportionate to their risks.

In the event that transaction monitoring and/or additional KYC is necessary, there is a likelihood that this will pose a number of practical issues for firms which need thorough consideration by all stakeholders.

- Customers may feel that the provision of additional KYC information is intrusive. Firms are still finding difficulty, on occasions, in obtaining basic documentation to evidence identity. It must be appreciated that obtaining additional information may be a lengthy process, especially in relation to existing clients and this would have to be borne in mind when setting a transitional period in the event that extra responsibilities are introduced.

- A certain amount of education will be required to make customers aware of the reason and purpose for requesting additional KYC information. This is not only an issue at the client take-on stage but also during the ongoing business relationship where existing clients are more likely to raise objections to requests for updated information. Whilst firms will play an important part in this process, we would also hope that the FSA and NCIS will continue the valuable role already initiated in the area of consumer education.

- In the event that firms are required to collect additional KYC information, minimum standards should be considered in order to ensure a level playing field both here in the UK and internationally. Guidance will be needed on the type of information to be requested, the level and depth that needs to be validated and the timing of updates. We would look to the Joint Money Laundering Steering Group to provide some industry sectoral guidance in this respect. Without a level playing field businesses with more robust requirements will find themselves at a competitive disadvantage. It is also a concern that firms who have a different perception of the risks, and apply a lighter touch, run the risk of being disciplined or prosecuted if their subjective views are not in parallel with the FSA or the Courts.

- Introduced business, or placing reliance on third parties, poses a number of problems. Regulated firms acting as Agents who retain the KYC information on the underlying investors must be made accountable to complete the KYC checks and reliance would have to be placed on them to monitor transactions. Introducers would need a thorough understanding of each firm's requirements in order that all parties can fulfil their obligations.

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

Firms need to consider the types of products and services they offer and the nature of their client base in order to decide on the type of monitoring considered appropriate. Depending on the outcome of this, further consideration will need to be given as to the level of KYC information necessary to support the process.

- For institutional investment management activity the risk of money laundering is perceived to be low. Thorough due diligence is obtained on each client as a matter of course in order to help a firm make investment decisions. Account Managers have a high level of oversight in respect of the client's activities. Monitoring on a case-by-case basis by the Account Managers is considered to be both effective and appropriate for these types of relationships.

- Collective Investment Schemes are also perceived as low risk in view of the legal restrictions and additional controls to prevent payments to or from a third party. However, it is recognised that a firm is likely to have obtained a minimal amount of KYC information, particularly for execution only business, and the increased number of transactions indicate less oversight in respect of each activity. A certain amount of monitoring may be necessary, by way of exception reporting, in order to detect unusual activity or incidents where criminal funds have been broken down into smaller amounts and dispersed throughout a firm. Additional KYC would not be necessary as the monitoring could be product based (ie, highlights activity which is out of keeping with the normal use of a particular type of product) rather than client focused (which highlights activity not expected by the known profile of a specific client). This type of 'smart monitoring' will not result in a disproportionate level of expensive software being purchased to meet the needs. The obligation on staff to identify and report suspicious activity will continue and the exception reporting will act to enhance the current system and must not undermine or de-value the important role played by members of staff.

- A private banking relationship might be seen as higher risk in view of the higher amounts involved, the types of investment vehicles and the possibility of cross-border activity. This type of relationship also benefits from close oversight by the Account Managers but may also benefit from some exception reporting to monitor transaction flows. The amount of KYC information to be obtained to support this process will also depend on whether the monitoring is product based or client focused.

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

It is hoped that this question will also be posed to NCIS and law enforcement for their views. Certainly money laundering prevention needs to be more intelligence led. Firms can only do so much to second-guess how to prevent and detect money laundering. Law enforcement are much better placed to provide the industry with the information needed to assist firms in making well targeted risk based decisions.

Law enforcement should be accountable for identifying and communicating the way in which criminals are laundering money in the UK. This information will help firms to adapt and re-define their systems and controls to mitigate the risks. A certain amount of prediction will be required in order for firms to try and stay one-step-ahead of the criminal. Whilst the NCIS UK Threat Assessment Report is an interesting document, it is too high level and does not serve to highlight the trends and threats faced by financial institutions. The recent NCIS Current Intelligence Assessment issued on 5th December 2003 was a superb example of what the industry needs on a regular basis.

It is appreciated that NCIS want to receive good quality suspicious activity reports. However, without feedback and guidance from those in a position of knowledge, it is difficult to assess the quality or usefulness of the reports being made. It would be valuable if NCIS appointed Relationship Managers who have industry knowledge and a law enforcement background to be a contact point for each financial sector. These Relationship Managers could provide feedback, guidance, advice, support and, possibly, training (at MLRO level). It is appreciated that extra resource may be needed at NCIS to fund this but the outcome would serve to create a better relationship between the industry and NCIS and it is felt that savings could be made by reducing the number of poor quality reports received and processed.

We appreciate that this may be beyond the FSA's remit, but the quality of reporting could be strengthened by a review of the Data Protection Act which currently results in a lack of transparency between financial institutions. Firms could improve the quality of reporting if authorised individuals within the regulated sector were able to discuss an unusual transaction with another regulated entity providing or receiving the funds. Clearly there are tipping-off issues that must be considered but, with appropriate controls in place, the reporting process would benefit if firms were to allow a certain amount of information sharing for the prevention or detection of crime. Whilst there is already an exemption under the Data Protection Act for this specific purpose, we understand that many firms will only respond to a request for information if contacted by a law enforcement officer. We would welcome a controlled extension of this exemption to the private sector to promote a better flow of information in respect of mutual customers.

NCIS are already under strain from the number of reports being submitted and there is no doubt that the introduction of additional transaction monitoring requirements would result in increased reporting. There is also a likelihood of an increased level of defensive reporting due to concerns about the objective test under the Proceeds of Crime Act. It would be disappointing if this legislation results in the prosecution of MLRO's that have acted in good faith, and with best intentions, when making a decision not to make a report to NCIS. It may take some time for MLROs to gain confidence in the judicial system and the industry is anxiously awaiting the Courts' interpretation.

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

The financial cost will depend on the type of transaction monitoring to be adopted by a firm. It is anticipated that basic exception reporting, without the need to purchase and implement sophisticated software, will not be expensive to develop and any costs will relate to staff training and the time taken to assess the output. For our Private Banking sector this is currently 3 man days per month.

Further resource and cost will be incurred in the event that additional KYC is required. The costs for this will relate to obtaining the information, managing the customer relationship, storage of information/documentation and staff training.

We recognise that there is a positive side to the costs involved, if measured more laterally, in the increased confidence firms would have in the financial system overall.

It may be beneficial to offer firms a financial incentive to help them meet their obligations. Perhaps by way of a percentage of criminal assets confiscated as a direct result of an SAR. Alternatively, HM Treasury could consider some tax incentives to firms who purchase expensive transaction monitoring systems.

Q5 which options presented do you prefer and why?

Schroders would recommend to the FSA that they elect Option 4: to make no settled decision now and review the position again at a later stage. Our reasons to support this decision are detailed below.

- Firms need a better understanding of the 'Risk Based Approach'. We are aware that this will feature in the JMLSG GN2004 where a separate chapter has been dedicated to provide guidance on this. Firms need time to implement any additional controls as a result of this further guidance.

- The introduction of the Proceeds of Crime Act and impact of the Money Laundering Regulations 2003 will result in an increase in the number of SARs made to NCIS. This comes at a time when NCIS are already under strain and restructure. NCIS needs to implement the recommendations of the KPMG report followed by a period of stability. They will then be better placed to handle the likely increase in reporting as a result of transaction monitoring.

- Investment Management firms would benefit from intelligence led feedback and typologies which are less banking focused. The recent Criminal Intelligence Assessment issued by NCIS was welcomed by the industry and additional reports such as these will help firms to adapt systems and controls to react to the risks of money laundering - thereby achieving maximum benefits and results.

Whilst a period of two years has been suggested before another review takes place, we would suggest that the matter be reviewed at a time when it is apparent that the system has stabilised and all stakeholders are better placed to meet their obligations.

Much has been done by the industry over the past ten years and the time has come now for a more joined up approach involving all stakeholders.

- NCIS and law enforcement need to provide better intelligence data to assist the industry in making risk based decisions.

- The industry needs to pool resources, become more transparent and learn from each others mistakes as well as adopt common good practices. In order to achieve this we need to keep regular dialogue via our trade associations.

- UK government and the FSA could help by working to improve the level playing field, both domestically and internationally. The future of FATF appears to be in some doubt and a more consistent system of reviewing the regime in all countries would be welcomed.

- Members of the public also have a part to play and need to be further educated and made aware of the obligations on firms.

We propose that all stakeholders might benefit from additional time to allow a period of reflection and stability with future consideration being given to maximising efficient, proportionate and effective controls.

SCOTTISH WIDOWS

Scottish Widows plc
PO Box 17036
69 Morrison Street
Edinburgh EH3 8YF
www.scottishwidows.co.uk

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

26 January 2004
☎ 0131-655-3838

Our ref: comp/ log510 /2004

Dear Mr Shonfeld

Re: Discussion Paper 22 -Reducing money laundering risk

We have detailed below our comments in response to the specific questions raised in the Paper. We would appreciate if you did not name Scottish Widows when quoting the monetary amounts disclosed in this letter.

Whilst we recognise the responsibilities that insurance firms have in regard to fighting financial crime, and that KYC and monitoring are integral parts in achieving this goal, it is critical that the FSA in conjunction with individual sectors of the industry reach agreement as to the activities which will satisfy the requirement to have appropriate KYC and monitoring systems and controls in place. This consensus understanding of what's required, appropriately tailored for different sectors of the financial services industry, will assist in allowing a level playing field to prevail with regard to firms anti money laundering operational activities and costs.

A further point which should be considered in the debate is the KYC available to an insurance or investment firms may be minimal, where the original sale has been arranged by a financial intermediary. The lack of KYC may make it difficult for firms to assess the money laundering risk of individual transactions at the outset of a relationship or thereafter compared with an assessment that the introducing intermediary could undertake. As a consequence, the debate should consider the responsibilities and sharing of information between intermediaries, product providers and investment firms.

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

KYC information will assist firms reduce their risk of dealing with a money launderer. However, there are a number of practical considerations to be taken into account:-

a) method of acquisition of KYC where business is introduced by an intermediary
b) costs associated with collecting and inputting additional KYC into systems and databases

We envisage that to ensure adequate KYC is collected an undertaking will be required across the industry as to the minimum level of KYC to be collected at the commencement of any relationship and thereafter. Also, the agreement will have to reflect the apportionment of responsibilities over the collection of the KYC between intermediaries and product providers. Furthermore there will be particular circumstances where potentially higher level KYC requirements might apply such as customers who are transacting business from NCCT jurisdictions.

The key issue for KYC is in our view that provider firms adopt the same standards and therefore the intermediary and customer experience is similar within respective sectors of the industry. As to the specific KYC details some of the information would be common to all transactions other information may be required utilising a risk based approach reflecting product type and levels of investment.

Clearly monitoring is vitally important in demonstrating that a firm is meeting its regulatory obligation to fight financial crime. As a product provider we would be seeking to continue with the development of a monitoring program which reflects an event driven risk based approach. This would result in our focus on early cancellations, large investments or encashments, and would be on an exception basis rather than an approach which was fully automated or based on patterns of behaviour. We do not envisage being able to monitor by patterns of behaviour for a single customer since within the insurance sector, individual customers rarely deal with firms on as frequent a basis as may occur within the banking sector.

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

Our view is that individual firms should be allowed the flexibility to adopt an approach which takes account of their products, distribution channels, customers and geographical location. However, in developing their own approach a firm would be expected to take notice of available analysis and guidance provided be bodies appropriate to their sector of the industry. For life and pension providers we would be looking to the ABI and JMLSG for guidance, based on discussion with law enforcement agencies, independent specialists and the FSA, on what might constitute an appropriate approach.

The above view reflects our overall theme of encouraging a level playing field approach to the activities of similar firms within each sector.

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

We have not provided detailed comments in response to this question, as we believe that the relevant Agencies will be responding.

We would however expect the Agencies to recognise that not all firms will hold the same level of information on a customer and their activities due to the nature of the firms relationship with the customer. As an example a product provider will not be in possession of detailed KYC information where the customer has been introduced to the firm by an intermediary. As a consequence the development of mandatory information as part of the reporting activity would be required to consider the respective roles of the intermediary and product provider within the life insurance, pensions and investment sectors.

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

The benefits in simplistic terms appear to fall into two categories

a) greater likelihood of SARs leading to the identification of money laundering activity by individuals and
b) opportunities for firms to use the KYC and monitoring to either market their products and services more effectively, with also the potential for the development of preventative measures for the detection of internal and external fraud.

Clearly the costs will be dependent upon requirements and the specific approach and processes undertaken by firms within each sector. At this stage the costs can only be estimated. Based on our experience figures of upwards of £6M could be envisaged for those firms with legacy systems which require to be taken into account.

In 2003 alone our firm has spent £1M in IT development for initial AML monitoring, further spending and development in 2004 is also envisaged. These figures do not reflect the associated training costs and staff resource required to implement and operate the monitoring program.

If firms are to be expected to sanction costs of this magnitude in developing their KYC and monitoring programs the FSA need to present a compelling argument to sectors of the industry such as life and pensions, which view themselves as low risk as ultimately it is consumers and shareholders who will pay the costs.

Q5 Which options do you prefer and why?

Option 4 is our preferred option. The reasons for arriving at this conclusion are:-

a) that a two year window will provide the industry, law enforcement agencies and the FSA with an opportunity to arrive at a consensus understanding of the most appropriate risk management and monitoring techniques for each sector e.g. banking life insurance, pensions.
b) as a consequence of a) allows time for the issue of appropriate guidance by the FSA in conjunction with the JMLSG, which would require firms within specific sectors to carry out activities to broadly similar standards and provide potential for co-operation between firms within the sector (such as intermediary and product providers).
c) time for the development of suitable software tools and techniques by in-house or external providers tailored to the guidance in b).

d) the industry having been subject to major change in recent years and at present (Prudential Source Book, BASEL, PPFM , Sandler Proposals and Depolarisation) with associated costs, any proposal for further change and costs will be unwelcome unless introduced alongside a clear set of requirements leading to a level playing field for all firms.

e) the success of operating an effective risk based approach will for many firms be dependent on its staff. Firms will have to invest significant amounts of time into a continuing program of staff development and awareness. This investment would be most cost effective once the industry had debated and reached a common platform of understanding on the level of KYC required and best practices for monitoring of customers within the specific sectors of the industry.

Please do not hesitate to contact us if you should require further information, or clarification on any of the responses provided.

Yours sincerely,

Elizabeth McHugh
Head of Life Company Technical

Scottish Widows plc, Company No. 199549. Registered Office in the United Kingdom at 69 Morrison Street, Edinburgh, EH3 8YF. Tel: 0131 655 6000.

Search Space

Response to DP22

Financial Services Authority

Reducing money laundering risk; Know your Customer and anti-money laundering monitoring

Questions	Response
How necessary is the collection of KYC information and an active approach to monitoring in reducing money laundering risk and in meeting legal and regulatory obligations, in particular reporting?	<u>KYC Information Collection</u> We consider the collection of KYC information an important part of an anti-money laundering program. In particular, it offers two key control assessments for evaluating the risk associated with any customer and their transactions: ∉ In the first instance the process of collecting KYC information should involve the verification of relevant identification provided by the customer, thus documenting the customer and their personal details and providing an audit trail supporting the integrity of this process. ∉ Secondly, the collection of information relating to the customer's personal situation and potentially their likely use of financial services products offered to them, provides a means for subsequently considering this information when monitoring that customer's activity. This represents a risk-based approach to anti-money laundering, with KYC information being useful in both determining if the customer is undertaking the types and styles of business that they indicated they would, and the ability to adjust the relative sensitivity, and hence risk-consideration, of any automated anti-money laundering monitoring system to take into account the KYC information provided (or potentially not provided) by any given customer. While the collection of KYC information is a valuable step toward providing an understanding of the customer, their origin and the likely range of behaviours they may exhibit, we feel strongly that it can only provide comprehensive protection against money laundering and terrorist financing when combined with the other aspects of an effective anti-money laundering program of which we believe an integral component is an active approach to monitoring all customer activity.

Active Monitoring

There are several factors that support the need for active monitoring:

- Issues with KYC information collection and usage in isolation
- The need for timely issue identification set against the sheer volumes of business conducted in the world's financial services industry
- The dynamic nature of the methods employed to launder money and finance terrorism
- The ability of any given firm to implement a cost effective risk based approach to anti-money laundering

Issues with KYC information collection and usage in isolation

A critical weakness of relying solely upon KYC information collection is that the information is provided at a point in time, and that given the right resources, the documentation used to demonstrate key aspects of KYC information can be either be forged or otherwise appropriated. Those that seek to launder money and/or finance terrorism have substantial resources available to them and one should expect that key control points in an anti-money laundering program will be breached and plan continuously for this likelihood.

The 'point in time' issue is also important when considering anti-money laundering. An account may be set up with only some future intent to use it illegally. Moreover, an account may be set up for entirely legitimate purposes and only be 'taken over' for the purposes of money laundering or terrorist financing at a later stage. In both cases, KYC information collected at the point of account opening does little to indicate the then current risk profile of the account, in fact it may provide contrary information relative to the risk represented by the account and thus be counter-productive if used in isolation to determine the risk of money laundering.

When implemented correctly, active monitoring programs, typically utilizing sophisticated transaction monitoring software provide a means for assessing customer activity based upon the behaviour that they actually exhibit, rather than that which they told you to expect or which you might expect based upon the KYC Information provided.

The need for timely issue identification set against the sheer volumes of business conducted in the world's financial services industry

	The timeliness with which potential money laundering and/or terrorist financing are detected and ultimately reported is clearly an important parameter in determining how effective any anti-money laundering program will be in addressing the core objective of the legislation and associated regulation – to reduce money laundering and terrorism by aggressively prosecuting those that knowingly handle the funds or do not execute their obligations with sufficient levels of diligence. Given the sheer volumes of information flowing through the financial services community, active monitoring provides the only way in which potentially egregious behaviour can be quickly identified, investigated and if necessary reported. With many financial services firms routinely dealing with tens of thousands of transactions, and the largest dealing with tens of millions on a daily basis, software tools are critical to interpreting behaviour and identifying potential money laundering violations. It is possible to apply software tools in a 'reactive' manner – allowing humans to use database review software such as queries and visualisation to look for patterns of interest. While such approaches may identify patterns of interest, we find that both the timeliness of identification and the completeness of the review can be seriously compromised. This is because the volumes of information are so great, that even with sophisticated tools, people have to decide which pockets of transactional data they are going to examine and when they are going to do so. This greatly increases the likelihood that money laundering activity is not identified and even when it is it is not done so in a timely manner. To examine <u>all</u> transactions reactively via a human driven process in a timely manner would require so many analysts as to create excessive burden for all but the very smallest financial services firms. 'Proactive' monitoring has become the standard in anti-money laundering programs over the past few years. Using sophisticated technology it is possible to have computer systems automatically and systematically examine every transaction that flows through a financial services firm. This results in the continual assessment of the full range of activity exhibited by the customers of the financial services firm, greatly increasing the likelihood that suspicious behaviour is identified, and that it is done so in a timely fashion. **The dynamic nature of the methods employed to launder money and finance terrorism** Those that launder money and finance terrorism are typically highly motivated individuals or organizations, often with substantial resources available to them. They expect that

competent authorities will attempt to disrupt their 'business' and will go to great lengths to both acquire information on how anti-money laundering programs attempt to identify them and in continually changing and innovating in their methods in an attempt to avoid detection.

Because of this, while certain typologies of money laundering are known, it is not possible to specify the precise means by which money laundering and terrorist financing will be conducted. Moreover, the very measures implemented to specifically identify certain forms of behaviour will often become known to the money launderers and therefore directly influence, even accelerate, changes in the ways in which money launderers operate.

When correctly implemented, active monitoring approaches can adjust their perception of risk dynamically based upon the actual behaviour exhibited by the customer base by way of their transactions. The power of this approach is twofold:

- Firstly, by making risk assessments on the basis of the behaviour most recently exhibited by customers, the definition of 'suspicious' behaviour is more subtly defined and itself continually changing, making it more difficult for money launderers to design their activities to circumvent detection
- Secondly, as the behaviour of money launders does change over time, perhaps as a result of the introduction of new products and services, a firm utilising active monitoring is not solely reliant upon defining new typologies, but can also use the power of an automated system to uncover emergent patterns that may be indicative of risk

The ability of any given firm to implement a cost effective risk based approach to anti-money laundering

Finally, active monitoring approaches provide a direct means to integrate the firms determination of relative compliance risks – based upon a range of factors including business operations, available KYC Information and specific regulatory directives – directly into their ongoing anti-money laundering process. We thus feel that active monitoring is the key underlying platform from which a tangible risk based approach to anti-money laundering can be effectively and cost efficiently implemented within large financial services organizations.

<u>Summary</u>

	In summary we believe that both the collection of KYC information and active monitoring are critical components of an effective anti-money laundering program. When executed properly, these two important tools can be integrated in a complementary manner in which the net result is greater than the utility of the methods used in isolation.
How should firms pursue a risk-based approach to anti-money laundering?	It is our belief that a risk based approach to money laundering centres on the ability of a firm to systematically incorporate their continual assessment of compliance risks directly into the operational procedures of their anti-money laundering program. Specifically, we refer to mechanisms whereby the interpretation of jurisdiction specific regulations, localized relative compliance risks and operational considerations can be used to parameterise or adjust some aspect of the ongoing operational compliance processes. Examples, of this might include requiring additional information from a customer who wishes to open an account to support a specific type of business in a particular location, through to incorporating the perceived risk differences in transactions that differ by source location or product utilization. The customer acquisition phase is clearly a critical stage and should be used both to determine risk profiles as well as itself being adjusted on the relative risk that different channels and customers may represent. A useful extension to KYC information could be to identify the expected use of each account, in broad terms (e.g. finding out how much a person estimates they will save per year when opening a savings account). The basis for a risk-based approach to anti-money laundering will be some sort of 'risk profile assessment'. While it is likely that the specific methods used to achieve this will vary by organization, broadly one would expect a review and assessment of those areas of a business' operations that relate to the acquisition or customers and the provision of products and services to those customers. Considerations will likely include a full assessment of the number and complexity of accounts within the institutions, the range of product lines, transaction volumes experiences, relationships with correspondents and third parties the relative degree of risk that each of these pose with respect to money laundering. This type of assessment should be made routinely on an ongoing basis and identified changes used directly to adjust operational procedures such that the risk based process remains relevant and appropriate. A successful anti-money laundering staff-training program is also a key component that must be in place to ensure a risk based approach. Training should cover all of the compliance policies and procedures, account opening due diligence, the risk assessment

	process, and suspicious activity monitoring and reporting. The level, intensity, regularity and focus of training can be adjusted based upon the overall risk profile assessment undertaken. It should be noted that a risk-based approach to anti-money laundering should, in our opinion, not be interpreted as 'ignore certain customers and activities because they are low risk'. Historically, the anti-money laundering efforts of many firms focused exclusively on those aspects of the business considered to represent the highest (some may have believed the only) risk for money laundering – areas such as private banking and wire transactions. Furthermore, the global push to incorporate legislation to restrict the financing of terrorism within broad anti-money laundering initiatives also adds perspective to the need for completeness in monitoring and business oversight, as virtually any current account can be used to finance terrorist activities. Thus, we believe that any appropriate risk based approach to anti-money laundering must be based upon the foundation of a holistic approach in which every customer interaction is considered. For all but the smallest financial institution, a holistic approach to considering customer interaction and the execution of a risk based approach to determining suspicion will necessarily involve some type of computer software based transaction monitoring. With many organizations routinely handling upwards of 100,000 transactions each day (and plenty well into the tens of millions), software based transaction monitoring is the only way in which a risk-based and consistent approach to monitoring can be cost effectively enacted. Correctly implemented, software based transaction monitoring can provide a highly effective means for a firm to apply its risk based approach consistently and systematically. Through appropriate parameterisation, software can adjust the level of risk it perceives in a certain set of transactions, based upon the customers involved, the products used, jurisdictions crossed and the specific behavioural characteristics of the transactions. We believe that this last point is a critical cornerstone of a risk-based approach to transaction monitoring. For higher risk firms with over 100,000 daily transactions a monitoring system is required with an automated, technology driven approach. The sheer volume and increased complexity of transactions at this size of firm requires profiling and monitoring the behaviour of every customer and every transaction. Traditional monitoring systems utilise

	a rules-based approach, engineered to detect pre-defined fraudulent activity rather than suspicious patterns of behaviour. This type of approach does not work well in detecting money laundering activities in this size of firm and generally produces a higher number of false positives, creates increased staffing levels and adds to management oversight. A true risk based approach for this size of firm requires a more effective system with true analytics capabilities to find unusual transactions and determine organizational risk. For medium and lower risk firms with less than 100,000 daily transactions a rules-based monitoring system or a manual monitoring system is effective for a risk-based approach. The ability to identify patterns and thresholds of behavior provides effective monitoring for the relative complexity of these firms. Summary We believe that a risk-based approach to anti-money laundering should be conducted in a consistent, integrated and holistic manner based on regular assessments of the relative risks encountered in the course of business. If done correctly, such an approach offers the firms an objective means for executing and assessing their compliance efforts and can help control the total costs involved by focusing resources appropriately.

What are, or may be, the costs and benefits of KYC and monitoring?	The primary aim of any KYC and/or monitoring implementation must be to ensure the firm's compliance with the specific regulations enacted. The key benefit is thus the avoidance of costs associated with failure to effectively comply with the regulations. Involvement with the failure to detect money laundering and/or terrorist financing brings with it very significant costs. Fines imposed by regulatory bodies can be substantial and indeed should be if they are to act as a meaningful deterrent. For many firms however, the fines levied are only one, often small, aspect of the overall cost of failure to use appropriate levels of due diligence in considering the actions of ones customers. Legal costs can be high, but typically even these are insignificant compared with the cost of extensive executive involvement in dealing with regulatory and sometimes legislative bodies and the potentially massive cost of reputational damage caused by public disclosure of infractions. Compliance is a cost for financial services firms. Many would almost certainly prefer not to have to do it, however, the nefarious activities that regulations are introduced to eliminate require that someone seeks to identify violators. Within the financial services community, the firms themselves are best positioned to conduct this process with respect to money laundering and terrorist financing given their proximity to the customer and ownership of the relationship. It is our opinion that the vast majority of financial services firms understand the need for them to bear certain costs associated with compliance and the part that they play in enforcing laws designed to benefit all law abiding citizens. This does not mean however that financial services firms have unlimited budgets for compliance and in this regard the correct implementation of KYC and active monitoring in particular can assist financial services firms from meeting their regulatory obligations in a cost effective manner. In order to interpret the cost efficiency of solutions one must consider the Total Cost of Ownership (TCO), which firms will seek to minimize in ensuring regulatory compliance. TCO is the combination of the acquisition costs of any systems and processes implemented plus the ongoing usage (staffing, maintenance, etc.) costs of the system over the likely period of use, which for anti-money laundering solutions is typically an extended period. Costs The upfront costs for both KYC and monitoring components of an effective anti-money

laundering program include the following:

- Internal Costs: The firms staffing costs related to the review, design, procurement, integration (data and processes), training & management of the methods and/or systems used for KYC and monitoring
- External Costs: The monies paid to third parties for the provision of consulting, integration services, training software and hardware as it relates to the KYC and monitoring programs

Ongoing costs include:

- Internal Costs: Staffing costs associated with the execution of the KYC and monitoring programs, audit costs related to process review and affirmation
- External Costs: Ongoing system maintenance, training, etc.

While the upfront costs can be significant in investment terms, as part of a TCO evaluation that may look at the operational life of the KYC or monitoring program as being 5 years, or indeed many more, it is the ongoing costs that are typically the most significant component and of these from a TCO perspective the firm's internal costs are typically the clear majority.

The costs associated with KYC should be relatively stable, with a standardised process for the collection and evaluation of necessary information. If an institution has a high rate of expansion in its customer base then there are clear advantages in making the upfront investment to ensure that the cost per customer acquisition is minimized.

The costs associated with monitoring relate to the costs associated with dealing with the output, typically some form of exceptions list, in a manner that is considered appropriate by the firm and its regulators. There are three principle parameters that control the magnitude of this cost, alerting accuracy, alerting configuration maintenance and alert processing efficiency.

Alerting accuracy

There is a broad range of options for firms seeking to implement anti-money laundering monitoring solutions. In simplistic terms, the solutions available vary in sophistication from transaction filters, through simple rules based systems, to scenario spotters and at the high-end customer modellers. One key difference of these approaches is their relative ability to automatically identify suspicious behaviour and the knock on impact that this can

	have in terms of cost. The two principle considerations here are so called false-negatives and false-positives. False Negative Costs A false negative is a genuine case of money laundering that is not detected by the system. The more simplistic the alerting approach deployed, the greater the likelihood of false-negatives. The costs associated with false negatives are all of the downside risk items discussed at the beginning of this section. False Positive Costs A false positive cost is an exception produced by a monitoring system that on review is determined to not be of interest with respect to potential monitoring (i.e. false). Transaction filters and rules based systems are notorious for their high false positive rates, with systems often producing literally thousands of alerts per day. No matter how efficient the alert review and sign-off process, these systems typically result in the requirement for a very significant support staff to review alert output. Scenario spotters, which monitor well-known high-risk scenarios are more highly tuned and can result in slightly lower false positive rates. Customer modellers which use behavioural models of assessment produce the lowest false positive rates and hence have the lowest costs associated with pure false alert handling. The reason for this is that customer modeller systems incorporate behavioural modelling into their transaction monitoring and are capable of making contextually relevant decisions. It is the lack of context in transaction filtering, rules based systems and often scenario spotters that results in the high false positive rates and accompanying excessive costs in alert review. Alerting configuration maintenance The methods used to launder money and finance terrorist activity change. The people that seek to perpetrate these crimes are highly motivated, well funded and have access to considerable resources. This means that they are aware of the processes and methods engaged to try and identify them and it is thus likely that they seek to continually adjust their behaviour in an attempt to complicate these efforts. For this reason, ‘static’ solutions such as transaction filtering, rules based systems and scenario spotters can quickly become outdated and require periodic updating. This process can become quite expensive if one aims to both manage false positives (by defining many different configurations for different aspects of the business) and remain relevant with respect to changing patterns of money laundering.

It is possible to deploy customer modeller systems that are ‘dynamic’ in that they are capable of adjusting their interpretation of activity based upon what has occurred most recently. These types of solutions provide a high degree of protection against changes in the underlying behaviors without the need for continual configuration adjustment. Hence, this offers substantial reductions in the ongoing costs associated with using a monitoring solution.

Alert processing efficiency

The final important aspect of TCO for monitoring solutions is the cost associated with processing a system alert through to resolution. This process is a critical and substantial part of a comprehensive risk based approach to risk management. Organisations will typically define a process whereby an alert will be examined, possibly referred to other groups/people, investigated and ultimately closed off or reported. The features that a monitoring system offers can greatly impact the costs associated with this. A low-end system may provide a simple exception list of alerts. In order the deal with this a firm will require that its staff somehow access and review all transactional activity associated with a customer and then manually conduct an investigation and group review process through until resolution. The costs associated with the time to deal with cases (often many hours) can result in a very high TCO.

Sophisticated monitoring systems, which typically carry higher upfront costs, often come equipped with a comprehensive range of tools to assist this process. From providing detailed evidential cases to users rather than simple alerts, through to an integrated workflow, action automation (e.g. referral letter generation, suspicious transaction report filing, etc.) and comprehensive audit trails – these solutions can greatly simplify the costs associated with dealing with exceptions resulting in a substantially reduced TCO.

Benefits beyond compliance

Many of the initiatives introduced with respect to KYC and monitoring are providing substantial benefits to firms beyond the management of risk and minimisation of operational costs.

Beyond the direct regulatory compliance benefits of KYC and monitoring are the insight that they can bring to an organization regarding its customers. The necessity to capture and organise sometimes massive quantities of customer information to ensure effective and accurate interpretation of intent and activity, presents unique opportunities to firms who choose to proactively use this resource for addressing problems beyond compliance.

	The very same factors that have made money laundering so prevalent in financial services firms – convenience of access, disintermediation, real-time transactions, etc. – have created substantial problems for firms seeking to understand customer behaviour to tackle core business problems such as fraud detection and management and effective customer communications and marketing. Many firms are realizing substantial benefit from leveraged the infrastructure they have put in place for anti-money laundering to address these areas and generate substantial ROI. Increasingly, we are seeing many firms who choose to implement monitoring systems for anti-money laundering decide at an early stage, often in parallel with their anti-money laundering effort, to leverage the infrastructure to address a range of other critical business functions that share many of the same underlying issues as money laundering detection. This would not be possible with the low end monitoring systems that lack the contextual understanding of high end systems.

SEMAGIX'S RESPONSE TO DP22

January 2004

RESPONSE ON DP22

These consideration points have been generated in response to DP22 and provide detail on how semantic technologies can address the KYC issues being faced by the financial services sector

SUMMARY (addresses the 4 questions posed)

1. KYC information is the cornerstone of any effective risk-based approach to AML. The effectiveness of the KYC process is therefore a factor of the scope of the information collected and the ability to analyse and utilise this information.

   Response

   a. Internal information should be leveraged from all touch points with a customer, and augmented with information gained from external sources.
   b. Analysis of this information should be based on sound and trusted AML risk profiles that are specific to the line of business.

2. Transaction monitoring(TM) and Know Your Customer (KYC) are treated separately within DP22, with mention only made to the automation and technical considerations for best practises within transaction monitoring.

   Response

   a. A layered approach to reducing the anti money laundering risk should be adopted, and one in which TM and KYC are considered together within an integrated approach to **customer risk management**.
   b. Semagix's view is that current semantic technologies provide a technology platform to support a comprehensive KYC process that is fundamental to the overall AML approach.

3. Law enforcement agencies require a cross section of detailed information associated with a customer that is deemed as high risk, and within a short time frame of that suspicion being identified.

   Response

   a. There is a critical need to ensure that suspicious information is passed to law enforcement agencies in a timely manner. This is best served through the electronic submission of reports detailing all information as it relates to the customer, and on which the organisation has based its suspicion.
   b. As outlined in Point 1 Customer Risk is a combined function of TM and KYC, and therefore suspicion of an individual would be a combination of the information and results generated from both of these areas.
   c. Inclusive in this, is a feedback loop from the law enforcement agency back to the financial service community, both on the improvements to the reporting process and on the results to the information submitted by the financial institution.

4. The cost/benefit analysis of implementing a risk-based approach that provides a unified view of the customer for dealing with credit, fraud and compliance risks, is seen at the group level as the optimal approach.

Response

   a. Hiring more compliance heads to cover the short-fall in resources resulting from the ever more detailed KYC requirements is not a viable cost option for the long term. This approach increases the operational overheads, whilst providing no ability to scale
   b. If customer information is reused from across various business units there will be a reduction in the continuous and intrusive need to request customers to provide information that they have already provided, albeit to a different business unit and for a different reason.
   c. The unified view of the customer, used to support the Know Your Customer process, provide additional benefits in other business lines wishing to provide more appropriate services and reduce other risk areas , such a miss-selling.

5. Semagix supports the adoption of Option 2.

Response

   a. This would allow for more integrated approaches to key topics, such as Operational Risk Systems, to be adopted by the financial institutions. This would place the onus on the institution to detail the risk environment as it relates to them, and the systems and processes required to address these risks.
   b. Technology supports this approach, as it can be appropriately used to provide a consistent, systematised and auditable approach to KYC as it applies to a specific institution, and allows for the adoption of best practises across the financial services sector as a whole.

The following sections provide the detail that supports the answers to the previous 4 questions, and relate to the specific paragraphs within DP22.

SCOPE OF INFORMATION – Para 3.7 and 3.8

6. The collation of KYC information is the cornerstone of any effective AML process and has a direct and positive impact on any follow-on activities. Semagix enables the collation of a broad scope of information, which includes both qualitative and quantitative information.

   a. The nature and depth of the information collected should mirror the risk environment it is supporting (e.g retail or private banking).
   b. For increased effectiveness of results, the scope of the information should be broad as possible. This should not be limited by technical challenges and can be inclusive of elements such as; customer photographs and other biometric inputs.
   c. Banks should not seek the compromise of reducing the number of information sources so as to reduce the burden on a process or reduce the number of false positives being produced.

d. Information sources might be internal as well as external, with the ability to re-use existing customer data held across different operating divisions; this also has a positive impact on CRM.

BUSINESS DRIVERS OF INFORMATION – PARA 3.9, 3.10

7. From an information perspective, depth and quality of information are the two main determinants of the effectiveness of a KYC process, however this effectiveness is degraded if the information is not managed or used intelligently.

    a. Information should be used to support and model the risk based approach adopted. Semagix looks to model certain aspects of the information gained, such as transaction risk, occupation risk or relational risk.
    b. Semagix ensures that the information collated can be used to create accurate risk profiles that can support the efficient allocation of resources.

WHY FIRMS HAVE EXISTING CUSTOMER INFORMATION PARA 3.8 - 3.12

8. Traditionally the two control measures of KYC and Monitoring have been treated separately. Semagix takes the view that these two measures can be, and should be, treated within an integrated approach.

    a. The benefits of adopting this integrated approach are seen as; reducing the cost of the client adoption process, the reduction of information requests on the customer and more effective result and result handling.
    b. Due to the resources, time, cost and CRM impact of such a process, KYC should not be seen as just a gateway of accepting or declining customers but as an integral part of continuous customer risk monitoring.

    The reasons why these processes have previously been treated separately are seen as;

    c. The two control measures (TM and KYC) are performed at different stages of the banking value chain, and rely on different processes supported by different technologies.
    d. An additional factor to why they have been treated separately is that these processes have grown organically from within different operating divisions and hold different reporting lines of those responsible for the processes.

PRACTICAL ISSUES – PARA 3.18

9. An efficient KYC process is central to reducing the associated cost of compliance.
    a. Logical view over centralise view: the cost of replicating of centralising the storage and management of customer data can be extremely high and carries with it its own risk. The ability to have a logical view is seen as being more efficient and reduces the risk of such a project.

b. Maintenance and updating: Semagix enables the changes of customer details that are made at the business unit level to be reflected in the logical view for that customer. If there is a change in the risk profile of that customer caused by this update then an alert triggers some additional workflow.

AML MONITORING – SECTION 4

10. AML monitoring is less effective if it is not used in conjunction with KYC information.
    a. The integration of KYC profiles into AML monitoring can improve the overall effectiveness of such systems by reducing the number of exceptions generated and can help prioritise these exceptions when they are generated.
    b. As proactive monitoring should be based on the identification of suspect characteristics then Semagix can help identify the qualitative characteristics that transaction monitoring systems are not that good at detecting.

GENERAL POINTS

11. The benefits of adopting a more integrated approach are seen as;
    a. Granular risk profiling of customers removes the blanket approach of risk categorisation, which will actually increase the amount of clients that can be taken on.
    b. Continuous KYC monitoring, which doesn't mean a large incremental cost or heavy resource involvement, is something that can be used to reinforce the adoption of a risk-based approach.
    c. Automation enables the adoption of a more flexible and adaptable process.
    d. Seamless delivery of information across and outside the organisation, which also impacts on the effectiveness of law enforcement agencies.
    e. Typology modelling raises the bar on the due diligence and the effectiveness of the results returned.

SUBMISSION OF SKANDIA GROUP TO FINANCIAL SERVICES AUTHORITY

DISCUSSION PAPER 22

Reducing Money Laundering Risk: Know Your Customer & anti-money laundering monitoring

January 2004

1. Introduction

The UK operations of the Skandia Group include Skandia Life Assurance Company, which offers unit linked life assurance and investment contracts, Skandia MultiFUNDS Limited, which is an investment firm involved in "fund supermarket" activities, and Skandia Investment Management which is an operator and manager of collective investment schemes.

We welcome the opportunity to comment on DP22.

2. Summary

- The use of KYC and monitoring information and tools are indeed relevant to an effective contribution to the fight against money laundering, crime and terrorism.

- Detailed cost benefit analysis is required to support any intended future prescription given likely time and cost implications if IT solutions are required.

- Any KYC details have to add value to the process of identifying financial crime and a lack of KYC information should not be equated to suspicion or high risk. Flexibility must also be allowed to ensure costs and risks are proportionately balanced.

- Increased transparency on acceptable KYC and monitoring standards are welcome and should promote industry best-practice.

- Buy-in and support from all parties involved in business from customer, to adviser to provider, and relevant enforcement agencies is needed to maintain standards and robust processes across all sectors of the industry. The FSA should ensure it appropriately addresses these perspectives within its recommendations and the scope of its responsibilities.

- The situation that must be avoided is the imposition of oblique requirements without clear guidance and rules.

- Any consultation proposals must recognise the restrictions on some firms being outside the usual ‘advice’ and ‘KYC’ sales process.

- We are not in favour of immediate changes and a period of consolidation and reflection is required at a time of significant legal and regulatory change.

- It is important that firms are given time to develop the ‘risk management’ approach supported by more feedback from the regulator/enforcement agencies on money laundering activity and typologies.

3. Detailed comments

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

It is also important that any prescriptive provisions recognise the fact that some firms may be more distanced from the sales process and might be restricted from access to existing KYC and best-advice information due to an independent business relationship, client confidentiality and data protection considerations or client information which is not relevant to the product/service.

It should also be recognised that certain KYC information adds little or no value in terms of identifying financial crime e.g. NINO, or indeed it may not be appropriate for the firm to request/seek it given the nature of the product/service offered e.g. occupation.

Any attempt to impose new or additional KYC requirements on the industry can not be progressed in isolation from the need to engage other parties, especially the client, in their awareness and acceptance for any increase in UK business standards and legal and regulatory expectations.

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

Firms should retain the flexibility to be able to meet its requirements in a way that reflects its assessment of the risks within its client-base and product/service offering.

A one-size-fits-all approach to rules and/or guidance is inappropriate and is unlikely to ensure any enhanced provisions are properly targeted across the industry where risks and practices may need most strengthening.

The threats, and the need for more KYC/Monitoring control, do vary dramatically by the type of business and that should be more clearly recognised within any requirements.

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

Enforcement agencies are best placed to input on this. However, the quality and value of output from firms to NCIS and other relevant agencies arising from any future provisions in these areas must be demonstrably significant and capable of being effectively managed by those agencies. To this end it is important that any increased reporting is not put into place without there being a more effective feedback process between the industry and the various enforcement agencies. This would provide useful intelligence and feedback on the quality of a firms policies and procedures.

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

The existence of legacy systems in most firms may prevent or impact on their ability to introduce cost effective automated monitoring solutions. Whilst manual monitoring is certainly not infallible the robustness of any automated monitoring process relies on the quality of its design as much as its correct and timely practical application by the firm.

If additional data/information has to be kept this will need to be provided by customer/intermediary as part of sales process which will impact on related costs e.g. documentation. There would also be cost issues in terms of handling and storage of that data as well as how firms effectively use it.

These factors need to be taken into account in any proposals.

Q5: Which options presented do you prefer and why?

Given the breadth of recent legal and guidance changes in the UK via Proceeds of Crime Act, the New 2003 Regulations and impending GN2003 and further GN2004 changes scheduled, we would favour a period of consolidation and reflection rather than see the continuance of perpetual change in this area i.e. Option 4. Existing rules provide the FSA with sufficient powers to achieve its anti-money laundering objectives. This should ensure firms have adequate risk-based systems and controls, including appropriate monitoring and KYC processes.

In this period any expansion of existing rules in respect of KYC or transaction monitoring should, as far as possible, take the form of high-level directional guidance, as opposed to any prescriptive rules or guidance on specific KYC and monitoring requirements. This should seek to promote better money laundering risk management by firms, but also might usefully qualify the requirement on firms to adopt an appropriate approach in its use of KYC and monitoring data and tools, and to reflect this within its risk-based policies and procedures. The JMLSG Guidance Notes would continue to amplify best-practice and support the processes for firms to make well informed risk management decisions. The UK financial services industry is too diverse to accommodate prescriptive rules, and the application of existing requirements under SYSC should enable the appropriateness of policy and practice to be preserved and where necessary addressed within the UK regulated financial sector.

However, we accept that the UK position needs review in light of both national and international events and developments, and so an underlying periodic review process would be sensible.

4. Other questions

DP22 Section 3.7

Very few (if any) regulated activities will be undertaken using only customer ID information. However, if both legal and supervisory standards will expect and judge firms on their ability to obtain information above and beyond ID then some element of prescription in the form of guidance or rules will be needed to support consistency of interpretation and application across the industry. It is imperative that ‘best-practice’ is not confused with ‘regulatory requirement’.

DP22 Section 3.9 & 3.12

Any future provisions should not disadvantage those firms who are remote from the KYC and suitability requirements processes under COBS. Also, product providers like Skandia, who do not provide advice may not be the prime relationship manager with the customer. Therefore regardless of any risk-based approach, it will not be practicable, appropriate or necessary for all firms to know their customers equally well. The onus should not be left to firms alone to justify any enhanced obligations to their customers.

DP22 Section 4.22

It is agreed that the unusual should not equate to suspicion. Similarly, the frequency of transactions should not be seen as a denominator of risk.

DP22 Section 4.24

Whilst it is agreed that manual systems are not infallible, many firms will face problems e.g. legacy systems and time/cost issues, in implementing effective automated solutions. The relevance and value of automated systems must be determined with each firm and judged to be appropriate to a proper risk-based assessment of its business.

Conclusion

We would be happy to discuss with the FSA any of the issues raised and comments made in this submission.

Please note submission details requested in your pro-forma not covered in the above response:

Submission from:

Name:	Steve Blackbourn
Position:	UK Group MLRO
Company:	Skandia
Capacity:	As a representative of an authorised firm

Enquiries:

Steve Blackbourn

UK Group MLRO

Address for correspondence:

Skandia Life

PO Box 37

Skandia House

Portland Terrace

SOUTHAMPTON

SO14 7AY

Phone: 023 80 729575

Fax: 023 80 726463

Mobile: 07970 088242

January 2004

Discussion Paper 22 (DP22)

Financial Services Authority (FSA)

Reducing money laundering risk

Know Your Customer and anti-money laundering monitoring

Response from

The Society of Financial Advisers (SOFA)

The Society of Financial Advisers (SOFA)	SOFA is the financial services arm of The Chartered Insurance Institute (CII). It is specifically dedicated to the professional advancement and education of financial advisers and planners. SOFA's activity revolves around its four principal objectives: ∉ To raise professional standards ∉ To encourage professional qualification ∉ To facilitate continuing professional development ∉ To achieve recognition for professionally qualified financial advisers and planners. SOFA's principal thrust is to develop the financial services professional of the future, i.e. one who is professionally qualified at a high level, who is committed to their personal professional development and who practices according to high ethical principles.
	The Society of Financial Advisers 20 Aldermanbury, London EC2V 7HY tel: 020 8989 8464 fax: 020 7600 0766 email : info@sofa.org website: www.sofa.org Managing Director : Brian Lawless Tel: 0207 417 4448

The short response shows a preference for a combination of Options 3 and 4 – make no settled decision now and review the position again in, say, two years time, in the meantime, the FSA should make no new rules or guidance and should rely on the Joint Money Laundering Steering Group (JMLSG) Guidance Notes to promote adequate standards in regulated firms.

It seems to us at SOFA that the Proceeds of Crime Act 2002 (POCA) together with the JMLSG revised Guidance Notes should be sufficient to ensure that the financial services industry adhere to the anti-money laundering rules. There should be no need, currently, to create further FSA rules or guidance.

It does not mean, however, that the FSA should actually do nothing. SOFA feels that the FSA should be active in two areas:-

i) the FSA should work with the JMLSG to produce the reviewed Guidance Notes. This should ensure that both the JMLSG and the FSA requirements as far as the Guidance Notes and the financial services industry are concerned are all met. There should only be one set of Guidance Notes. Firstly to avoid confusion and secondly to try and cut down on the information/change/ consultation papers overload that the industry is suffering at present. It is appreciated that money-laundering is a serious subject but it cannot be necessary to have two different sets of rules and guidelines covering the one industry.

ii) the FSA should provide training to Money Laundering Reporting Officers and senior managers responsible within firms to ensure that they are fully aware of their responsibilities and how to carry them out. This will enable these individuals to onwardly train their own relevant staff. This is such an important subject that there should be a requirement to attend such training and some form of testing to be carried out afterwards – a form of maintaining and enhancing competence in the subject.

Two further points are made in this response.

Firstly, referring to the importance of anti-money laundering and record keeping in 4.11 of DP22, this should be emphasised in the FSA's current initiative brought forward recently by John Tiner on the whole subject of record keeping in general in relation to mis-selling.

Secondly, and this could be very important, part of the emphasis of DP22 is on the Know Your Customer (KYC) rules and their importance in anti-money laundering procedures. What will happen when Sandler products are launched if either of the Option 1 or Option 2 sales processes is chosen by the FSA as the way forward (see FSA Discussion Paper 19). There will be no KYC (or indeed conduct of business) rules so how will the anti-money laundering procedures take place? SOFA can only see the Option 3 sales procedure working where there will be limited KYC rules – in any event, the FSA are fully aware of our view that Sandler products are totally unnecessary.

Returning to anti-money laundering procedures, it seems that Sandler products (the lump sum investment variety) with little or no early surrender penalty and no KYC rules will be ideal for those wishing to indulge in money laundering activities. It seems likely that if Option 2 in Discussion Paper 19 is chosen there will not be “face-to-face” business of this type being transacted. The danger of this is actually brought out in DP22 at 4.8(i). We do realise that the anti-money laundering rules limits on size of investment before more stringent checking procedures kick in may limit the problem but they will not eliminate it altogether.

It is imperative that some further “joined-up thinking” is employed between these various discussion and consultation papers – this is again borne out in assessing DP22 in relation to DP19.

Group Compliance
1st Floor East
Standard Life House
30 Lothian Road
EDINBURGH
EH1 2DH
Tel: 0131 2450712
Fax: 0131 2450720

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

29 January 2004

Dear Daniel

FSA Discussion Paper 22: Reducing Money Laundering Risk

On behalf of Standard Life Assurance Company, Standard Life Bank and Standard Life Investments, I welcome this opportunity to comment on Discussion Paper 22. As a Group of companies, we have individually contributed to and broadly support the responses already made by the ABI, BBA and IMA, but I also felt it appropriate to provide our separate comment on this important Discussion Paper.

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

We acknowledge that information relevant to 'Know your customer' (KYC) is important in reducing risks associated with money laundering and is necessary in meeting our legal and regulatory obligations. However, we consider the amount of information collated must be proportionate to the risks associated with customer and product types. KYC information should be used in conjunction with effective transaction monitoring. In the main, the suspicions Standard Life report to NCIS, are based on specific and 'unusual' transactions, they are generally not initiated by the KYC information held. KYC information however very often compliments or supports the suspicions that we report.

Unlike high street banks, our companies have lower volume transactions, so transaction monitoring or exception reporting tools would be instrumental in identifying and thus reducing money laundering risk. Appropriate KYC would obviously compliment any transaction monitoring measures introduced.

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

To pursue an effective risk-based approach, a firm needs to apply consistent standards. This can only be achieved by understanding ones customer base, the products marketed, transaction types and the distribution channels used. A thorough review of these internal risks and ranking them against each other is therefore necessary.

In addition, our experience, networking with peer companies and discussions with the JMLSG/NCIS/Police and Scottish Drug Enforcement Agency have all (in varying degrees) been used to risk assess our approach to anti-money laundering. A fundamental knowledge of our products and clients – and how they can be used in money laundering is essential. However without collaboration and agreement within the industry and guidance from trade bodies, Law Enforcement Agencies and the FSA, inconsistent standards and practises will continue throughout the industry. A KYC product risk-matrix drafted and agreed by the industry and approved by the FSA would be favourably viewed and would provide consistency across the industry to help ensure we all work from a level playing field.

We subscribe to the ABI response in that it is important to assess risk in the context of other firms, using for example:

- Industry bodies i.e. trade associations and the Joint Money Laundering Steering Group (JMLSG)
- Law enforcement data (NCIS/FIUs/TFUs)
- Networking at conferences, IMLPO meetings, Compliance Officer discussion groups
- Guidance from the local FSA supervisor
- Industry press and
- Use of external consultants

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

The various law enforcement agencies are best placed to answer this question themselves.

However, under the current disclosure environment (and enforced by legislation), we are required to report all suspicious activity. This includes any additional customer activity after a report has been made (e.g. client change of address, client request to surrender etc). As a result and taking into account the information that we currently report, it is difficult for us to identify what other information (or report) could be of benefit to the authorities.

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

As stated in Q1 – the cost of obtaining KYC information needs to be proportionate to the risks involved.

If required to collect more KYC information than that currently collated, it is envisaged that by requesting more, we would experience higher processing costs. Applications would be returned to customers and intermediaries due to detailed information not being supplied in the first instance. In addition, the cost of delay experienced by customers will inevitably result in customer frustration and possible disinterest, resulting in some cases, in loss of business.

Other costs associated with the need to collect more KYC would include:

- Collecting more customer information and obtaining customer consent.
- Retaining and using information
- Compliance with the Data Protection Act 1998.
- Education and awareness raising with intermediaries and customers
- IS costs associated with the designing of business processes to collect, collate and retain information.
- Updating company literature, to ensure application forms are clear regarding the new requirements;
- Addressing legacy systems and historic record keeping issues
- Additional stationery
- Staff training
- Monitoring and auditing
- Collecting supplementary or updating existing information

The benefits of collecting additional KYC (apart from an obvious compliance with regulations) would include:

- Potential information for marketing purposes
- Possible fraud reduction.

Transaction Monitoring costs for firms will cover:

- Building data extracts from legacy systems;
- Complications associated with integrating the business units within a ‘group’ belonging to a ‘parent company’
- Manpower including internal IT staff resource;
- Software and software licences;
- Cost of pursuing exceptions that are not suspicious;

Benefits for firms:

- Likely marketing benefits from automated systems.
- The likely reduction in fraud;
- Protection to the firm and its staff from abuse of its products and services (by customers and intermediaries)

Q5: Which options presented do you prefer and why?

Option 1 – include in the Handbook specific rules and/or guidance on KYC and/or monitoring

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

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

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

Option **4** is our preferred choice.

Since N2 and 9/11, there has been much change in the Anti-Money Laundering arena. The introduction of the Proceeds of Crime Act 2002 and the new JMLSG Guidance Notes due to be published in 2004 have (and will) require further change – the benefits of which are not yet completely apparent. Furthermore with the radical review of the JMLSG Guidance taking place in 2004/2005, we feel it would be beneficial for the FSA to delay further regulatory change but rather wait and see what positive changes result from the recent and impending legislative changes.

Supporting the status quo we also believe that the high-level rules currently in place (e.g. Approved Persons regime and the FSA ML Source book) already provide the FSA sufficient opportunity to directly influence industry practice and reduce the risk of Money Laundering without the need of introducing further rules.

Should you require any further information or clarity regarding any of our comments please do not hesitate to contact me.

Yours sincerely

Phil Hay
Group Money Laundering Reporting Officer
Standard Life

STB

STB Systems Limited
India House
45 Curlew Street
London SE1 2ND

t ::+44 20 7403 2188
f ::+44 20 7403 4425
e :: info@stbsystems.com
w :: www.stbsystems.com

Daniel Shonfeld
Financial Crime Policy Unit
Prudential Standards Division
15th Floor
The Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

Dear Daniel,

Re: DP 22 Reducing Money Laundering Risk

STB Systems is a company specialising in compliance solutions for financial institutions, specifically including regulatory reporting and anti money laundering. We have customers around the world and get feedback from them on the issues they encounter in attempting to reduce their exposure to the risk of money laundering. As such, we feel it appropriate to respond to DP 22 to express our view on the specific issues you have raised, based upon that feedback and our own experiences.

You asked five specific points:

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

Firms already need to gather KYC information to properly manage credit risk, customer relationships and to eliminate miss selling of products, so AML does not represent a significant additional burden in this respect. However, they have not been so good at maintaining the currency of this information. We would recommend any institution to automate document and verification controls and renewal schedules in order to maintain future conformity of the documentation for KYC. Many firms still only retain paper copies in poorly organised facilities, many of which are off-site and remote, making ready access to such documents difficult. We would encourage that guidance is given to firms to improve upon such methods.

Active monitoring is the only way to protect against the significant operational risks of, not just AML, but also fraud, both internal and external to an organisation. Firms cannot afford to sit back and wait for something to happen, KYC alone is not sufficient. Technology is now readily available to perform checks of payment records against all international, local and internal sanction lists and further systems are available to monitor transactions and accounts for unusual, potentially suspicious, activity. Firms should be encouraged to consider the implementation of such technologies to assist in risk reduction.

2) How should firms pursue a risk-based approach to anti money laundering?

Financial regulation has increasingly encouraged firms to improve their management of risk and has led to the development of risk-based models for management of all significant exposures. The main principles of Basel II are further supplementing this approach. With AML, firms need to assess the riskier parts of their business to money laundering practices, the profiles of segments of their customer base and review their policies and procedures accordingly. If active monitoring for money laundering is to be implemented, firms should assess whether business volumes will negate the effectiveness of purely manual processes. It was interesting to read from the FSA's own survey and review of Operational Risk as it is being implemented by UK firms that not one of those firms had defined the level of risk they were prepared to accept in attempting to define their policies. It would seem clear that in this area, which includes the exposures contained within AML, firms still have some way to go and that the FSA should offer guidance as to how firms should make that risk assessment.

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

Only the law enforcement agencies can properly address this issue. However, we would expect that more consistency in the level of detail provided and the accuracy of that data would be a primary concern. The availability to the firm of consolidated information regarding a customer about whom the firm is suspicious would be a significant step forward and should significantly reduce the time taken by firms in preparing adequate reports and for the law enforcement bodies to get to first base in their investigations. If this includes electronic copies of supporting KYC documents, then NCIS should be able to respond much more quickly to reports submitted by firms as the initial step of identification should be much easier for them.

4) What are, or may be, the costs and benefits of KYC and monitoring?

As discussed at 1), the benefits of KYC information are well known to support other areas of a business and a clear cost benefit is likely to be derived by most firms, especially as the additional burden for AML purposes is likely to be minimal. The benefits of automated monitoring are not quite so obvious and there is often a considerable cost of implementation, though probably lower ongoing costs than for KYC. It is our belief that significant benefit can be derived from automating much of the monitoring process, particularly where moderate to high volumes are involved, and products, such as STB's own STB-Detector, are now being competitively priced to represent value for money. Firms will benefit from having a consolidated database representing all of the business they conduct with customers in one place. Rules-based technology in particular can be utilised to mine the data for much more then just AML control purposes. The resulting compliance database, needed to satisfy automated AML monitoring, can be utilised to support all areas of a busy institution effectively.

5) Which options presented do you prefer and why?

Here you are asking whether the FSA should 1) make specific rules to force KYC and/or monitoring compliance, ii) make high level rules to promote better AML risk management, iii) make no new rules or guidance and rely upon the Joint Money Laundering Steering Group to provide adequate guidance, or iv) do nothing now and reassess in about two years time.

STB would promote the second option as being the most appropriate response from the regulator. NCIS estimates that £25 billion is laundered through the UK every year, so this issue must be taken seriously and firms be given responsibility to manage money laundering risks appropriately. Nonetheless, although this is clearly a major issue for the UK and international economy, it is not a "one size fits all" issue, so a more prescriptive regime would not be appropriate and would be liable to force further consolidation and closure within the financial industry if a high cost of compliance is imposed.

We feel that the FSA should also work closely with the JMLSG to provide guidance to firms as how best to make risk assessments and apply the most suitable degree of "best practice" response for the exposures faced by each individual firm and type and scale of business. There are clearly gaps in the understanding of these risks within firms, which leads to poor assessment and definition of acceptable risk.

Finally, we do not believe this issue can be left for a further 2 years as the scale of money laundering is much too significant to be ignored and technologies are now available to make the improvement of controls viable. There would be a significant systems risk from delaying this issue into the same timeframe as Basel II. If significant systems changes were to be introduced during 2006 for AML requirements, this would have a serious impact at a time when firms will be dealing with the considerable cost and complication of Basel II.

We recommend swift action on this issue by the FSA to avoid a logjam of systems improvements.

We hope that our comments will assist the FSA in this process and would be pleased to discuss these and other related issues with the FSA at any time.

Yours sincerely,

Michael J. Thomas
Group CEO

APCIMS
EASD
Working for the
Investment Community

114 Middlesex Street
London E1 7JH
Tel: +44 (0) 20 7247 7080
Fax: +44 (0) 20 7377 0939
email: info@apcims.co.uk

27th January 2004

Daniel Shonfeld
The Financial Services Authority
25 The North Colonnade
Canary Wharf
London

Dear Daniel,

Discussion Paper 22 Reducing Money Laundering Risk

APCIMS is the trade association that represents the interests of stockbrokers and investment management firms that act on behalf of the private client. We have around 240 members, based in the UK, the Channel Islands, the Isle of Man and across Continental Europe. A list of our members is attached.

We have responded to the issues raised in the Paper, but it would be useful once these issues have been discussed to move the discussion forward as well. The problems with identification and KYC are well known. There is doubt that monitoring will actually enable firms to detect money laundering, and hence firms are concerned at what else can be done to improve their ability to play their part in fighting financial crime.

Firms need to identify clients and verify addresses, but the tools available are inadequate. None of the documents used to verify identity were actually designed with that purpose in mind and they can be easily forged or faked. Firms feel that the present requirements inconvenience the innocent and do little to deter the criminals who can find their way through the system. Furthermore, the need to enforce a paper trail that is widely acknowledged to be deficient is counterproductive to firms' efforts to build a strong compliance culture. The FSA hosted a very useful workshop on identity theft and impersonation fraud in 2003, at which the representative from the Home Office informed the delegates of the project they are running on proof and verification of identity. Initiatives like this will take the debate to the next level and could lead to more robust methods of verifying identity.

The discussion about monitoring in the DP22 overlooks the basic problems with automated monitoring systems. These systems can only generate reports within certain parameters and these must be set so that the firm is not overwhelmed by reports that all require investigation. Whilst only unusual trades can be highlighted, the discussion also overlooks the fact that money launderers are often sophisticated criminals who will ensure that their business conforms to expected parameters. (Indeed the financial arrangements used to fund the 11 September attacks in the US were not unusual transactions and would not have alerted any business to the underlying intentions of the terrorists). We must assume that many financial criminals are sophisticated and well enough informed to be able to ensure that their trades conform to a pattern and blend in with the general business of the firm.

We are sure this is not intentional, but the conclusion being drawn from the proposals in DP22 is to ensure that more reports are made to NCIS in order to prove that the reporting regime is working. APCIMS does not believe that this will lead to an optimal solution, especially in light of the NCIS estimate that they will be overwhelmed with well over 100,000 SAR reports in 2004.

For the reporting regime to be more effective, there needs to be a balance between public and private sector resources and priorities. In many instances, it could well be more logical and successful to follow the trail from the predicate crime to the money, rather than create thousands of reports to be sifted through in the hope of spotting something suspicious. The FSA, NCIS and the LEAs should develop ways of sharing information with firms about suspicious activity and suspected or known criminals so that a true partnership to fight financial crime can be developed.

We agree the way forward is through the risk-based approach. In theory, most firms would agree with the approach outlined in paragraphs 2.8 and 2.9 of DP22, but in practice, there is so much uncertainty and lack of clarity, and the risks of getting anything wrong are so high, that few, if any, firms consider that they can take a risk-based approach to anti-money laundering.

Additionally, the FSA has already recognised that the most obvious money laundering activity generally takes place where cash enters the system, and that some types of businesses (such as banks and bureau de change), are more attractive to criminals than others. This was stated by Carol Sergeant at the July 2002 FSA money laundering conference, and is certainly supported by all the available typologies provided by the Assets Recovery Agency's proceeds of crime update, NCIS Current Intelligence Assessment and HM Treasury's UK anti-money laundering strategy. However, despite repeated high level statements from FSA management, the reports that APCIMS has received from many of its member firms are of FSA regulatory teams not being prepared to accept that investment management and stockbroking firms are allowed to take a risk based approach.

The possible conflict between anti-money laundering requirements and other legislation, such as the Data Protection Act and HMSO rules needs to be addressed. Some firms have had guidance that when data is being used for legal purposes and in accordance with a regulatory requirement, there is no obligation to obtain the client's consent for that use. This seems clear, but as there is still some uncertainty about such conflicts, it would be useful to give them further consideration.

DP22 presents us with four options. We suggest that in addition, a very useful option not included in the paper would be for the FSA to promote and facilitate a full and open examination (and cost benefit analysis) of the present arrangements, by all parties involved, to determine whether or not the gathering of KYC material and anti-money laundering monitoring have the desired effect in the fight against crime and terrorism. If they do not, the implication is that firms are gathering such data and carrying out monitoring merely to comply with FSA Rules, rather than to fight crime. If this is so, then we need to improve the system or explore alternative approaches.

APCIMS would also like to see an anti money-laundering framework that is based on the following principles.

1. Know Your Customer. Once a firm has undertaken the initial anti money laundering KYC checks on a customer (upon their entry into the financial system), then these checks do not have to be repeated by other regulated firms, except in specific, higher risk situations.
2. That a risk based approach is implemented that recognises the low risk nature of much of the financial services industry
3. That the FSA allows, and accepts, firms to use their judgement in respect of submitting SARs. We note with interest that NCIS have put forward a new SAR disclosure form aimed at those reports that are of 'limited intelligence value.'

In spite of these criticisms, we welcome the paper and would encourage the FSA to continue its efforts to examine and improve the anti-money laundering framework in the UK. Our firms are committed to the fight against financial crime and are well aware of the importance of protecting the financial industry against criminals, but there is strong anecdotal evidence that the present framework is very expensive and not particularly effective. Additionally, we call upon the FSA to recognise that even small changes in terminology or guidance can lead to considerable costs for firms in relation to systems changes and documentary changes, at both client entry and client transaction level.

Please feel free to contact us for further discussion on any of these matters.

Yours sincerely,

Mark Peate
Investment Services Manager

DETAILED COMMENTS

We have followed the paragraphs in DP22.

KNOW YOUR CUSTOMER

What is the purpose of KYC?

3.2
The requirement for firms to obtain KYC information predates any anti-money laundering requirements. The reasons for collecting and holding information about customers are examined in paragraphs 3.9 to 3.12 of this paper and we would argue that those purposes are actually more relevant and important that the anti-money laundering requirements.

Evidently, we recognise firms' obligations to help to fight crime, but on a risk-based approach. Currently, the two most important reasons for collecting KYC are:

- to enable a firm to know who it is contracting with by confirming the identity and address of the customer;
- to enable the firm to provide suitable advice to its customers to ensure that they invest in products that are suitable for them.

In the light of current concerns about misselling, suitability requirements are probably the most important reason for collecting KYC information. For most of our firms, under a true risk-based approach, managing money laundering risks and fulfilling reporting obligations are probably less important reasons to gather KYC information than establishing the client's appetite for risk and their investment requirements.

3.3
KYC information undoubtedly plays an important part in a number of investigations, but it would be a very rare instance when KYC information itself determines whether or not an investigation should be pursued. Statements from various police authorities confirm that they have found KYC information to be very useful, but we have not heard any of them state that the information itself has been the primary influence on their decision to initiate and pursue an investigation.

Legal and regulatory requirements

3.4
There are specific regulatory requirements, even if they do relate to the suitability requirements (see comments in 3.2 above). In DP22, the FSA state that "there are no specific legal and regulatory KYC requirements." If this is the case, then firms will have difficulty in avoiding breeching the Data Protection Act, either by collecting KYC information without telling the customer is will be used for anti-money laundering purposes, or by using KYC information they have gathered to comply with suitability requirements and then using such information for a different purpose, or by asking the client for more information than they are strictly required to gather under the rules.

3.5
Many firms routinely gather the items of information mentioned in this paragraph. It is not made clear whether the intention is to make these mandatory fields on the prescribed form, which we presume is the point.

Good practice standards

3.6
It is worth noting that the Basel Committee and the Wolfsberg Group are both banking entities and the JMLSG itself may have been reconstituted, but is still trying to establish its independence from the BBA. The role banks play and the risks they face in the world of money laundering differ from firms that are non-deposit taking institutions that do not deal with cash. APCIMS members therefore remain concerned that the anti-money laundering requirements are still largely influenced by banking considerations, and so require them to undertake inappropriate checks.

The assumption that being able to spot the unusual necessarily places the firm in a better position to manage its money laundering risk has some merit. However, the intelligent or experienced money launderer will know not to do anything that would be considered unusual for him. He will establish a pattern of dealing or business and will not usually deviate from that unless he has a very plausible explanation to hand. It is therefore necessary to have practices and standards that are relevant and appropriate to the different types of business.

Scope of KYC information

3.7
We were surprised that details of occupation and employment are considered relevant only for personal bank current accounts and that sources of wealth or income are considered particularly important within a private banking relationship. We would be interested to hear what these assessments were based on.

Very few clients are prepared to disclose details of their net worth to a financial institution. Customer privacy is mentioned in paragraphs 3.21 and 3.22. It is not just firms that must respect these rights, but also those responsible for drafting anti-money laundering rules and regulations and for enforcing them.

Why firms may have existing customer information.

3.8
While we are aware that there are exemptions in the Data Protection Act to enable data to be used for the purposes of fighting crime, there is every possibility that firms could find themselves in breach of the Act if, for anti-money laundering purposes, they use personal data of people who are not suspected of committing a crime or of being money launderers.

We would welcome clarification from the FSA on the interaction between money laundering requirements and the Data Protection Act. The statement in paragraph 3.23 that "we do not consider that data protection considerations constrain the effective use by firms of KYC information to meet legal or regulatory requirements" does not explain how it has reached this conclusion. We urge the FSA to discuss the issue with the Data Commissioner and issue a clear explanation on the interaction between the two sets of requirements.

We think the last sentence in paragraph 3.8 states only one side of the effect of the objective test under PoCA. The other is that the objective test makes actual information or knowledge that the firm has irrelevant. What is relevant is what information or knowledge the firm should have had in order to decide whether or not a firm has grounds for suspicion.

Some practical issues

One of the most vexing issues that many firms have to deal with is the uncertainty over the requirement for one regulated firm to verify the clients of another regulated firm. Discussions between all the trade bodies, the FSA and the Treasury have been going on for over a year without any clear resolution. This affects a great number of firms, causes large unnecessary costs through repetition, is a prime generator of frustration and generates a great deal of ill-feeling and inefficiency.

We will not repeat the detail of the arguments in this response, but this is a subject we believe the FSA should consult on further and we are disappointed to note that it has not done so in this paper.

3.16
From the customers' perspective, this is strong support for our suggestion that there should be a single entry check for every individual who enters the world of financial services. A bank would usually carry out this check of identity and address, as that is usually the first point of entry into the system.

Each organisation would have to decide how much more KYC information (i.e. over and above the proof of identity and address) it would need for its purposes. The requirement for multiple checks of identity are not well understood by the customers, and in reality add little value and are not likely to deter the determined criminal, but they do present a very real inconvenience the innocent.

3.17
We agree with the statements that "under a risk-based approach, it will not be appropriate for every service supplier to know their customers equally well" and that "firms' information demands need to be proportionate and capable of being justified to customers". We would welcome the inclusion and recognition of these statements across all divisions of the FSA and not just in the Policy areas.

Anti-money laundering monitoring

The FSA has stated clearly on a number of occasions that it has no intention of making automated monitoring mandatory. It also states in paragraph 4.2 that the Paper deals with both automated and non-automated monitoring. We agree with this approach. Automated systems can be very useful in some firms and for certain types of business, but they are certainly not appropriate for all businesses.

4.2
It is doubtful in most cases whether monitoring will enable a firm to "detect and address circumstances that suggest their products and services may be being used to launder money". Monitoring, whether it is automated or non-automated, is based on models which use set parameters and criteria to highlight the unusual. Most determined money launderers will be well aware of this and will know that to avoid detection they need to establish a pattern of business and ensure that they do not deviate from that pattern.

Good practice standards

4.5
The FSA must take care when quoting the JMLSG Guidance Notes as authority. The Guidance Notes are by their nature a derivative document. They are not a body of rules, nor are they a primary source of anti-money laundering requirements. They seek to give guidance on existing rules and requirements. The reason they contain guidance on monitoring is because in practice firms are required to monitor their business for anti-money laundering purposes.

The present Guidance Notes were written before the JMLSG was reconstituted. The new JMLSG with its wider and more diverse membership has not yet discussed the merits of transaction monitoring, nor its actual value in detecting money laundering.

Firms are required to report the suspicious, not the unusual. As monitoring will only detect the unusual, it would have been more useful at this stage to have a full investigation into the actual real benefit that monitoring and reporting brings to the protection of the firm and the industry and the fight against money laundering and other financial crime.

It was difficult to understand what is meant by the phrase "different to their peers". If the FSA means that firms should be comparing the nature of their customers' business with business conducted through other firms, that would be next to impossible or at least extremely unlikely. If the FSA means that customers should be compared with each other, it is difficult to see how this could aid any anti-money laundering effort, as the nature of the service many of our members offer and indeed are required to offer, is advice tailored to the individual needs of the individual customer. We would welcome clarification from the FSA.

Industry practice

4.7
This statement is made in isolation and no conclusion is drawn. The use of the word "but" would seem to suggest that the FSA considers automated systems to be superior to staff vigilance complemented by exception reporting.

We suggest it is inappropriate, however, to make such a judgement, even by implication, in a paper in which one of the topics is the efficacy of various types or methods of monitoring. For some businesses automated monitoring may prove useful (if not necessarily for anti-money laundering purposes), but for many of our members automated monitoring would serve no purpose at all. For some firms every transaction for a client would probably be considered unusual and no monitoring programme could replace the human judgement needed to monitor that type of business.

Reasons for increased industry interest in monitoring

Changing business methods.

Monitoring its business will not enable a firm to detect what business its clients are doing elsewhere. We question whether this "propensity of customers to change service providers and to have multiple service providers" has really "increased the industry's focus on anti-money laundering monitoring. If the FSA has any evidence to support this statement, we would be very interested in seeing it.

Increased industry risk awareness.

It is undoubtedly true that the industry has become more sensitive to reputational and particularly the regulatory risks and this may have increased the industry's focus on anti-money laundering monitoring. However, this increased focus is also as a result of many firms questioning the benefit of the current monitoring requirements for anti-money laundering purposes.

They consider that the risk of reputational and regulatory risk has increased, and one of the reasons for that is that they are required to carry out monitoring, but they question whether monitoring will ever enable them to detect a money launderer or a money laundering transaction. A money launderer will probably only ever be caught by those investigating the predicate crime tracking the money from the other direction. In which case the firm will probably suffer regulatory action and reputational damage despite its best efforts to monitor its business.

Terrorist finance

Terrorist finance does not fit easily into the anti-money laundering requirements. The sources of the finance are often otherwise respectable people or organisations, conducting legitimate business through firms. It would probably be impossible for a firm to spot customers providing terrorist finance through transaction monitoring. It is extremely unlikely that any transfers of funds would go direct to a terrorist or terrorist group, so the firm would not even detect them through monitoring transfers of funds either.

It seems a little strange to mention the use of the sanctions list in this section, as it would appear to be more related to KYC requirements.

There needs to be a full investigation into the role firms can be expected to play in relation to terrorist finance, the use and application of the sanctions list. The present arrangements place an unrealistic burden on firms.

Monitoring processes

We particularly welcome some of the statements in this section, particularly that "it is the individual firm that is best placed to identify what is unusual" and that "the unusual is not the same as the suspicious".

However, some of our firms report that some FSA staff seem unclear about this difference between unusual and suspicious- a message we have been trying to get across to the FSA for some time. We are pleased that those in policy have recognised these truths, but we would ask the FSA to ensure that other divisions such as surveillance and enforcement take the same approach.

Some practical issues

4.18

The last sentence in this paragraph contains the crucial statement: "the overall benefits significantly depend on SARs making a material contribution in practice to the fight against crime and terrorism". This raises two related issues.

If studies show that SARs actually make no material contribution to the fight against crime and terrorism, this would mean that the reporting regime is not working and alternatives should be explored.

Firms suspect that the reason there is not a higher success rate is that the public sector bodies, NCIS and the LEAs, are not provided with the funds or resources to carry out their duties properly. We are aware that NCIS has restructured itself to handle the SARs more efficiently and we commend them on this. However, anecdotal evidence also suggests that economic crime is not set as a high priority for most police forces, with the result that many forces are not able to investigate reports unless they involve substantial amounts of money.

The issue is therefore not one of cost, but of cost benefit analysis on one hand and balance of spending, effort and input between the public and private sectors on the other. Firms are not looking for the lowest cost option: they are looking for one where their costs are reasonable, proportionate and justifiable. We would like to see equivalent priorities and resources given to the relevant public bodies.

4.20

In this paragraph the relationship between monitoring and identification is addressed. This discussion is continued in paragraphs 4.22 and 4.23.

We feel that this is a meaningless debate. The amount of resources a firm commits to one will not necessarily effect how much it spends on the other. Shortcomings in identification of clients will not be rectified by increased monitoring of the business those clients conduct. As this paper acknowledges, there can be little effective monitoring without comprehensive KYC information, including identification details.

The real issue underpinning this is that there are serious problems with both requirements in the context of detecting and preventing crime. The methods of verifying identity and address are flawed and can be easily circumvented by professional criminals. Monitoring is based on models, so all a criminal has to do to avoid being caught is to establish a pattern and not deviate from it.

The real issue is therefore not whether increased monitoring can make up for deficient or less rigorous identification procedures or vice versa, but whether either monitoring or identification makes any "material contribution in practice to the fight against crime and terrorism". If they make no such material contribution, then there is no sense in asking firms to continue to conduct these processes for anything other than their own commercial and risk management purposes. (This may of course call into question the value of the reporting regime itself, but that is worth exploring as well).

OPTIONS AND QUESTIONS

5.1
As we have said in the paragraph above, the main issue relating to KYC and anti-money laundering monitoring is whether either of them makes any material contribution in practice to the fight against crime and terrorism, but this is not explored in this paper.

5.2
The FSA states that "too many firms do not take the basic steps of identifying...their own specific money laundering risks..." The FSA should support this assertion with information about the numbers and types of firms it has found to be failing in this regard. It would also be helpful to include descriptions of the steps that the firms had failed to take.

Options

We agree with DP22 in that the options should not be mutually exclusive. The way the four options are worded and explained means that elements of all of them would be useful.

In addition, the FSA has subsequently announced that it is considering replacing the specific rules in the Handbook with high-level principles or reference to existing principles and requirements elsewhere in the Rule Book. APCIMS would welcome this approach, but it would seem to make the options in the Paper meaningless.

We also consider that in addition to the options provided, one body should co-ordinate a review of the entire framework of anti-money laundering provisions and requirements and the FSA is probably best placed to play this role. The review should ensure that the anti-money laundering framework in the UK is truly effective and that requirements on firms are reasonable, truly risk based and stand up to cost benefit analysis.

<u>Option 1 – include in the Handbook specific rules and/or guidance on KYC and/or monitoring.</u>

(a) New specific rules: some firms or sectors may well welcome this, as it could provide more certainty where there is so much uncertainty about what a risk-based approach means in practice and what the impact of the objective test will be.

(b) New specific guidance: This could also be valuable, but the FSA would need to co-ordinate its guidance with any guidance issued by industry.

(c) Extend the specific link between ML and the Guidance Notes beyond identification to cover (at least) KYC and monitoring: this would bring the FSA rules in line with the provision in PoCA and the Money Laundering Regulations which requires the courts to take a firm's compliance with the Guidance Notes into account when assessing its performance under the Act and the Regulations. Many assume that in practice the FSA already takes account of the whole of the Guidance Notes.

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

Currently, there is no widely used effective risk-based approach to anti-money laundering. There are now so many detailed provisions contained in so many bodies of rules and pieces of legislation, and the risk of getting anything wrong is so great, that in practice firms tend to follow a risk averse approach, adhering to maximum requirements rather than trying to attempt to apply a risk-based approach. Defensive behaviour has sadly become the norm.

The FSA assesses the risk that firms pose to its statutory objectives. As money laundering and financial crime in the wider sense is considered such a high risk by the FSA, firms are obliged to give it the same high priority regardless of the actual risk money laundering poses to the individual firm

If the FSA is going to follow option 2, it will have to stop assessing firms on the basis of the threat they pose to the FSA and it will have to accept the firms' own risk assessments. Only then will any guidance given under option 2 have any real meaning and benefit.

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

This option could only be followed if (c) in option 1 were applied as well.

We reiterate the point that the Guidance Notes are reactive in the sense that they are guidance on primary source material and there is some risk in developing the Guidance Notes to go beyond that. The Guidance Notes themselves should not introduce new requirements, as they then take on some of the characteristics of a rule book, which they should never do.

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

This is the option that many firms would recommend. It would seem to be a good idea to leave ML unchanged, especially in light of the fact that there will probably be a Third Money Laundering Directive from the European Commission next year. However this option also

Questions

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

The answer is obviously that they are essential for the firm to meet its obligations. The important part of the question is whether the collection of KYC information (including identification) monitoring can have any impact at all on money laundering and other financial crime. In other words if firms are expected to detect and prevent money laundering and other financial crime, are the tools they are required to use adequate and suitable for the job?

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

This is a crucial question and we would be very interested to hear the FSA's answer to it!

Firms face two major risks in relation to money laundering: the risk of being used by a money launderer and the risk of punishment by the FSA if it fails to meet regulatory expectations.

The answer to the question should be that firms deal with the risk of actually being used by a money launderer. Every firm should assess the risk it faces from money laundering based on a matrix of clients, products and services and geographical spread. It should then design systems and controls appropriate to its business and apply its resources appropriately. In doing this, the firm would be protecting itself against use by money launderers and would, almost as a consequence, find itself in compliance with its legal and regulatory obligations.

In practice, however the reverse happens. The risk that firms really manage is the risk of regulatory action by the FSA. There is little hard evidence to show that gathering KYC information and monitoring the customers' business has any real effect on money laundering. What firms do know is that if the FSA finds that they do not have robust systems, controls and procedures in place, they face severe punishment, heavy fines and reputational damage, even if no money laundering has actually taken place.

In effect firms follow the FSA's assessment of risk, rather than their own. The FSA's risk assessment of each firm is based on the threat that a firm and its business pose to the FSA, rather than the actual threat that the firm faces from money laundering.

While the FSA continues with its risk to objectives approach and while firms are subject to so many detailed and often contradictory requirements, with the threat of severe penalties for any mistake, it is unlikely that firms will pursue a truly risk-based approach to money laundering.

This Proceeds of Crime Act makes it even less likely that firms will pursue a risk-based approach. PoCA introduces an all crimes provision, with no de minimis and contains an objective test of behaviour, which is unusual in criminal law. Many firms and authorities on money laundering consider PoCA to be incompatible with a risk-based approach.

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

This question should surely be directed to the agencies rather than to the reporting institutions.

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

This is the study the FSA should either conduct or co-ordinate. It is difficult to establish the costs directly attributable to these requirements, though there are some academics who are working on the problem. What is clear is that many firms feel that the amount of time and resources they devote to anti-money laundering is disproportionate to the risk that they will actually be used by a money launderer.

The benefits are also difficult to assess and probably impossible to quantify. As we have said above, it is impossible to measure the extent of financial crime, and it is therefore impossible to quantify the effect that KYC and monitoring requirements have on financial crime.

At best, firms feel that they carry out these measures as part of their duty as good citizens. They do the best they can with inadequate tools to protect their own business and reputation and that of the industry as a whole. At worst, firms feel that what they are doing is a waste of time and resources and that KYC and monitoring will achieve little or nothing. This feeling is compounded by the fact that financial crime appears to be very low on the list of priorities for many of the public sector bodies, with the result that many of these bodies remain under-resourced and unable to play their part in the framework.

Firms are concerned about costs, but they are not looking for the lowest cost option. They are willing to commit resources, but they want to be part of a system that is truly effective, not just cheap.

Q5: Which options presented do you prefer and why?

See the discussion above.

APCIMS
EASD
Working for the Investment Community

ASSOCIATION OF PRIVATE CLIENT INVESTMENT MANAGERS AND STOCKBROKERS MEMBERSHIP 2003/2004

Ordinary Members

Abbey National – City Deal
Aberdeen Asset Management Plc
ADM Securities
American Express Financial Services Europe Ltd
Anderson Charnley Ltd
Andrews Gwynne & Associates
S P Angel & Co
Ansbacher & Co Ltd
Arbuthnot Fund Managers Ltd
Arnold Stansby
Ashburton (Jersey) Ltd
Astaire & Partners Ltd
Barclays Private Bank Ltd
Barclays Stockbrokers
Barratt & Cooke
Berry Asset Management Plc
Blankstone Sington Ltd
Brewin Dolphin Securities Ltd
Brook Partners Ltd
Brown Brothers Harriman
Brown Shipley & Co
BWD Rensburg
C. Hoare & Co
Cambridge Investments Ltd
Campbell O'Connor & Co
Cardale Stockbrokers Ltd
Carr Sheppards Crosthwaite
Cave & Sons Ltd
Cazenove Fund Management Ltd
Charles Stanley & Co Ltd
Cheviot Capital Ltd
Chiswell Associates Ltd
Christows Ltd
City Asset Management Plc
Close Fund Management Ltd
Close Private Asset Management Ltd
Collins Stewart (CI) Ltd
Comdirect Ltd
Credit Suisse (UK) Ltd
Cripps Portfolio Ltd
Cunningham Coates Ltd
Davy Stockbrokers
Deutsche Bank Private Banking
Direct Sharedeal Ltd
Douglas Deakin Young Ltd
Dryden Wealth Management Ltd
Edward Jones Ltd
Ely Fund Managers Ltd
E*Trade Securities Ltd
Everys Solicitors
Farley & Thompson
F H Manning Financial Services Ltd
Fiske Plc
Fyshe Horton Finney Ltd
Generali Portfolio Management (UK) Ltd
Gerrard Ltd
Gibraltar Asset Management Ltd
Goy Harris Cartwright & Co Ltd
Halifax Share Dealing Ltd
Hargreave Hale Ltd
Hargreaves Lansdown Stockbrokers Ltd
Harris Allday
Hedley & Co
Hichens Harrison & Co Plc
Hill Martin (Asset Management) Ltd
Hill Samuel Bank (Jersey) Ltd
Hoodless Brennan & Partners
HSBC Bank Plc, Stockbrokers
HSBC Investment Management
I A Pritchard Stockbrokers
Iain Nicholson Investment Mgmt Ltd
IDealing.com Ltd
iimia Plc
Insinger Townsley
Irwin Mitchell
James Brearley & Sons
James Sharp & Co
J M Finn & Co
J O Hambro Investment Management
John Scott & Partners Investment Mgmt
J P Jenkins Ltd
KAS Bank N.V.
KBC Peel Hunt
Killik & Co
Kleinwort Benson Private Bank
Laing & Cruickshank Investment Mgmt
Leopold Joseph & Sons Ltd
Lloyds TSB Stockbrokers Ltd
London York Asset Management Ltd
M D Barnard & Co Ltd
Merrill Lynch Investment Managers
Morgan Stanley Quilter
Murray Beith Murray Asset Management
NatWest Stockbrokers Ltd
NCL Smith & Williamson
Nichols Williams Durrant & Co Ltd
Noble Asset Managers Ltd
Norwich & Peterborough Sharedealing Services
ODL Securities Ltd
Pershing Ltd
Philip J. Milton & Company
Pilling & Co
Premier Asset Management
Principal Investment Management Ltd
Private Client Department, Baring Asset Management Ltd
Ramsey Crookall & Co Ltd
Rathbone Investment Management Ltd
Raymond James Investment Services Ltd
Redmayne Bentley
Reyker Securities Plc
Rothschild Private Management Ltd
Rowan Dartington & Co Ltd
Royal Bank of Canada Investment Mgmt
Ruffer Investment Management Ltd
Russell Wood Ltd
Saga Investment Direct
Savoy Investment Management Ltd
Seymour Pierce Ltd
The Share Centre
Shepherds Financial Ltd
Shore Capital Stockbrokers Ltd
Speirs & Jeffrey Ltd
Standard Bank Stockbrokers Jersey Ltd
TD Waterhouse
Taylor Young Investment Management
Teather & Greenwood
Thesis Asset Management
Thornhill Investment Management Ltd
Tilman Asset Management Ltd
Tilney Investment Management
Truro Stockbrokers
Vartan & Son
W H Ireland Ltd
Walker, Crips, Weddle, Beck Plc
Williams de Broe

Total: 135

Associate Members

ADP Wilco
Advent Europe Ltd
Aitken Campbell & Co Ltd
Archipelago Europe Limited
Bank of Scotland
Barlow Lyde & Gilbert
BPP Professional Education
Bristol & West
Business Architects International
Cantor Index Ltd
City Compass
City Consultants
City Index Ltd
ComPeer Ltd
Consort Securities Systems Ltd
CRESTCo Ltd
Deloitte & Touche
The Depository Trust & Clearing Corporation
Dresdner Kleinwort Wasserstein
Exact Technical Services Ltd
Exchange Data International Ltd
Financial Tradeware Plc
Fortis Clearing London Ltd
HSBC Bank Plc
Information & Trading Systems Ltd
Instinet Europe
Investmaster Group Ltd
Investment Sciences Ltd

JHC Plc
Knight Securities International Ltd
Knowledge Technology Solutions Plc
KPMG
Lawshare Ltd
London Stock Exchange
MBA Systems Ltd
Merrill Lynch International
Minnie Business Systems Ltd
Misys Asset Management Systems Ltd
Monument Securities Ltd
OFEX Plc
OM Technology
On Bourse Ltd
Optima Financial Systems Ltd
Penson Worldwide Settlements Ltd
Performa
Peter Evans & Associates Ltd
Proquote Ltd
Pulse Software Systems Ltd
R A McLean & Co Ltd
Royal Bank of Scotland – Financial Institutions Group
S J Berwin
SAM Systems Ltd
Securities Institute
Speechly Bircham
Summerson Goodacre
State Street Bank & Trust Company
The Stuchfield Consultancy
SunGard Investment Systems UK Ltd
SWIFT
Syntegra
Talos Securities Ltd
Telekurs Financial
Thomson Financial
Virt-x Exchange Ltd
Willis Limited
Winterflood Securities Ltd

Total: 66

Affiliates

Attorners at Law Borenius & Kemppinen
Brown Rudnick Berlack Israels LLP
Chaintrier & Associes
Covington & Burling
Credit Agricole Indosuez Cheuvreux
De Bandt
Doughty Hanson
Fontana e associati
Gomez Acebo & Pombo
Hannes Snellman Attorneys at Law Ltd
Houthoff Buruma
Lombard Odier & Cie
Plesner Svane Gronborg
Prager Dreifuss
Puilaetco
Santilli e Associati
Solidarietá of Finanza
Sullivan & Cromwell
TELFA
Travers Smith Braithwaite
Verband unabhängiger Vermögensverwatter
Wedlake Bell

Total: 22

The Financial Services Authority

Reducing Money Laundering Risk;

Know Your Customer and anti-laundering money monitoring

Discussion Paper 22

Response of the Law Society

Introduction

1. This response has been prepared by the Law Society with the assistance of the Society's Money Laundering and Serious Fraud Taskforce. We welcome the opportunity to respond to this discussion paper for two reasons. Firstly some firms of solicitors conduct mainstream investment business and are therefore subject to the Money Laundering Sourcebook and therefore any changes in the FSA's rules will be directly relevant. Secondly, we are interested in contributing to the debate on Know your Client issues from the broader perspective, both for the legal profession and for society as a whole.

2. We are concerned that the burdens being placed on solicitors and others are being seem to be excessive and out of proportion with the potential benefit. Solicitors are concerned that the UK regime is the most onerous in Europe and that goes far further than was required by the Second Money Laundering Directive. This raises important competition concerns. This could damage the standing of the City of London.

3. Solicitors already face significant new requirements in the field of money laundering. The introduction of part 7 of the Proceeds of Crime Act 2002 in February 2003 is having an enormous impact on firms, in relation to training, understanding the new legislation and in particular the new "objective" test. In addition, firms will have to consider the new Money Laundering Regulations 2003 very carefully to ensure that they implement any necessary changes to their systems, controls and procedures. Some firms will have to ensure compliance with any changes in the FSA's rules as well.

4. In our response to CP46, we expressed concern that the introduction of the FSA's Source Book would create a separate but parallel regime for firms to contend with. Problems will arise if there are any inconsistencies between the two regimes. The result would be that firms comply with the money laundering regulations and Law Society Guidance but could still be disciplined by the FSA for breaching the Money Laundering Source Book. This danger was particularly acute if the FSA's proposed Rules for client verification had been implemented. Similar concerns were raised by others. This led to the FSA concluding:

   > "..the overriding message of the concerns was that, by including in our Rules the proposed amount and nature of the detail about identification methods, we were creating confusion and risk as to the respective roles of our Rules and the JMLSG Guidance Notes which was contrary to a stated aim of CP46. "

5. The FSA decided not to proceed with detailed verification rules and commented that the JMLSG Guidance Notes were a key factor in this decision. We believe that the same logic applies equally to the proposals in relation to KYC. The Law Society

has published its own detailed Guidance, a copy of which is attached. . This includes detailed guidance on client verification and a risk based approach. We are concerned that this guidance will be undermined by the introduction of the FSA Rules on KYC. We are also concerned that a risk based approach should be taken and that too prescriptive a requirement will be over burdensome and disproportionate for the potential benefit. It is important that firms make a proper assessment of a case rather than relying on a tick box or check list approach which may result in them overlooking a vital piece of information.

6. We are concerned at the "one size fits all approach" and believe the money laundering risks facing solicitors are quite different from, say, a bank. Solicitors often have longstanding relationships with their clients and pride themselves in giving commercial advice and thus their understanding of their clients business. In most cases solicitors meet with their clients on a regular basis during the course of their relationship. Moreover, professional conduct obligations and duties in contract and tort require solicitors to be familiar with their client's affairs in order to provide services competently and professionally.

7. The problems cannot be overcome by limiting the scope of any KYC requirement. A firm of solicitors offering investment management services will often attract clients from the private client department. That private client department will have substantial information about the client from acting on the case, for example, the trust lawyer will know why the trust was set up, who the trustees are, where the money has come from etc. The level of information available to the trust lawyer will be completely different to the information available to a stockbroker meeting a client for the first time.

8. We feel that the issues raised in the discussion paper are very useful as they are likely to help firms to assess the risks within their own business.

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

9. In our view, the existing regulatory requirements would appear to be sufficient. Firms who are subject to the FSA's rules and the Money Laundering Regulations will have to satisfy the requirement to identify their clients.

10. Over and above the identification requirements, firms should be able to make the assessment themselves as to what types of KYC may be required in what circumstances. We do not believe that rules on KYC are necessary for the reasons set out in paragraph 6 above.

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

11. Firstly, we welcome the idea of a risk based approach, as this seems far more sensible than the current position where, for example, verification is sought in all circumstances, regardless of whether there is an actual requirement or whether there is any risk of money laundering. As to how firms should pursue a risk based approach, this will depend on the individual sector and guidance on the sorts of issues to consider would no doubt be helpful. The issues that are relevant to solicitors are set out in paragraph 6.Firms will need to assess the impact and costs of monitoring for their firm.

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

12. The section in the discussion paper considers more what types of monitoring are available to firms and it is quite difficult to answer this question as we are not clear as to the FSA's thinking behind the question. The issues about usefulness of reports etc to law enforcement are perhaps issues to be considered in terms of the overall UK strategy to combat money laundering. The KPMG review, of course, considered the issues in relation to the SAR process and the Government Taskforce is now taking those issues forward. It is important that the relevant bodies are clear as to their role in the regulatory regime.

13. In any event, this question is more one for law enforcement, although it is important for the credibility of the whole regime that firms are not obliged to over report. If a firm is concerned about a particular transaction, a report will be made to NCIS, who will then pass the information to the law enforcement agencies.

14. We would comment that the Law Society's Practice Standards Unit will be routinely monitoring compliance with the regulations and Forensic Investigations, which includes the Investment Business Unit, will be investigating all breaches of those regulations. There is a memorandum of understanding between the Law Society and the FSA for exchange of information.

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

15. It is difficult to answer this question as the costs and benefits will vary according to firms and according to sectors. A prescriptive approach in relation to KYC and monitoring is likely to result in unnecessary costs for the financial sector. There will then be a knock on impact to customers and this may not have any real benefit. We agree with the FSA that firms' information demands need to be proportionate, appropriate and discriminating, and capable of being justified to customers. We are concerned that a prescriptive approach would have a

detrimental effect on the UK's competitive position in providing financial services.

Q5. Which options presented to do you prefer and why?

16. Option 4 – We believe that to impose further requirements on the financial sector at the moment would be unreasonable and could result in the imposition of requirements that needed to be changed in the light of experience.

17. The Proceeds of Crime Act should be given time to bed in. There are many legal issues and questions arising from the new legislation. In addition, firms will have to implement any changes required by the Money Laundering Regulations 2003. As the FSA comment, there may also be changes to the SAR process in the light of the KPMG review. We feel that firms should be given the time to consolidate and absorb the recent and prospective changes.

The Share Centre

DP 22 – Reducing Money Laundering Risk

Please find below our comments.

3.5. Mandatory information regarding individuals 'might include the date of birth, occupation, employer and National Insurance number'. At present there is no requirement to obtain all this data, whilst there is a requirement, under Data Protection, only to hold relevant data. As an execution-only broker, we have not seen the need to obtain this data for all clients as a matter of course, though if obtained it is, of course, recorded. If these details are to become mandatory, we would ask for a commencement date to the requirement so that we would not be penalised for not being able to provide all these details for an account opened in 1996, for example.

5.5… Option 1

We would prefer specific rules to specific guidance, especially as the rules would contain an element of flexibility in being risk-based. Also, the rules would be complemented by guidance, which would mean that the link between ML and the Guidance Notes would need to be extended. It would be most useful if the Guidance Notes also took a risk-based approach, detailing what would be reasonable in different circumstances. Whilst we appreciate the industry flexibility a risk-based approach brings, the 'tick box' approach still has an appeal: most cases will be looked at with at least some element of hindsight, so the more objective the criteria to be followed, the easier it is to assess action taken.

5.12. Option 2

This appears to be unnecessary as it seems to be a duplication – '[firms] are already required under our Handbook to establish and maintain effective systems and controls for countering the risk that they might be used to further financial crime, which includes money laundering.' (FSA briefing note July 2003)

5.13… Option 3

We look to the Guidance Notes for clarification, so an update to the Notes would no doubt be taken on board by the industry. However, we are of the opinion that it is not beneficial for FSA to get its point made 'through the back-door' of the Notes. Whilst FSA may have due regard to the Notes, it seems to us that regulation and industry guidance should be kept separate.

5.15. Option 4

On the face of it, this is the best option. However, in 2 years' time there will no doubt be other reasons for delay, other developments occurring. Rather than another review in a year or so, we would prefer a longer transitional period.

5.16. Risk considerations

As a company, we are looking at money laundering risk from the point of view of both product and client. Whilst a lot of monitoring is still manual, we are relying more and more on exception reports to identify clients and/or transactions that are either unusual or exceed our internal criteria.

It is still very difficult to assess how a firm is doing with regards to money laundering without any specific feedback regarding prevention, detection and monitoring: it seems the industry bears the cost, but as to who gets the benefit, even if there is a benefit… And whilst a risk-based approach seems sensible, any launderer worth his salt will be aware of this, which could lead to low risk products becoming high risk!

Transparency

It can be difficult to work out what exactly is required, especially as the goal posts are continually moving. Where clarification on a point is required, it can be difficult to get clarification and/or guidance. And it is very difficult, in complying with the Regulations, not to potentially launder money, tip off or contravene the Data Protection or Race Discrimination Acts, which at times all seem to contradict each other. We cannot, in all confidence, say we know what is expected from us from all quarters.

Q1 The collection of KYC information is necessary in meeting legal, regulatory and reporting requirements. The question is, to what extent is KYC relevant and how should KYC requirements differ from product to product? From experience, it would seem easier to obtain a platinum credit card with a credit limit of £6,000 than to sell shares to the value of £700 on an execution only basis. This seems totally illogical and without justification.

Where a client is provided with an advice service of any sort, then KYC is of importance, but with the execution only or 'dealing at a distance' type of business, detailed KYC seems inappropriate. And the problem with KYC information, as opposed to pertinent information, is that a company cannot insist that it is continually updated, leading to out of date data being held, contrary to the Data Protection Act.

Whilst, in theory, transaction monitoring should identify suspicious transactions, it can be very difficult to differentiate between the out of character, the stupid, the mistake, the change of mind, the one-off, the unusual, the unexpected and the criminal. At some point in their history, all laundered funds hit the banking system; banks are generally a lot more helpful to each other than they are to others within financial services and banks have access to a lot of KYC information (through mortgage payments, direct debits, credit card repayments etc.). A way forward would therefore seem for the major KYC requirements to lie within the banking system itself. The vast majority, if not all, SARs will contain bank details, providing a way in to the bank's KYC data for the law enforcement agencies.

With all KYC gathering, there should be a limited number of mandatory fields, with the remaining fields for completion if required. The majority of applicants will probably complete the latter, with the former being available for those who are very unhappy with the amount of information held about them by companies and who object to providing anything that is not on a 'need to know' basis. There is a very real danger that, even if there isn't a privacy back-lash, there will be a reluctance to provide, and keep providing, information that has no real relevance to the product in hand.

Q2 It seems that risk should be assessed on a combination of product and client. However, this can be difficult. If, for example, a number of frauds are seen to come from people with Martian sounding names, it would surely be a contravention of the Race Discrimination Act to treat these people differently to anyone else, even though they seem to be in the high risk category.

Within any risk-based approach, the size of the investment is going to be considered: it is not cost effective to effect a detailed KYC interview for a one-off sale of £1000 worth of Abbey National shares and it is always assumed that launderers invest in large amounts. However, as the risk-based approach becomes well known and established, launderers may well start to change their investment strategy to compensate – low risk could become high risk!

It should never be forgotten that any launderer worth his salt will know the regulations better than most MLROs. It is therefore very difficult to implement a robust risk-based approach, especially as we seem to get no feedback as to current trends in criminal activity, standard ploys that are used etc.. An awful lot of industries and agencies are involved with AML, yet there appears to be very little joined-up thinking and a general reluctance to share information and experiences. This just plays into the hands of the launderer and makes risk assessment that much more difficult.

Any risk-based approach must be regularly assessed to take into account any changes and developments in technology, industry bench-marking etc.. It is accordingly something that changes over time. With laundering cases being looked at by the courts with the benefit of hindsight, there is the real danger that the details will be looked at through the current mind set, rather than that prevailing at the time. A risk-based approach, with no set criteria, can therefore leave firms feeling very vulnerable.

Q3 Reports are completed by all sorts of companies, so a 'one size fits all' approach as we have at the moment doesn't work that well; perhaps trade bodies could be involved in the design of the reporting forms.

Q4 With regard to the detection and prevention of financial crime, the industry doesn't know, and at present has no way of knowing, the benefit of ID verification, KYC and/or monitoring. As a firm, in the past we have found it difficult to get police interested in financial crime (specifically fraud) and have lost contact with the suspected perpetrators as a result. It certainly seems that firms have all the cost and none of the benefit!

For advisory clients, KYC is obviously of great importance, but there is no change here; it always has been. For execution only clients, the benefit of KYC is a lot less obvious: indeed, complicated application procedures can be detrimental in attracting this type of client.

One of the possible consequences of KYC could be the use of this information for marketing purposes: while this could lead to a more targeted marketing policy, it could also lead to a lot more junk mail and dissatisfied clients. Should it be a requirement that KYC data is only available for KYC purposes and cannot be used for marketing purposes?

What would be of great benefit to all participants would be a centralised database, where any company covered by ML regulations could check for ID, inclusion on the Sanctions List etc.. Since this site would be for use by the industry only, any audit trail could assist with monitoring: indeed, the same person applying to many different institutions at the same time could itself generate a suspicion report.

The use of Experian etc. can give rise to concern among clients since, as I understand it, a Money Laundering check creates exactly the same log as a credit reference check. There are already two versions of the Electoral Roll, so there is no reason why the same could not apply for ID checks too.

Q5 As can be seen from our comments above, our preferred option is Option 1. Consistency of approach across the industry makes things easier for the client, enables firms to feel fairly secure in their procedures, gives the courts and law enforcement agencies a benchmark from which to assess a firm's compliance and gives comfort to MLROs, who are aware that their decisions are likely to be looked at (and judged) with the benefit of hindsight. There is, however, still a place for a risk-based approach within this option, with different rules for different types of business and client.

Thinking about Crime

Q1 = The collection of KYC information (above and beyond standard customer identification verification) is crucial to reducing money laundering risk. The law requires individuals to report suspicions of money laundering, and I am firmly of the opinion that suspicion can be generated only by behaviour that is out of the ordinary. And extraordinary behaviour can be spotted only if you know the ordinary, abnormal only if you know the normal, and unusual if you know the usual. A customer's projected behaviour is not communicated in basic identification checks: it is only through more thorough KYC checks that an institution can start to build a picture against which to compare future behaviour.

And if KYC is the start of the process, monitoring is the continuation. There is no point collecting a wealth of KYC information at the start of a relationship and then not maintaining that information so that it is current and relevant.

It would be of great assistance to regulated firms if the collection and maintenance of KYC information were a legal or regulatory requirement, as this would ensure that budget were dedicated to the process. As long as it remains optional, MLROs and compliance departments will fight a losing battle for both money and staff commitment. Q2 = The process outlined in paragraph 2.9 of DP22 seems to me to be ideal. The documentary element should be stressed, to ensure that firms do in fact go through the process. Q3 = I am led to believe by my law enforcement contacts that the most useful information that financial institutions could suppply about their customers and transactions concerns source of wealth and source of funds. Q4 = AML has always been a difficult sell, as it does not increase the profits of those who implement it. It may reduce their losses, but it does not increase their profits. The main cost, I should imagine, will be one of manpower - gathering and recording additional information. There will also be training implications, as staff will need to be made aware of the enhanced requirements.

The main benefits are those outlined in the response to question 1. Anything that makes a financial institution (or whole sector) less attractive to launderers must be welcomed. Q5 = I prefer option 1. As mentioned in the response to question 1, I believe that little will be done on this issue until it is made an explicit requirement. The MLRO will not be able to garner further budget for this initiative unless he can show his board that there is no option but to do so.

From a trainer's point of view, the more explicit and clear the requirements are made, the better. If the matter is left to individual interpretation, this causes confusion for both MLROs and their staff. Each insitution makes its own interpretation, which is a waste of time and effort when the correct interpretation could be made once for everyone. If the MLRO changes, so does the interpretation, and the staff are further confused. We should aim for a crisp set of rules and associated guidance, clearly interpretated by the Guidance Notes. Consent = Yes

----

Remote Host: 213.104.13.33
Remote IP: 213.104.13.33
User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Referer: http://www.fsa.gov.uk/pubs/discussion/dp22_response.html

.

Tipton
Coseley
BUILDING SOCIETY

JJM/KAH

8 December 2003

Mr D Shonfeld
Financial Crime Policy Unit
Prudential Standards Division
Financial Services Authority
25 the North Colonnade
Canary Wharf
London
E14 5HS

Dear Mr Shonfeld

DP22

The Tipton and Coseley Building Society acknowledges and supports the FSA's financial crime objective. Anti money laundering policies are seen as non-competitive but we are aware that different firms interpret the JMLSG guidance notes in different ways particularly where the identification of customers is concerned. This can lead to the public having different experiences in what they are asked for with regard to identity.

Q1.

The level of KYC information necessary will depend on the risk analysis carried out by the firm and the products it offers. If the FSA expands the amount of information needed it should still be on a risk based approach. However, it would be helpful to firms if guidance could be given as to what is expected for different product levels.

Once the information is collected what purpose will it fulfill? To be relevant it needs to be up to date and that is where some sectors of the financial market may have difficulties. Many customers will not have experienced being questioned in the way that will be needed to ensure a level playing field exists and may not wish or be prepared to give the information. Is this suspicious in itself or just a reflection of the fact the public thinks government is becoming too intrusive? If all firms have to collect the same information it will at least show customers it is not just one organisation being "nosy" and, with proper government backed publicity for this type of project, it may make genuine customers aware of why firms need to take such an inquisitorial approach.

The major problem will be in ensuring that information is kept up to date without upsetting customers by regularly trying to update such information. Additionally, costly systems to store the information in an easily retrievable state will be needed.

With regard to monitoring, guidance on what is required is again needed. Is exception reporting as acceptable as fully automated monitoring systems? The cost of monitoring is a concern especially for small organisations (see question 4) but monitoring in some form is a necessary method of ensuring that our responsibilities are met.

70 Owen Street, Tipton, West Midlands DY4 8HG
Telephone: 0121-557 2551 Fax: 0121-557 8570 DX 700152 Tipton
www.thetipton.co.uk

[redacted]

If the reporting process is to work properly then the authorities need to tell the industry what is needed from them to ensure the correct information is captured to be able to form part of the NCIS report so that the quality of such reports meets the required standard.

Q2

Based upon the range of products offered, their customer profiles and guidelines from the authorities!

Q3

Surely this is for the law enforcement agencies to advise us so that we can provide the necessary information.

Q4

The capital costs for a monitoring system for the size of our organisation is around £20,000 with ongoing "maintenance" of £5,000. Add to this the ongoing staff costs to investigate the extra reports that will inevitably be produced we are approximately 1.5p onto our management expenses ratio.

For KYC information, new application forms, system changes and data imaging systems we have a capital cost of around £100,000 with ongoing maintenance and staff costs of around a further £10-15,000 another 3p will go onto our management expenses ratio. The benefits would be a more robust system but on a cost benefit analysis we would find it hard to justify the extra cost.

Q5

We prefer option 4. The industry needs a time of consolidation. We are already committed to the 2003 revised JMLSG guidance notes and a further substantive revision in 2004. The FSA would have the opportunity to feed its views into the 2004 revision if it has concerns that need to be addressed urgently.

General

The likelihood of additional help via the FSA industry training service is welcomed.

It is all very well for the government to give the FSA the objective of reducing financial crime but in reality it gives no help to firms by failing to introduce more robust anti fraud systems itself for example by not putting national identity cards higher up its list of priorities. The government persists in making the financial services industry the unpaid arm of the law enforcement agencies and gives no credit for the efforts made by the industry.

Finally we hope we understand the FSA's regulatory requirements and what you expect of firms but, as ever, the more guidance that can be given to assist us in helping you to meet your requirements the better job we can do to help you.

Yours sincerely

John J Miller
General Manager & Secretary

Turkish Bank

Q1 = Collecting KYC information and actively monitoring account transactions against this is essential if we are to meet the regulatory obligations particularly reporting. Q2 = Firms should pursue a risk-based approach to anti-ML by identifying higher risk transactions and accounts (non-resident accounts; business accounts paying in large amounts of cash, etc.) and monitor these more closely for unusual transactions. They should investigate / question significant transactions which do not fit the norm and record the customer's explanation. By establishing what are typical transactions / account operating patterns for each type of account staff will be able to judge what is unusual and in need of explanation. If the explanation is not credible or raises suspicion and documentary evidence is not available or unconvincing, a report can then be made as required. Q3 = Background customer information and file notes made of meetings / telephone conversations relating to specific transactions and account operations generally. Q4 = The costs to the bank in policing transactions and accounts in this way are difficult to estimate. They include additional staff costs to deal with monitoring and possibly an increase in the number of reports to NCIS. There will also be missed business opportunities (where customers object to providing detailed information). The benefits are: better KYC information (reducing reputational risk exposure); better marketing information (enhancing business opportunities) and fewer defensive reports to NCIS (reducing administration costs). Q5 = Option 1 is preferred as this will make clear the standard of due diligence and control required across the finance industry thereby encouraging a 'level playing field'. The FSA will then be able to take action against those firms not complying thereby encouraging a higher standard of anti – money laundering practice. Consent = Yes

----

.

Virgin Money

Q1 = Both KYC and monitoring are an important part of the overall toolkit for firms to use in their anti-money laundering procedures.

Both aspects need to be tailored to firm's individual requirements, in particular the type and level of monitoring undertaken. It is not feasible for all firms to go to the same extent that the clearing banks need to go to, primarily because of the product types (eg current accounts) that allow simple and seamless flows of funds from the account holder to third parties. Firms that only deal with the owner of the funds, and only allow funds to be passed to the owner of the product are immediately a reduced risk.

KYC information obtained must be driven by the information required by firms to set up accounts, and to verify customers' identity. Firms should not be expected to obtain anything in addition to this purely for anti-money laundering reasons. This could well be deemed to be excessive processing under the Data Protection Act 1998. FSA point to DPA not precluding processing of data where there is a legal or regulatory requirement for the processing. However, as FSA point out, there is currently no legal or regulatory obligation to use KYC information or to monitor for anti-money laundering reasons.

FSA also need to consider their other statutory objectives, particularly maintaining confidence in the UK financial system. This confidence can take several forms, one of which might be that customers prove unwilling to provide data (and therefore purchase products) where they feel this is being used excessively by financial firms.

KYC is essential as part of the reporting process to assess whether any activity is occurring which warrants either an internal or external report. Monitoring of accounts is not, because the Proceeds of Crime Act reporting requirements refer to information in the hands of 'persons'. In this context this refers to physical persons not legal persons, ie individual staff members not financial institutions as a whole, i.e. when an individual staff member obtains information about a person that gives reasonable grounds to suspect, they must report. This is a use of KYC information. However, information in the hands of the firm which does not pass through an individual (eg online transactions) would not be caught by the Act, therefore monitoring for anti-money laundering reasons is not a requirement and so cannot assist with compliance with the Act.

Q2 = At a high level, firms need to assess each of their products and services and the potential for money laundering with the use of each of these. They also need to overlay their customer base particularly in relation to the geographical location. UK/EU only customers should present a lower risk due to these people coming from states which are subject to the Money Laundering Directives. The main area where firms can implement a risk based approach is to the level of verification evidence they require. In terms of KYC and monitoring, again the lengths that firms will go to (particularly regarding monitoring) will depend on the perceived risk presented by the product or customer type. Q3 = Accurate and relevant reports should be seen as the outputs from a robust and successful monitoring process. The law enforcement agencies should not be concerned with the make-up of the monitoring provided it produces information which lead to such reports.
Q4 = FSA have already covered the costs and benefits in the discussion paper. We have nothing further to add to this.
Q5 = Our preference would be for option 2, high level rules & guidance. This supports the existing situation requiring robust risk management across all firms' operations, and allows firms to fulfil their obligations in a less prescribed manner which, in turn, allows a risk based approach. In addition, FSA could make the cross referral to the JMLSG Guidance Notes which would bring a level of consistency to the way firms seek to mitigate risk by way of KYC and

monitoring. We do not feel that this is a considerable shift to the current obligations on firms, and therefore strikes the appropriate balance for the industry, but without sending a message that FSA are lightening their approach to money laundering regulation. Consent = Yes

----

Remote Host: 213.104.10.193
Remote IP: 213.104.10.193
User Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 4.0)
Referer: http://www.fsa.gov.uk/pubs/discussion/dp22_response.html

.

FSA Discussion Paper 22: Reducing Money Laundering Risk

This document is in response to the FSA's Discussion Paper 22 the purpose of which is to stimulate debate regarding two anti-money laundering controls:

1. Know Your Customer ("KYC"); and
2. Monitoring

Visa EU very much appreciates this opportunity to provide input on the Discussion Paper and would be happy to provide further clarification on any of the points raised, if needed.

Discussion Paper 22 raises several options or possibilities but also seeks responses to certain questions. Although Visa EU is not part of the regulated sector, we support and recognise that upholding and improving standards in relation to anti-money laundering controls is of benefit to the financial services industry as a whole. It is also of benefit to Visa EU as we maintain our own high standards with regards to the fight against money laundering.

Visa EU in this response will concentrate on those possibilities that could be considered most relevant from this point of view.

Options 1 and 2

Discussion Paper 22 sets out four possible options. Options 1 and 2 both suggest developing new rules and/or guidance on KYC, monitoring or high level rules to promote better money laundering risk management by firms. These first two options we consider to be unduly burdensome on the industry. Options 1 and 2 in our opinion would impose another layer of regulation on Visa Members in an area which is already highly regulated. This additional layer would not, in our view, provide our Members' customers with any greater level of protection than they are already afforded. Ultimately, the cost of this additional layer of regulation would be passed on to our Members' customers through an increase in the cost of the products offered to them by our Members.

We consider however, that Options 3 and 4 require some further consideration and analysis. We deal below with each option in turn.

Option 3: "leave ML unchanged; rely on the JMLSG Notes"

Discussion Paper 22 proposes that in order to be consistent with the complementary roles of the Money Laundering sourcebook (ML) and the Joint Money Laundering Steering Group ('JMLSG') Guidance Notes: no extra or specific material is required; and that it could be left to the Guidance Notes to meet the financial industry's need for guidance on best practice for meeting legal, regulatory and risk management requirements.

Visa believes that the current Guidance Notes are comprehensive and provide clear directions for both the regulated and unregulated sectors. The Guidance Notes explain clearly the expected standards and also, various rules and laws in relation to anti-money laundering. Whilst the Guidance Notes do not have the force of law, historically they have always underpinned the statutory requirements and have been taken into account when assessing whether the statutory requirements have been complied with. Against this background, given that they are now undergoing a period of review (with new Guidance notes being released this year), it is expected that the new version will mirror current industry practice. For example, the 2003 Guidance Notes are expected to contain different sections for different business sectors including businesses, which have not before come within the Money Laundering Regulations e.g. jewellers and casinos. It is also expected that the new Guidelines will take account of the Proceeds of Crime Act. Although the Guidelines are only guiding principles and do not themselves have the force of law, industry practice has evolved to apply the Guidelines as though they had a statutory basis. On this analysis, Visa EU determines that an additional layer of regulation at this stage is neither necessary nor beneficial to consumers. Option 3 is the most appropriate option.

Option 4: "make no settled decision now and review position again in, say, two years time"

This option differs from Option 3 only insofar as the position would be reviewed again in 2005. This would allow for a longer period of time which the financial sector would have the benefit of experience in applying the new Guidelines.

How should firms pursue a risk-based approach to anti-money laundering? Most firms currently spend a large amount of their resources (money, staff, time) managing their commercial and regulatory risk in compliance with the FSA's Principles for Business (i.e. Principle 3). We would argue that provided firms continue to maintain appropriate internal policies, procedures and controls, which incorporate an effective programme against money laundering this would, we consider, fulfil the proactive approach required to meet FSA's objective of reducing financial crime. For example, internal policies or procedures such as those which most firms have already implemented, should, we feel, be adequate.

The FSA has been proactive in the monitoring of regulated firms and in particular, with respect to firms' KYC and general anti-money laundering procedures. Where it has found non-compliance with the rules, fines have been imposed. It is obvious that the FSA is certainly adhering to its stated objective of reducing financial crime by conducting reviews of firms and their compliance with all anti-money laundering rules. This approach ensures that the FSA continues to satisfy its statutory objectives in particular, the reduction of financial crime.

William Clowes

Q1 = I am fed up with having to provide forms of ID to exisiting Financial Service providers with whom I have dealt with over a number of years. If I was good enough to deal with for the last 10 years or so why do they have to trouble me now (they say FSA Requirements). Q2 = Assess the risk! Do not adopt a blanket approach. You will lose customers (who will then have to go through the whole shooting match anyway with new providers!)who believe their provider knows them when clearaly they do not. Q5 = Minimal intereference. Consent = Yes

----

.

Wainwright Training Management

Q1 = Essential. It should not cause a problem or extra cost to an IFA as it is an intrinsic part of being able to provide financial advice. In order for investigators to follow a trail we feel that the provision of such information, rather than just identification, is important. However guidance is often sort as to exactly how far an Adviser needs to go in establishing the source of funds. Q2 = This is a difficult question to answer. Most small to medium sized IFAs will believe that they are low risk. This is because there are no figures or guidance to show that money launderers target such firms. Q3 = Do not know. Q4 = In terms of general KYC there are no additional ML costs as KYC is a general requirement. However there is an un-quantified cost in collecting proof of identity. It is often seen as a waste of time and complicated, as different providers have different requirements. Some forms of identity are seen as ineffective. A call at the home of a client is often used as proof of residence because it is easy to record. However such evidence does not check that the client actually lives at the address visited and he is unlikely to do so if actually trying to launder money. Q5 = Option 1 (c)

New specific rules would be difficult to draft and undoubtedly would therefore become too cumbersome. This is because of the very different needs of various parts of the industry and the different types of process within those parts, e.g. the simple investment of £100 in a building society account compared with an in depth study of a clients financial circumstances for long term financial planning.

However, guidance in the JMLSG Guidance Notes could provide ideas for use in a variety of circumstances. A light touch to the change in the FSA ML rules/guidance would effectively allow the FSA to apply Option 4.

There would be no additional risk to the 'financial crime objective'. Risk mitigation tools are currently sufficient but not necessarily effective. The recent free CD ROM is an example of what can be effective. However the Industry Training seminars on Money Laundering in their present form are probably less effective for two reasons. I am OFTEN told by client that they are too expensive, both in their fees and in the actual cost and time cost of travelling a long distance. For example if one lives in Truro one might just attend a seminar in Bristol IF there is one, but highly unlikely to go to Canary Wharf. Therefore the Industry Training efforts in this respect often by-pass the small firms. Cost benefit etc. It is unlikely that any additional action by the FSA as suggested will increase cost to the IFA. Transparency. It is likely that most IFAs understand their obligations under the rules. However it is unlikely that they understand the benefit of their activity. They receive very little feed back and may assume that their activity is a waste of time as very few reports are made.

Consent = Yes

.

Walsh Lucas and Co

Q1 = We collect sufficient information already
Q2 = Sufficient guidance and rules already exist
Q3 = Current annual report is sufficient
Q4 = Cost of extra rules; beaurocracy and overkill cannot justify and change to what already exists Q5 = make no further rules or guidance; rely on JMLSG and leave things as they are. Waste of time; recources; cost; another unnecessary level of beaurocracy Consent = Yes
----

.