

## Introduction by Philip Robinson

As the FSA's Financial Crime Sector Leader, I am pleased to introduce our second Financial Crime Sector newsletter. You will recall that the main focus of our first issue was financial crime legislation and the FSA's financial crime policies. In this issue, we focus on the more practical aspects of how the FSA fulfils its regulatory objective to reduce financial crime. This includes an introduction to our new Financial Crime sector team.

Other issues covered are:

- our work to combat financial crime at each stage of the regulatory process – this includes an overview of the work done by our Risk Review Department;
- recent convictions for fraud, following work by the FSA;
- money laundering 'mules';
- company identity fraud;
- new 'boiler room' tactics; and
- the obligation to report significant frauds to the FSA.

Before covering these areas though, it is important that I update you on key legislative and policy developments since the last newsletter.

The publication in March by the Joint Money Laundering Steering Group (JMLSG) of a consultation draft on new Guidance is an important step forward in the fight against money laundering and terrorist finance. The draft Guidance, with its strongly risk-based flavour and its blueprint for a more streamlined customer identification (ID) regime, is part of what I see as a new era in the money laundering

regime. It offers the real and very welcome prospect of a properly risk-based, effective and targeted regime; and one in which customer identification procedures play an important, but proportionate, role in the fight against crime. As a consultation draft there is of course some 'unfinished business', and some aspects that we hope the JMLSG will be willing to amend. But, all in all, we warmly commend the JMLSG on the text and the radical thinking that underlies it. It is also marvellous news that the JMLSG propose to make a pdf version of the Guidance available to all on their website. This will be a big contribution to promoting good AML practice across the industry. For our part, we will continue to offer input to the consultation process and to encourage others to do the same.

The new Guidance is a key element in a more risk-based approach, but I recognise that statements of support for this change of direction are hollow without delivery of a risk-based approach by FSA supervisors on the front line. We must mean what we say and act on it. So training and equipping our supervisors to regulate in a risk-based, proportionate way is one of our highest financial crime priorities in the coming months. And as I have already stressed publicly – in my letter to Ian Mullen (Chairman of the JMLSG) last year – our enforcement policy will also be driven by a recognition of the risk-based approach. You can read more about this later in this newsletter.

Another area of risk-based activity is our work supporting the Treasury over their negotiation of the Third EU Money Laundering Directive. The wording of the new Directive will be absolutely crucial for the future of the UK money laundering regime. If that wording is too prescriptive,

we are in danger of losing some ground we have made in recent years in the development of a UK AML regime that works – that achieves what we all want in the fight against crime at a proportionate cost to all those involved.

The final piece of the risk-based jigsaw for us is to look at our Handbook provisions on money laundering, to see whether alternative provisions would better serve our aims. We have concluded that they might, so we will shortly be consulting on proposals which reduce the number of specific rules in the Handbook but emphasise the importance of senior management having in place appropriate risk sensitive systems and controls to reduce the likelihood of their firms being used as a conduit for financial crime.

As ever, we would welcome feedback, ideas for future issues and suggestions of how we might make this newsletter more useful to our external stakeholders. Our contact details are at the end of this newsletter. We aim to publish our newsletters on a quarterly basis but they might be slightly more or less frequent than that, depending on financial crime developments.



Philip Robinson

## FSA work to combat financial crime

### Financial Crime Sector Team

The new Financial Crime sector team has been in place for around two months and reports directly to Philip Robinson. It comprises Edna Young (Manager) and Rob Gruppetta. Edna and Rob both have a banking supervision background, and Edna spent many years in Whitehall (most recently in the Treasury). Immediately before their appointments, they worked in the FSA's Intelligence and High Street Firms departments, respectively.

The team's main role is to support Philip in ensuring that the FSA achieves its challenging financial crime objective by:

- helping the FSA become better at identifying risks early on and taking pre-emptive action to manage issues swiftly and decisively;
- building and maintaining strong relationships with external stakeholders to achieve our common goals in the fight against crime;
- ensuring that issues are considered on a cross-FSA basis so our financial crime objectives and priorities are understood by the whole organisation and that we achieve them in the most efficient way possible; and
- developing the skills and knowledge of our staff.

A key priority is to develop and deliver improved financial crime training for FSA staff – the sector team is directly responsible for this. This is particularly important as the industry moves towards a risk-based approach to anti-money laundering. Firms must be confident that supervisors understand how a risk-based approach might operate in their firms, otherwise they may be reluctant to move forward for fear of regulatory sanction. A risk-based regime cannot be “zero failure”.

It is important to point out that the FSA's staff already consider financial crime issues on a daily basis. Below, we outline how we identify, mitigate and monitor financial crime issues at each stage of the regulatory process.

### Authorisation

One function of our Regulatory Transactions Division is the assessment of corporate applications for Part IV permission from firms wishing to conduct regulated activities in the UK. We initially assess applications to identify risk impact and key risk factors. This assessment will determine whether an application is dealt with as routine and handled through our Authorisation department's ‘green channel’ mechanism, or presents something of a non-routine nature, in which case it will be referred and dealt with as a ‘red channel’ case. These risk factors include those relating to financial crime and whether the applicant could be used to facilitate, or be exploited for, financial crime purposes. A number of triggers can prompt a referral to the red channel. These can arise at the outset or may occur as a result of vetting checks or other enquiries made.

Where financial crime concerns are identified, case officers will work closely with colleagues in our Intelligence department and, where applicable, will also liaise with other internal and external parties. Staff in Authorisation have access to advice on financial crime issues, usually through their local sector lead, to ensure relevant issues are covered.

Over the last two years, formal warning notices have been issued through the Regulatory Decisions Committee to several applicant firms proposing to refuse their application on grounds of financial crime concerns. One of these reached 'final notice' stage; the remainder withdrew their applications before a final decision notice was issued.

## Supervision

In our Supervision department, we have done much work since N2 (1 December 2001 – when the FSA gained its statutory powers) on raising the standards of firms' anti-money laundering controls. We believe there has been a real improvement across the industry in understanding and managing money laundering risk. Even so, our interest in ensuring that firms maintain high standards of anti-money laundering controls is undiminished.

We are now looking more closely at fraud issues as part of our supervision of individual firms, where we expect there to be effective and proportionate fraud management systems and controls.

Our Handbook requires that firms take reasonable care to establish and maintain effective systems and controls for countering the risk of fraud. At a high level, we seek to assess whether a firm has a strong anti-fraud culture with a clear lead being given from the top. We expect there to be a clear allocation of responsibility for the day-to-day management of fraud risk; effective staff training arrangements; and good management information on fraud presented to the board and senior management.

We believe there are clear market incentives for firms to prevent fraud and so our response to fraud is reasonable and proportionate. We expect firms to report significant frauds, as our Rules require (see box on page 5). In most cases where we believe we do need to take action, we will use supervisory tools, probably through a firm's risk mitigation programme. We want firms to learn

from frauds and, where appropriate, strengthen their controls. Of course enforcement action is always possible, but is very much the exception rather than the rule. However, we would consider it if, for example, there were serious systems and controls weaknesses or if there had been significant detriment to consumers.

## Enforcement

The overriding consideration in this area is whether a firm has implemented an effective control structure that identifies and mitigates its own particular financial crime risks. High-profile anti-money laundering enforcement action over the past two years has sent clear and valuable messages, in support of earlier public statements. Firms now better understand what is expected of them and, as a result, evidence suggests that standards have risen.

Effective AML systems should reduce the risk that money laundering remains undetected, unreported and successfully completed.

It is likely that, in the immediate future, enforcement efforts will concentrate on actual money laundering where a high risk was identified; where there is a higher risk of money being laundered because of, for example, a failure to report suspicions or seek consent; or where there are specific weaknesses in systems and controls that result in high risk transactions not being detected or reported. We expect firms to identify any high-risk areas within their business and to ensure that sufficiently effective procedures are in place to control those risks.

### FSA rule SYSC 3.2.6R

A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime.

Enforcement's approach to money laundering has developed from a high-level, message-based focus to a strategy in support of the FSA's risk-based approach. So it is not our current intention to direct significant enforcement resources to ID and

record-keeping issues, but we are more likely to take these types of cases where there are particular aggravating circumstances.

Future disciplinary action is more likely to involve breaches of FSA rule SYSC 3.2.6R and involve failures that may appear to be very firm-specific or involve specific circumstances. More intelligence-led action is also expected, as we continue to develop our relationships with law enforcement and similar agencies.

## Risk Review Department

Our Risk Review Department (RRD) acts as an in-house consultancy, giving technical support to regulatory divisions across the FSA on credit, market, insurance and operational – including financial crime – risk issues. Reviews of FSA regulated firms' policies, procedures and controls are commissioned by line supervisors, who decide the scope and objectives of the exercise, which most commonly comprise an on-site visit of one to two days. However, sometimes a desk-based review of relevant documentation is sufficient.

The need for a review is often identified during an ARROW risk assessment but may also arise in response to an application for authorisation or to a specific concern about a firm which, for example, might be flagged by law enforcement agencies. The visit can be used to explore potential areas of risk, where we need to understand the risk management and procedures a firm is implementing, or could be part of a risk mitigation programme to assess progress in dealing with previously identified risks.

RRD also leads and contributes to project and theme work on sector- or industry-wide topics, including financial crime. This work not only assesses the financial crime risk associated with particular areas of activity, and how it is being managed, but also identifies standards of practice across regulated firms and informs FSA line directors, sector leaders and supervisors where those standards lie. A recent example of RRD's project/thematic work is their examination of information security risk in the financial services sector. You can find the information security report on our website at:  
[www.fsa.gov.uk/pubs/other/fcrime\\_sector.pdf](http://www.fsa.gov.uk/pubs/other/fcrime_sector.pdf)

## Recent fraud prosecutions and disciplinary action involving the FSA

We have recently contributed to two successful fraud prosecutions, full details of which can be found by following the links below to the Serious Fraud Office's website.

Over £1 million stolen in options trading deception: Malcolm Varrick was jailed for four years on 10 November 2004 after admitting he stole £1.16 million from investors deceived through his Durham-based financial businesses. He promised high and assured profits on options trading. He spent lavishly on himself, using some of the £4.25 million in investors' funds. For full details, click here:  
[www.sfo.gov.uk/news/prout/pr\\_360.asp?id=360](http://www.sfo.gov.uk/news/prout/pr_360.asp?id=360)

Two sentenced in trade finance fraud: David Mahood and Michael Cuzner-Charles were sentenced on 25 February 2005 at Belfast Crown Court to a combined six years' imprisonment (suspended for two years) in relation to the misuse of £2.5 million of investors' money acquired by their merchant finance business Regal Brook Ltd. They have been ordered to pay £125,000 each by way of compensation and each disqualified from acting as a company director for seven years. For full details, click here:  
[www.sfo.gov.uk/news/prout/pr\\_385.asp?id=385](http://www.sfo.gov.uk/news/prout/pr_385.asp?id=385)

In addition, the the Financial Services and Markets Tribunal directed on 6 April 2005 that the FSA fine Mr Arif Mohammed, a former PricewaterhouseCoopers (PwC) audit manager, £10,000 for committing market abuse. This is the first time that the market abuse provisions in the Financial Services and Markets Act 2000 have been the subject of a Tribunal decision. For full details, click here: [www.fsa.gov.uk/pages/Library/Communication/PR/2005/pr034.shtml](http://www.fsa.gov.uk/pages/Library/Communication/PR/2005/pr034.shtml)

## Money Laundering 'Mules'

A recent addition to the FSA website's 'Scams and Swindles' section warns consumers about them becoming so-called money laundering 'mules'. Prompted by calls to our Consumer Contact Centre and other referrals to the FSA Intelligence Team, the warning relates to emails or adverts purporting to contain an offer of employment.

The cover story used varies, but may typically claim that a company is looking for ‘account managers’ who can work from home and earn good rates of pay. A heartless example claimed to be from a charity requiring assistance because of what they described as the collapse of the banking system following the Asian tsunami.

All that is asked is that the prospective new employee has access to a UK bank account. They will receive payments into this account, but because the company or charity has ‘difficulties accessing the banking system’, the mule will be asked to withdraw these sums in cash, keep a commission for themselves and transfer the balance abroad using a money transmission agent.

Of course, as with all such offers, if it looks too good to be true it usually is. These mules are facilitating a fraud, usually involving ‘phishing’ attacks. Once the fraudster has access to an online bank account, they are faced with the problem of moving the funds. By recruiting and using mules they can have the money moved abroad to any destination they choose and break the paper trail by using cash. When the authorities investigate, the trail leads them straight to the unsuspecting mule.

## FSA warns of new ‘boiler room’ tactic

Companies and consumers were recently reminded of the dangers of dealing with unauthorised firms.

The FSA warned of a new tactic used by ‘boiler rooms’ – overseas investment firms that are not authorised by the FSA – to con both investors and UK small companies out of their money.

Boiler rooms traditionally use high-pressure selling techniques to persuade UK investors to purchase shares in foreign companies. But the FSA is now aware of boiler rooms that are selling shares in small companies based in the UK.

In a typical scenario, a boiler room would approach a small unlisted UK company and propose to raise capital by selling £100,000 worth of shares in that company on their behalf. Of this £100,000, the boiler room would take 60% as its fee, leaving the small company with £40,000 capital. In reality, the boiler room will cold call UK investors to sell the shares at up to 100% over the agreed price, take their fee and vanish. The small

companies involved may become liable to refund investors the full price paid for their shares.

The FSA reminded companies and consumers to check that a firm offering fund raising or investment opportunities is authorised. The Department of Trade and Industry (DTI) has warned small unlisted companies that, in many cases, selling their shares to the public is a criminal offence. Companies considering raising funds should seek legal advice.

## Your obligation to report significant frauds to us

We would like to remind firms that they are required under FSA rule SUP 15.3.17 to report significant frauds to us. ‘Significant’ does not relate solely to the amount of the actual or potential loss. Our Handbook makes it clear that you also need to consider the risk of reputational loss and whether the incident reflects weakness in internal control. Significant fraud reports should be sent to your relationship manager or, for smaller firms, the Firms Contact Centre.

### SUP 15.3.17R

A firm must notify the FSA immediately if one of the following events arises and the event is significant:

- (1) it becomes aware that an employee may have committed a fraud against one of its customers; or
- (2) it becomes aware that a person, whether or not employed by it, may have committed a fraud against it; or
- (3) it considers that any person, whether or not employed by it, is acting with intent to commit a fraud against it; or
- (4) it identifies irregularities in its accounting or other records, whether or not there is evidence of fraud; or
- (5) it suspects that one of its employees may be guilty of serious misconduct concerning his honesty or integrity and which is connected with the firm’s regulated activities or ancillary activities.

## Metropolitan Police and Companies House initiative to tackle company identity fraud

On 9 May, the Metropolitan Police launched a media campaign and crime prevention leaflet in partnership with Companies House, the Association of Chief Police Officers and key stakeholders to highlight a fraud targeted at British business.

This fraud relies on organised criminal networks being able to hijack the identities of legitimate companies by making fraudulent entries on their registration at Companies House and then using their credit rating to obtain high value goods and services. The loss to industry through this type of fraud is estimated to be over £50 million a year.

We would encourage you to read the leaflet which can be found at [www.met.police.uk/fraudalert/docs/CHleafletforlaunch.pdf](http://www.met.police.uk/fraudalert/docs/CHleafletforlaunch.pdf) and consider taking the measures suggested to protect your firm from this growing type of fraud.

## Forthcoming changes to the law on money laundering

The Serious Organised Crime and Police Act 2005 contains provisions amending Part 7 of the Proceeds of Crime Act 2002. When implemented, these will mean some changes to the law on money laundering. In particular, there will be changes in relation to:

- the position over proceeds deriving from conduct overseas;
- the circumstances under which pre-transaction consent needs to be sought where there is not much money involved;
- some limited exemptions over what has to be reported; and
- reduced penalties over the failure to use the form in which reports have to be made.

The Act is available on the internet at <http://www.opsi.gov.uk/acts/acts2005/20050015.htm>. Details of the coming into force of the relevant provisions will be posted on the Home Office website (<http://www.homeoffice.gov.uk/crimpol/oic/proceeds/index.html>) in due course.

## 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](mailto:financial.crime@fsa.gov.uk)

Individual contact details are as follows:

Edna Young (Financial Crime Sector Manager)  
[Edna.young@fsa.gov.uk](mailto:Edna.young@fsa.gov.uk)  
020 7066 0964

Robert Gruppetta (Financial Crime Sector Associate & Newsletter)  
[Rob.gruppetta@fsa.gov.uk](mailto:Rob.gruppetta@fsa.gov.uk)  
020 7066 0140

Chris Eridani-Ball (Anti-Money Laundering and Fraud Policy)  
[chris.eridani-ball@fsa.gov.uk](mailto:chris.eridani-ball@fsa.gov.uk)  
020 7066 3490

Ian Matthews (Fraud Policy)  
[ian.matthews@fsa.gov.uk](mailto:ian.matthews@fsa.gov.uk)  
020 7066 1092

Jamil Choudhry (Anti-Money Laundering Policy)  
[jamil.choudhry@fsa.gov.uk](mailto:jamil.choudhry@fsa.gov.uk)  
020 7066 1936

Helen Smith (Anti-Money Laundering Policy)  
[helen.smith@fsa.gov.uk](mailto:helen.smith@fsa.gov.uk)  
020 7066 0656

Abnash Sagoo (Anti-Money Laundering Policy)  
[Abnash.sagoo@fsa.gov.uk](mailto:Abnash.sagoo@fsa.gov.uk)  
020 7066 4734

## Useful links

FSA website 'Scams and Swindles' at:  
[www.fsa.gov.uk/consumer/01\\_WARNINGS/scams/mn\\_scams.html](http://www.fsa.gov.uk/consumer/01_WARNINGS/scams/mn_scams.html)

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