



Introduction by Philip Robinson

Welcome to the ninth edition of the FSA's financial crime newsletter, in which we give you an update on the work we

are currently carrying out on financial crime issues. I hope you find it interesting and useful.

In our last newsletter, we focused on authenticating and safeguarding customers' identities. Doing this effectively mitigates one of our key financial crime risks: the risk of information security and identity fraud. In our 2007/08 Business Plan, we committed to examine in more depth the information security risks for firms and consumers. We are currently carrying out thematic work into information security controls in authorised firms, and will be reporting our findings during the spring of 2008. It is important to remember that for those firms that have appointed representatives, their obligations apply to the conduct of those appointed representatives just as they apply to the conduct of the authorised firm itself. Firms should be careful not to overlook this part of their responsibilities; more information about what to consider can be found in the article on page 2.

The final date for implementing the European Union's (EU) Third Money Laundering Directive (3MLD) is now less than two months away. We have been working hard to ensure we are ready for the deadline on 15 December 2007. Businesses falling within the scope of these new money laundering regulations will be able to register with us from 15 November 2007.

We have published an Approach Document, available on our website at www.fsa.gov.uk/pubs/other/approach.pdf, which sets out how we will supervise these businesses. For details on what the Financial Crime Operations Team are doing to prepare for the implementation, please read the article on page 3.

Our approach to financial crime is inevitably influenced by international developments in the area, such as the 3MLD. The UK is a member of the Financial Action Task Force (FATF) on Money Laundering, and currently holds the Presidency. The FATF is an intergovernmental body that aims to develop and promote national and international policies relating to money laundering and terrorism finance. It is currently evaluating its members' policies against its standards. The UK's evaluation was published earlier this year; details of our assessment can be found on page 4.

When trying to fight against fraud, as with other aspects of financial crime, it is vital to understand how crimes are committed, as well as their wider context. Mortgage and property fraud has been growing in prominence in recent months, with some significant press coverage. We have been investigating the background of both individual and organised property fraud, to help us target our efforts most effectively. A summary of our findings is on page 4.

One of our key challenges in fulfilling our statutory objective to reduce financial crime is dealing with firms who operate outside our authorisation. Boiler rooms often operate outside the UK, which makes it harder for us to take direct action against them. However, we have recently shut down two firms for helping boiler rooms with their activities. You can

find out more about boiler rooms in the article on page 5, and read more about the action taken in our press release at:

www.fsa.gov.uk/pages/Library/Communication/PR/2007/101.shtml.

Finally, the Treasury has announced changes to the way the financial sanctions are administered in the UK. It has set up an Asset Freezing Unit, which will assume the Bank of England's responsibilities for administering financial sanctions. For more details, please see the article on page 5.

You can find the articles described above as follows:

- Information security in appointed representatives, page 2
- 3MLD supervision team, page 3
- FATF mutual evaluation result, page 4
- Our work on property fraud, page 4
- Boiler rooms, page 5
- Changes to financial sanctions procedures, page 5



Philip Robinson

Director
Financial Crime and Intelligence Division

Information security in appointed representatives

The most common financial crime incident we have been dealing with this year is the compromise of customer data by firms holding large amounts of sensitive information. Worryingly, nearly all of these data compromises were because of carelessness, breaches of procedures or poor controls – they were not due to sophisticated hi-tech attacks by organised criminal gangs. Data compromises can affect a limited number of customers, but the sensitivity of the lost data puts those consumers at a very high risk of financial crime and identity fraud.

Information security risk cannot be mitigated by hi-tech means, such as encrypting laptops, alone – though these are of course important. Protecting customer data is just as much about good vetting practices and clear and appropriate policies and procedures communicated to staff in a sensible way.

Another cause for concern is the way we have seen many firms deal with data security incidents. The general trend we see is that they often appear more concerned about the possibility of adverse publicity and reputational damage to themselves than the risk to their customers of financial crime or identity fraud.

This article is about data compromise in appointed representatives. We were prompted to write it by a particular case that we dealt with under joint action by our supervision and financial crime teams. Under s.39 of the Financial Services and Markets Act 2000 (FSMA), a firm is responsible for anything done or omitted by a representative that carries on business which the firm has responsibility for, in the same way as if the firm had done it itself. The principal firm must have accepted responsibility in writing for the whole or part of the business that it allows the appointed representative to carry on. The firm must also carry on its business with due skill, care and diligence, and it must take care to organise and control its affairs responsibly and effectively, with adequate risk management systems (Principles 2 and 3 of our Principles for Business). Also, under Principle 6, a firm must pay due regard to the interests of its customers (and treat them fairly).

As part of this, a firm should take steps to safeguard the customer information it holds for the purpose of carrying on regulated activities. And, in the case of an appointed representative, the firm must take steps to ensure the appointed representative acts similarly. Guidance in our Senior Management Arrangements, Systems and Controls Sourcebook (SYSC), 3.2.4G (1) states that a firm cannot contract out of its regulatory obligations and that under Principle 3 a firm should take reasonable care to supervise the discharge of outsourced functions by a contractor. Also, our Supervision Sourcebook (SUP) states the firm must establish (on reasonable grounds) that it has adequate controls over any person's regulated activities for which it has responsibility (12.4.2 R (3)).

Holding customer information is integral to carrying on regulated activities – the firm or the appointed representative could not carry them on without the information.

Significantly, SYSC 3.2.6R requires a firm to take reasonable care to establish and maintain effective systems and controls for compliance. It must also have applicable requirements and standards under the regulatory system for countering the risk that it might be used for furthering financial crime. Clearly client data may be used for committing financial crime.

The question we must answer in looking at firms is whether the requirements imposed on their appointed representatives are sufficient controls. It is not enough to only require the appointed representatives hold data protection licences as controllers. This does not address the question of whether the appointed representatives are actually taking adequate steps to keep customers' confidential information secure. While the security of confidential information is the subject of the Data Protection Act, it is also integral to carrying on a regulated activity. Also, holders of confidential information may separately owe a duty of care to the subject of that information to keep it secure.

Firms should do more than expect appointed representatives to hold a Data Protection Act licence. They should satisfy themselves that their appointed representatives have adequate safeguards in place to protect client data for which they owe the client a duty of care. Firms must perform further checks to ensure appointed representatives are holding confidential information securely. While firms will never be able to prevent all instances of data loss, they may consider using systems which would restrict access to confidential information if a loss is to take place. We can take enforcement action against a firm for inadequate controls by an appointed representative, in the same way as if the firm itself had offended.

In summary, the principal firm is responsible for the acts and omissions of its appointed representatives. So if the appointed representative's actions gave rise to a liability to the customer, and the customer suffered a loss because of those actions, the principal would be responsible. The rules and principles and the common law require a firm to take reasonable

care to protect its' clients confidential information. So a firm should have controls in place to check its appointed representatives are similarly taking reasonable care.

3MLD Supervision team

We are now going ahead with preparing for the new areas of supervision under the Third Money Laundering Directive (3MLD). The team members (Greg Southall, Mark Vowells and Debbie Curtis) are working towards being ready for when registration begins on 15 November. Our aim is to be ready one month before the 3MLD implementation date of 15 December. You will notice we use the term 'business' for entities being registered, rather than 'firm' to differentiate it from the FSMA regime.

We will organise our supervision of the new businesses using a risk-based approach. This means we will supervise by doing thematic work and dealing with cases of crystallised risk using a method similar to the way our Small Firms Division supervises its firms. The early theme work will be all about making sure the right businesses have registered with us. We will need to understand the industry the businesses operate in, the business models they use and the money laundering risks they face. Most registrations are likely to be from businesses involved in lending and leasing where the particular type of lending or leasing carried out is not covered by the Office of Fair Trading. The definitions in the Approach Document will be of great significance in ensuring we are clear about which businesses we supervise and which we do not (please see the introduction for a link to the Approach Document). We expect that businesses such as invoice discounters, factors and those providing finance leases will be the bulk of those registering. The key focus for the team will be to understand the technical side of these businesses as they are not typical of the financial services businesses we are familiar with under the FSMA regime.

Financial Action Task Force mutual evaluation result

On 1 August 2007 the Financial Action Task Force (FATF) published their full report on their mutual evaluation of the UK's anti-money laundering (AML) and combating the financing of terrorism (CFT). The publication of the report marked the completion of the mutual evaluation process. While the Treasury led the UK's effort during the evaluation process, we provided support and assistance. We did this in line with our statutory objective to reduce the extent to which firms can be used to further financial crime, and our statutory duty to cooperate with other agencies with similar financial crime functions. A number of FSA representatives were in the UK delegations for the assessors' on-site visit, the face-to-face meeting and the FATF plenary session where the report was discussed and adopted by the FATF members.

The full report shows the UK was awarded 36 'compliant' (C) or 'largely compliant' (LC) ratings for the 40 recommendations and nine special recommendations, which the FATF have produced as standards of best practice for AML and CFT systems. This was a broadly positive result and served as an endorsement of the UK's systems. Achieving 36 out of 49 C/LC ratings places the UK joint third (with Portugal), behind the US (44/49) and Belgium (41/49). It is well above the FATF average of 29/49 in the current round of mutual evaluations. Of particular note is the UK achieved the highest number of 'compliant' ratings (24) of any nation evaluated so far.

Key elements of the UK's approach, notably the Proceeds of Crime Act 2002 and the work of Serious Organised Crime Agency (SOCA), were recognised as valuable by the assessors. The report also refers to the effectiveness of the UK's regime. Of particular interest to us is the support for the risk-based approach to supervision, with recommendation 23 being graded 'largely compliant'. Despite this, we are continuing to work on some of the recommendations made by the report. Measures include creating our new Financial Crime and Intelligence Division and starting several new workstreams to strengthen our efforts on financial crime.

It is important to note that, while the full report makes a number of recommendations on perceived gaps in the UK system, we will address most of these when the Money Laundering Regulations 2007 take effect on 15 December 2007. This is when the EU's Third Money Laundering Directive is implemented (see the article on page 3 for the work we are doing to implement these regulations).

In addition to the mutual evaluation outcome, the UK, with significant FSA support, achieved an important milestone when the FATF Plenary adopted a paper co-submitted by Philip Robinson (Director of our Financial Crime and Intelligence Division). This paper offers guidance to both territories and institutions on implementing a risk-based approach to financial crime.

Our work on property fraud

We recently completed work to improve our understanding of property fraud, relating to both residential and commercial mortgages. The work sought to understand the way such fraud works, so we have a better chance of mitigating the risks associated with it in the future.

Residential property fraud can take one of two forms: one-off income inflation fraud perpetrated by individuals (those trying to buy a larger home, for example), and organised fraud using a network of complicit individuals in a systematic criminal attack on the financial sector.

Commercial property fraud occurs when the rental potential of properties is manipulated to inflate the value of the property. Our work paid specific attention to organised residential and commercial property fraud.

Our findings confirmed that:

- To conduct both organised residential and commercial property fraud, there must be at least two fraudsters working together. These networks are often organised by a 'controlling mind'.
- Profits from the frauds are often used as 'seed money' to fund other crimes, including those not necessarily associated with the original fraud. Examples include drug and people trafficking.

- Documents used for fraudulent mortgage applications are available to buy in the public domain and the quality is increasing.
- Fraudsters tend to target certain locations, for example areas where house prices are rising or where there are new developments.

We are now working with the industry to gain better data on the scale of this fraud.

Boiler rooms

We do not authorise boiler rooms. They act illegally by promoting and selling shares in the UK that are overpriced, restricted for onward sale and have little or no realisable value. The boiler rooms then often vanish, leaving the investor – who may have committed their life savings – out of pocket.

Boiler rooms are mainly based outside the UK, so we are usually unable to take direct action to shut them down. A City of London police threat assessment conservatively estimates that, in total, victims of this type of organised fraud annually lose over £50 million. It also suggested the victims of boiler rooms tend to be male, over 50 years old and experienced investors with a long history of investing.

Clearly consumers should always be cautious when called out of the blue by anyone promoting or offering to sell shares, and at least check that the firm is authorised by us. But boiler room fraud may have a direct impact on financial institutions: for example, banks and building societies will lose deposits.

One financial institution seeks to tackle boiler room fraud by, among other things:

- using information on our website on unauthorised firms;
- searching transactions for key words such as ‘share purchase’; and
- maintaining a database of accounts they believe may be connected to boiler room fraud.

Of course, firms have a legal obligation report any suspicious activity of money laundering or proceeds of crime to SOCA.

Firms may wish to refer customers to our MoneyMadedclear website which contains more information on boiler room fraud:

www.moneymadedclear.fsa.gov.uk/news/share_Scams.html

We have recently closed down two boiler rooms (www.fsa.gov.uk/pages/Library/Communication/PR/2007/101.shtml). Two UK-based firms, Chesteroak Limited (Chesteroak) and Bingen Investments Limited (Bingen), incorporated in Gibraltar, have been placed into compulsory liquidation by the High Court for helping boiler rooms. The boiler rooms were unlawfully promoting and selling shares to UK investors and, we believe, about 800 investors sent money for shares to the two companies.

Firms can email information about possible boiler room fraud activity to the City of London Police at operationarchway@city-of-london.pnn.police.uk

Changes to financial sanctions procedures

The Treasury has recently launched a new Asset Freezing Unit, and has taken over responsibility for administering financial sanctions in the UK. The Asset Freezing Unit has been set up in line with the government’s strategy for tackling money laundering and terrorism finance, which was outlined in February this year. The new unit will increase the government’s resources in asset freezing, and will operate from 24 October 2007.

At the same time, the Treasury will also assume responsibility for all other aspects of the financial sanctions regime. The Asset Freezing Unit will become a single point of contact for financial sanctions issues. The Bank of England, which has historically performed this role for the Treasury, will remove the financial sanctions pages from its website on 23 October 2007. From 24 October, the consolidated list of sanctions targets will instead be available on the Treasury’s web pages, at www.hm-treasury.gov.uk/financialsanctions. Firms should be aware of this change to ensure their financial sanctions procedures are up to date.

For more information on the Asset Freezing Unit, please contact assetfreezingunit@hm-treasury.gov.uk.

Contact details

As ever, we welcome feedback, ideas for future issues and suggestions of how we might make the newsletter more useful for you.

Please send your comments to **financial.crime@fsa.gov.uk**. You can also use this address to tell us if you would like to receive this newsletter in future.

Financial Crime Sector Team

Lauren Jordan (Team Leader)
lauren.jordan@fsa.gov.uk
020 7066 4594

Louise Eggett (Associate)
louise.eggett@fsa.gov.uk
020 7066 3506