



Introduction by Philip Robinson

Welcome to the sixth edition of our financial crime newsletter. Since we published our last issue in March 2006, there has been lots of activity to refine the UK's anti-financial crime regime and, in particular, to embed a risk-based approach to anti-money laundering (AML) controls.

First, the industry is adapting to the new AML regime that came into effect at the beginning of September, when our new Handbook provisions and the new edition of the Joint Money Laundering Steering Group (JMLSG) Guidance came fully into force. The new regime puts more emphasis on firms taking a risk-based approach and on the importance of senior management engaging with AML issues. I know that over the last few months many firms have been reviewing their procedures, to establish which of them need changing to meet the new requirements and – just as importantly – what the opportunities are for fresh thinking over how they fight money laundering.

Second, FSA staff, and particularly our supervisors, have been taking part in the substantial re-training programme that we have rolled out to reflect the evolution of thinking on how best to fight financial crime: our new e-learning package, followed by workshops, and then our new formal guidance to supervisors. The financial sector trade associations will also be delivering training for our staff on the sectoral chapters of the new JMLSG Guidance over the next couple of months. I would like to thank the trade associations and their members for working with us in this way to ensure that

regulatory and industry approaches to AML are well aligned.

And finally, we have all been preparing for the implementation of the Third EU Money Laundering Directive and the forthcoming mutual evaluation of the UK's AML regime by the Financial Action Task Force, whose evaluation team will be visiting the UK later this year.

The thread running through all this activity has been the need to design and deliver a more risk-based approach to AML. This newsletter focuses principally on the risk-based approach, with items on:

- our actions in recent months to promote a more risk-based approach to AML;
- a progress update on our work to 'defuse the ID issue' and details of a factsheet we have recently issued to explain to consumers the reasons for identity checks;
- an update on the Third EU Money Laundering Directive and its implementation;
- recent thematic work on how firms deal with politically exposed persons;
- the Identity and Passport Service's Validation Service – an exciting project which should help users to conduct more effective ID checks;
- recent FSA research on boiler room scams; and
- recent FSA 'thematic work' on insurance claimant fraud.



Philip Robinson

The Risk-Based Approach: Clarifying our supervisory expectations

Over the last couple of years in particular, we have been strongly encouraging firms to make their AML practices more risk based. One of the ways in which we have been doing this is through a series of publications setting out our expectations and hopes for the future of the regime. Two publications in particular are relevant to all the firms we regulate, as well the work they need to do.

First, on 10 April 2006, Philip Robinson wrote to Ian Mullen, the then Chairman of the JMLSG, setting out our expectations of firms under the new AML/counter-terrorist finance (CTF) regime. In that letter he stressed our commitment to supervising in ways that promote the risk-based approach, and described how we have been investing in an extensive programme to retrain our supervisors to help deliver this.

Second, as part of this training programme, Philip Robinson circulated material to our supervisors and other staff who deal with firms at the end of August which explained the implications of the new regime for the way we supervise. We also sent this material to Martin Hall, the new Chairman of the JMLSG, and published a copy on our website at: www.fsa.gov.uk/pubs/other/money_laundering/letter_310806.pdf

The key messages in both these publications were that:

- i. we expect firms to:
 - deliver high AML/CTF standards;
 - assess where their risks lie and manage them appropriately; and
 - have regard to the content of the JMLSG Guidance in designing, implementing and monitoring their AML/CTF systems and controls; and
- ii. we expect senior managers to give a clear lead and take ownership of the firm's AML/CTF efforts.

Further information on our thinking about the risk-based approach is contained in two recent articles by Philip Robinson, also available on our website: www.fsa.gov.uk/pubs/other/money_laundering/MLB0906FSA.pdf
www.fsa.gov.uk/pubs/other/money_laundering/MLB0706FSA.pdf

This is not FSA guidance

Defusing the ID issue – the challenge

'We all know that identification is a problem. Firms don't like getting ID from customers. Customers don't like having to provide it. Both read about the insecurity of standard ID documents and question their anti-money laundering value. The regime in general, and the FSA specifically, are perceived as too preoccupied with ID.'

'Whatever the rights and wrongs, the present perception of the ID issue is very unhelpful and damages the support of the industry and their customers for the anti-money laundering effort....'

In April 2004, Philip Robinson said this in a speech challenging the FSA, government and industry to 'defuse' the ID issue. Two and a half years later, what progress have we made? The ID issue clouded the overall view of the anti-money laundering regime and what it was trying to achieve. Customer identification is crucial to the international fight against money laundering and terrorist finance, and a legal obligation. But in 2004 questions were asked about how this obligation was discharged. Was the ID regime proportionate? Did it command sufficient industry and consumer support? Did it deliver value to law enforcement?

The answers were not comfortable. And, more generally, it was clear that the regime had lost sight of the fact that most customers are law abiding. It was processes and regulatory risk that were driving practice, not how an ID check could contribute to the fight against crime.

When we launched the ID initiative we wanted to help create a system that was better at preventing and spotting money laundering. ID checks need to provide a reasonable level of certainty that people really are who they say they are; but checks must be proportionate in terms of the time, inconvenience and expense for the firm and customer. Customer ID is one tool against money laundering, to be deployed alongside others in the AML toolkit. It is not the 'be all and end all'.

With these aims in mind, we set up a working group of all the key AML stakeholders – firms, law enforcement, government, consumer groups, consultants, and electronic ID firms. Some of the conclusions we reached were unsurprising: ID was giving rise to a real issue of financial exclusion (albeit for a small minority of potential customers).

Those without the standard documents for proving identity – full-time students, those on State Benefits, refugees etc – clearly faced problems in proving their identity and particularly their UK address. Other conclusions were less predictable: law enforcement told us that a record of address at the start of a business relationship was less important than a person’s current address (which a firm will be keeping up to date anyway). This meant less work in the future to verify a person’s address at the outset.

The group agreed a package of ‘key propositions’ to improve the regime:

- reduced requirements over the number of documents needed to prove ID;
- better methods for financially excluded persons to prove their identities;
- electronic methods of verifying identity as a viable alternative to documents in many circumstances;
- the elimination of unnecessary repeat ID checks on the same customers;
- stronger checks underlying the issue of government documents used to prove ID;
- work to tackle the ‘fear factor’ – firms being unduly conservative in their ID practice because of fear of FSA sanctions; and
- less weight on ID relative to wider Know Your Customer procedures, monitoring and the other AML tools.

Progress to date

The task of delivering on these propositions fell to the JMLSG, us, individual firms, and various government bodies. What progress have we made?

The detail of good practice over how firms should conduct ID checks is set out in the JMLSG Guidance. The JMLSG published a new edition of their Guidance in February which is consistent with the outcomes of the work on ‘defusing’ the ID issue. The Guidance allows firms in many circumstances to use a single government-issued document (e.g. passport) to verify the identity of a personal customer. The variation in the robustness of different documents as a means of verifying identity (a driving licence, say, is a much better token of address than a utility bill) is more clearly

reflected in the guidance on how to verify ID. The approach over non-personal customers is considerably simpler. Electronic ID methods are given higher profile, and firms have more indicators on how to assess the quality of the provider’s method for verifying identity. More options are available for verifying the identity of people without passports etc. And there is a new set of arrangements for the use of streamlined ‘introduction certificates’ to reduce unnecessary duplicate ID checks.

The challenge for us is to ensure that supervisory and enforcement approaches promote effective, risk-based ID techniques. In the two letters to the JMLSG mentioned earlier in this newsletter, for example, Philip Robinson confirmed that if a firm can demonstrate an effective system of controls that identifies and mitigates the money laundering risks, enforcement action is unlikely.

To underpin this policy, we have (again, as outlined above) invested in an extensive retraining programme for supervisors and other staff. Our new ‘ARROW II’ risk assessment methodology should align our supervision more to the risks to our statutory objectives. And we have put together a major new financial crime training programme. Our staff need to understand what a risk-based approach to money laundering should look like and the challenges that firms face in managing money-laundering risk in a sensible, proportionate way. Our supervisors need to appreciate that one size no longer fits all, and they should expect to see different approaches from firms, even where they have quite similar business.

In the public sector, the government’s strategy for tackling identity fraud has contributed significantly to the ‘defusing’ of the ID issue. The initiatives by the UK Identity and Passport Service to enhance the security of the British passport and the passport-issuing process, and similar work by the DVLA over driving licences have contributed to reducing the scope for identity fraud.

The challenges that remain

Much has changed for the better since we launched our ID initiative in spring 2004. The theory is better aligned with the ultimate goal – what firms should be doing is more focused on what works in fighting money laundering. What then are the outstanding challenges?

The theory in the JMLSG Guidance needs to be turned into reality. Once new practices have bedded in this should lead to a substantial change to firms' ID and other AML procedures. We recognise that firms are not obliged to make all these changes. But firms should use this as an opportunity to enhance the effectiveness of their AML risk management. Firms should look at adapting their ID requirements for 'standard' customers, for example by:

- considering whether they need in every case to verify address for personal customers;
- ensuring that frontline staff and customers without commonly used ID documents like passports are made aware of the new options;
- reducing unnecessary duplication of ID checks; and
- changing the balance between the use of the different AML tools.

Efforts to enhance the quality of ID checks should continue. The crucial thing is that firms need to do checks well. One element of this is good customer experience, and we believe firms are for the most part delivering that. The check must also establish to an appropriate level of certainty that a person is who he/she claims to be, and an appropriate record must be kept. The person conducting the check needs to be:

- vigilant – on the look out for discrepancies in the information provided; and
- diligent – in ensuring that copies are legible or information is recorded correctly and stored so that the information can be easily retrieved.

There have been specific initiatives to promote quality. These include the work by trade associations, law enforcement and the relevant government agencies on providing information to firms on how to spot false passports, driving licences etc, and the JMLSG's work on quality criteria for the use of electronic ID methods. The Identity & Passport Service's new Passport Validation Service has already been trialled and UKPS plan to develop it in the coming years. It provides a validation service that enables accredited private sector organisations, such as financial services businesses, to check the validity and authenticity of a passport. You can read more

about this service in a separate article in this newsletter.

We have the prospect of further change to the legal context over ID. There will be new ID obligations from January relating to electronic payments under the new EU wire transfers regulation. In addition, we have the implementation of the Third EU Money Laundering Directive by December 2007, with its provisions on Simplified and Enhanced Due Diligence, spotting Politically Exposed Persons, and radical new arrangements for relying on third parties over ID. We need to keep a close eye on how these forthcoming obligations will impact on the ID issue, to ensure that ID does what it is meant to – contribute to effective and cost-effective risk management. We must not lose the ground gained in recent months. The Treasury deserves much credit for its efforts in negotiating in Brussels, to try to preserve the UK's ability to act in a risk-based, practical, proportionate way over checking ID. And finally, at the FSA, we need to deliver on our commitments to regulating in a risk-based way.

We believe we are well on course for 'defusing' the ID issue. And having a regime which, when fully implemented, will really deliver the win-win that we were hoping for – better for firms, law enforcement and for us all as customers. But most importantly as citizens, let us not lose sight that these efforts are all about reducing crime.

The blueprint is in place. It is for all of us now to ensure we deliver it.

ID: Delivering a positive consumer experience

A key element in our 'defusing' the ID initiative has always been the delivery by firms of a good consumer experience. We believe that two of the fundamentals for this are:

- firms telling their potential customers about the full range of options available to them over proving their identities, and explaining the purpose of ID checks;
- firms recognising in their ID policies the issues presented by those who do not have documents like passports and driving licences; and
- firms bearing in mind the Guidance in the FSA's Handbook that they should take

‘appropriate measures to ensure that procedures for identification of new customers do not unreasonably deny access to its services to potential customers who cannot reasonably be expected to produce detailed evidence of identity’.

As a contribution to delivering a good consumer experience, we have recently taken two initiatives:

- To help firms, we have made it clear in our published guidance to supervisors (see above) that we hope that they will take advantage of the flexibility over financial exclusion set out in our Handbook – using the other AML/CTF tools as necessary to deliver effective risk mitigation in these circumstances. ID should not be a significant barrier to financial inclusion.
- To help customers, we have updated our factsheet on ID. The new factsheet explains the reasons for ID checks and gives advice for those having difficulty proving their identity. It also explains how identity checks help prevent and detect crime, including terrorism and identity theft.

We are keen to get copies of the leaflet into the hands of all those organisations and individuals who would find it helpful. Free hard copies can be ordered online at www.fsa.gov.uk/consumer/consumer_publications/online/tpl_orderform.html or by calling our consumer helpline on 0845 606 1234.

Update: European Commission adopts implementing measures to the Third EU Money Laundering Directive

As reported in our last newsletter, the 3rd EU Money Laundering Directive was passed late in 2005 and must be implemented in the UK by 15 December 2007. The new Directive provides a common basis for implementing, at the EU level, the revised 2003 Financial Action Task Force (FATF) recommendations and will replace the previous two Directives. It is wider in scope than its predecessors and incorporates for the first time measures to combat terrorist financing.

The Directive provides for the adoption of legally binding implementing measures by the European

Commission in order to complete the legal framework created by the Directive – a process called ‘comitology’. The first implementing measures were adopted by the Commission in August 2006 and provide for the following:

- *A definition of Politically Exposed Persons (PEPs)*. The EU’s definition of PEPs is an aid to the interpretation of the high-level definition of PEPs contained in article 3(8) of the Directive, and gives examples of categories of PEPs. In line with international practice (e.g. the FATF, Basel Committee on Banking Supervision and the Wolfsberg Group), it is an open list. The PEPs definition is complemented by a number of recitals that further clarify the definition and set out how the Directive’s PEPs provisions should be implemented. Overall, the EU’s approach is similar to that set out in the 2006 JMLSG Guidance.
- *Technical criteria for situations in which the procedures for customer due diligence may be simplified*: The article on Simplified Due Diligence (SDD) contains criteria for customers, products and transactions that could be designated by individual Member States as representing a low risk of money laundering and terrorist financing. This means that for certain situations, firms need not apply ID and verification measures. The Directive does, however, state that a risk assessment must take place to determine whether a customer qualifies for an exemption. This implies that there is an ongoing obligation on firms to conduct monitoring of business relations on a risk-sensitive basis, in order to detect unusual transactions. Any money laundering or terrorist financing concern will override SDD.
- *Technical criteria allowing Member States to exclude from the scope of the Directive those persons or entities conducting financial activities on an occasional or very limited basis*. The comitology provisions also cover financial activity on an occasional or very limited basis, which means that Member States may consider legal and natural persons who engage in a financial activity and fulfil a set of criteria as not falling within the scope of the Directive. Examples include hotels that provide currency exchange services for their customers.

The Commission has started negotiations on the second set of implementing measures, which will cover criteria for situations which, by their nature, present a high risk of money laundering and terrorist financing and to whom enhanced customer due diligence measures must apply. The Commission has also invited comments from member states on criteria for identifying equivalent jurisdictions.

Politically Exposed Persons (PEPs): Good practice

During summer 2006, our Wholesale Firms Division visited 16 of the firms it supervises (banks, investment banks, investment firms and insurers) to assess their systems and controls in relation to PEPs.

PEPs have come increasingly into the spotlight of international anti-money laundering efforts. This is reflected in the revised JMLSG Guidance and the Third Money Laundering Directive¹ (the Directive), which came into force last year and which the UK will have to implement by December 2007.

The 2006 JMLSG Guidance (Chapter 5, paragraphs 5.6.12-18) points to the higher money laundering risks associated with customers who, by virtue of their position in public life, are vulnerable to corruption, and sets out ways for firms to deal with such customers. In line with the requirements of the Directive, the Guidance recommends that firms:

- have appropriate risk-based procedures to determine whether a customer is a PEP;
- obtain appropriate senior management approval for establishing or maintaining business relationships with such customers;
- take reasonable measures to establish the source of wealth and source of funds of such customers; and

- conduct enhanced ongoing monitoring of the business relationship.

This can be done on a risk-sensitive basis.

Given the nature of their business, the firms visited were generally observing the Guidance and were compliant with the Directive's PEPs provisions, and even the smaller firms were aware of their obligations. However, there are areas that firms can improve on. These are set out below along with some good practice tips. As always, firms should adopt a risk-based and proportionate response.

Areas for improvement

- *Importance of senior management approval:* while most firms were aware of and practised senior management approval, all firms should be planning to adopt it in order to ensure compliance with the Directive.
- *PEP specific training:* although PEPs were sometimes covered as one element of more general AML training, none of the firms visited delivered PEP-specific training. In future, firms with PEP clients should consider whether specific PEP training would benefit relevant staff.
- *Maintaining PEP account lists:* not all firms were able to produce a list of current PEP accounts on demand. Although we do not require firms to maintain a list of their PEPs, the fact that it could take some firms several days to produce a complete list of PEPs (not just high-risk clients) is of some concern. In addition, while firms did thorough checks to identify PEPs at the account opening stage, the processes used to determine if/when an existing customer became a PEP were less formal, with reliance placed on the informal relationship and knowledge of the client.
- *Use of PEP databases:* while senior management, compliance staff and the MLRO were typically aware of the limitations of such

1 In the Treasury consultation document, 'Implementing the Third Money Laundering Directive', the UK objectives for identifying and performing enhanced due diligence for politically exposed persons are:

- to help and protect national economies and to prevent the misappropriation of UK and International Aid;
- identify higher risk individuals that by virtue of their position in public life are vulnerable to corruption;
- alert firms to an obvious risk factor and specify certain risk mitigation measures that should be taken;
- to protect the integrity of the UK's businesses and retain their reputation as an efficient and fair dealing place to do business, by creating a hostile environment for illicit assets; and
- through the above, meet the requirements of FATF recommendations and the UN Convention Against Corruption.

databases, it was unclear how much the staff executing searches knew about the importance of setting the correct search parameters and using the most up-to-date lists. Similar issues also arose where firms used third parties or another business area to conduct customer profile checks.

- *Reputational risk:* the firms we visited defined the reputational risk of PEP business as the risk that a PEP might be involved in a public scandal, not that they were actually corrupt. A PEP with a high profile or impending ‘whiff’ of scandal might be immediately turned away. However, a PEP with lower risk of public controversy may be more likely to be accepted. This risk assessment was regardless of the source or legitimacy of the PEP’s funds. Reputational risk and financial crime risk are not the same and steps to mitigate reputational risk will not always reduce financial crime risk.
- *Internal Audit:* reviews by Internal Audit teams of anti-money laundering policies, procedures and controls tended not to look specifically at PEP risk. It would be good practice for Internal Audit always to review PEP risk as part of their anti-money laundering reviews.

Good practice

In addition to the JMLSG’s recommendations, we have identified the following ‘good practice’ in the course of our work:

- *Regular forums:* several firms held regular dedicated forums or committee meetings as part of their systems and control environment for PEPs. Such forums or meetings may cover a range of issues including unusual transactions, discussions about potential new client accounts and Suspicious Activity Reports (SARs).
- *PEP Take-on:* one firm established its own independent take-on committee chaired by the CEO which decided whether to open PEP accounts. Some firms have also developed their own in-house forms and checklists designed to capture all the necessary information required at take-on which are then stored on the group’s global database.
- *MLRO Report:* Some firms included specific reference to the management of PEPs risk in the MLRO Report.

- *No automatic declassification of PEPs accounts after expiry of a prudential period:* the team visited one firm where declassification from PEP status following a specified period out of public office was not automatic and had to be approved by the firm’s Management Committee. Where a person remained in the public eye, although not necessarily in a public position, declassification from PEP status would not occur.
- *Managing Conflicts of Interest:* at least one firm did not remunerate account managers on the basis of number of accounts opened.

Typical ‘boiler room’ scam victim loses £20,000

We recently carried out some research on boiler rooms to demonstrate how boiler rooms operate, as part of our campaign to raise awareness of the scam. This showed that people who fall victim to these scams by purchasing virtually worthless shares lose an average of £20,000.

Boiler rooms are not authorised by the FSA and act illegally by promoting and selling shares in the UK. In most cases, the shares are worthless and the boiler room vanishes, leaving the investor out of pocket. Because boiler rooms are typically based outside the UK, we are usually unable to take direct action to shut them down.

58% of respondents to the survey had fallen victim to the scam by purchasing worthless shares. Of the victims, 13% had been conned by more than one boiler room, while three victims each reported losses of over £100,000.

The survey found that boiler rooms tend to prey on older people. Of those who had fallen victim to boiler rooms, 38% were aged over 60 while 26% of victims were 51-60 years. The majority of victims were male (81%) and most were experienced investors, with 41% of victims saying they had been investing for over 11 years.

Many respondents reported that they were first contacted by the boiler room out of the blue on the telephone. Around a third said that boiler rooms used marketing firms to contact targets on their behalf.

The Passport Validation Service (PVS)

The Identity & Passport Service (formerly the UK Passport Service) has launched the Passport Validation Service to help to combat fraud and identity theft. This service is now available to organisations regulated by us.

Passports are a commonly used method of proving identity. Unfortunately, there are many false passports in circulation and many have been used to attempt to de-fraud financial institutions. The Passport Validation Service (PVS) allows firms the opportunity to confirm that UK passports presented as evidence of identity match the computerised records of UK passports issued by the Identity and Passport Service (IPS). This helps reduce the risk of fraudulent applications made with lost, stolen or counterfeit passports.

Due to the nature of the information provided, IPS needs to be certain that it does not share sensitive data with any organisation that should not have access. To ensure this, there is an application process that all potential users of PVS must first go through. Once approved, organisations are given access to the PVS via their own designated 0845 number and passports can then be validated in just over a minute.

To use the PVS service there is a one-off fee of £5,000 to cover set-up costs and administration; this will only be charged once the application to access the service has been approved. Once operational, there is a £1.20 per minute call charge rate and the average call time is 1 minute 20 seconds.

For more information or to apply please email pvs@ukpa.gsi.gov.uk or call the Passport Validation Service on: 020 7147 1022.

Insurance claimant fraud: Thematic work

In December 2004, our Insurance Sector Non-Life newsletter outlined the key findings from a survey which reviewed the approach taken by small and medium sized insurers in managing the risk from claimant fraud.

The problem remains significant and the Association of British Insurers now estimates that

losses of £1.5bn each year are attributable to claimant fraud. In recognition of the risk claimant fraud poses to the industry and the FSA's objectives, we have recently undertaken a thematic exercise involving the larger insurers. The purpose of the review was to assess the material claimant fraud risks the industry currently faces and the systems and controls insurers are using to reduce their exposure to the threat. The review focused on: key risks (life & non-life sectors); governance; systems & controls; and data sharing.

The detailed findings of the review will be published in our next insurance sector newsletters (life & non-life). Current copies and back issues of the insurance sector newsletters can be found on our website at: www.fsa.gov.uk/Pages/About/Teams/Insurance/publications/index.shtml.

Changes to cheque writing: Cheques made payable to banks and building societies

From now on, people writing cheques made payable only to a bank or building society will need to break that habit. Instead, they will have to add extra details about the beneficiary of the cheque, like the name or account details. This is because, since the beginning of October 2006, banks and building societies are likely in certain circumstances to decline cheques made out to only a financial institution.

The new arrangements are intended to make it absolutely clear who should benefit from the funds and help prevent fraudsters paying in stolen cheques. As banks and building societies hold accounts on behalf of millions of customers, there is nothing to identify which of those account holders should benefit from the funds if the cheque is made payable simply to 'XYZ Bank/building society'. By making a cheque payable to 'XYZ Bank' and adding the account number or name, it is clear who the funds are intended for. Cheques made out to personal or business customers will be unaffected.

These changes were announced last December and are designed to help tackle fraud. Since then, the industry has been advising people to start adding the extra details immediately, through leaflets and information on cheque books and statements.

We have worked closely with the industry on this initiative. The revised procedures are consistent with advice given in The Banking Code.

Dates for your diary

We will hold the next **FSA Financial Crime Conference** on 22 January 2007 at the QEII Conference Centre, Westminster. Speakers include our Chief Executive, John Tiner; Bill Hughes, Director General of SOCA; Mike Bowron, Commissioner – City of London Police; and Professor Mike Levi, Cardiff School of Social Sciences. Bookings open soon through our website at www.fsa.gov.uk/Pages/Doing/Events/events/index.shtml.

The **Concerted Inter-agency Criminal Finances Action Group (CICFA) annual ‘Payback’ conference** is being held on 28-29 November 2006, at Novotel London West Hotel & Convention Centre. Vernon Coaker MP, Under Secretary of State for Policing, Security and Community Safety, will be giving the keynote address. Other speakers include: Jane Earl, Director of the Assets Recovery Agency and Sir Stephen Lander, Chairman of the Serious Organised Crime Agency. For further information, please contact CICFA’s Conference & Events Coordinator on 020 7029 5714 or email: conferences@ara.gsi.gov.uk.

Milestones in 2006-2007

As mentioned in our last newsletter, there will be some significant changes to the law on anti-money laundering during 2007, as a result of initiatives by the European Commission. In the build-up to this, there will be some important milestones, which we have set out below.

Date	Milestone
Late 2006	FATF Mutual Evaluation on-site inspection of UK
6 December 2006	Closing date for responses to the Government’s consultation on the regulation of Money Service Businesses in the UK
1 January 2007	Wire Transfers Regulation comes into force
Early 2007	Consultation on draft Money Laundering Regulations
Mid-2007	Publication of Money Laundering Regulations
15 December 2007	Latest date for implementation of 3MLD

Coming soon! Look out for the FSA’s new financial crime web pages at www.fsa.gov.uk

Contact details

If you would like to receive this newsletter in future or have any comments on its content or format please contact us by e-mail at:
financial.crime@fsa.gov.uk

Individual contact details are as follows:

Financial Crime Sector Team

Edna Young (Financial Crime Sector Manager)
edna.young@fsa.gov.uk
020 7066 0964

Robert Gruppetta (Financial Crime Sector Associate & Newsletter)
rob.gruppetta@fsa.gov.uk
020 7066 0140

James Cadwallader
james.cadwallader@fsa.gov.uk
020 7066 2932

Greg Southall
greg.southall@fsa.gov.uk
020 7066 8512

Anne Crestinu
anne.crestinu@fsa.gov.uk
020 7066 5722

Sonia Dohil (Team Administrator)
sonia.dohil@fsa.gov.uk
020 7066 0546

Financial Crime Policy Unit

James London (Manager)
james.london@fsa.gov.uk
020 7066 0984

Carol Hyams (Secretary to James London)
carol.hyams@fsa.gov.uk
020 7066 4542

Further financial crime information is available at:
www.fsa.gov.uk/Pages/About/Teams/Crime/index.shtml