



Introduction by Philip Robinson

Welcome to Issue 12 of the FSA's Financial Crime newsletter. I hope you had an enjoyable Christmas break and I'd like to wish you all a happy New Year.

This theme of this newsletter is one of collaboration. In July we revealed a series of initiatives that we are putting in place to tackle the growing problem of mortgage fraud. It's a programme that requires close cooperation with regulators, law enforcement, firms and the newly established National Fraud Strategic Authority (NFSA).

The NFSA aims to coordinate the public and private sectors effort to make the UK a hostile environment for fraudsters. This is of particular importance at a time when firms believe that financial crime is on the increase, as shown in the results of this year's financial crime perception survey, which also attempts to measure how successful we are in tackling financial crime.

One of the key findings of the survey was the need for a greater focus on small firms, to ensure that they are adequately equipped to cope with the threat of financial crime to their business. In current conditions it is vital that companies are alert to the dangers of financial crime and are able to protect their revenue streams. We are in the middle of the visit programme of our thorough review of the anti-financial crime systems and controls that small firms have in place. We will complete the programme of visits mid-2009 and intend to publish a full analysis of the review findings late next year.

It is not just domestically that there is a need to collaborate. The scourge of boiler room fraud requires us to think beyond our shores and seek international collaboration. We organised our first ever International Boiler Room Conference in November 2008. This was attended by regulators, banks and law enforcement agencies from over twenty jurisdictions to discuss and share tactics for tackling this menace.

You can find out about our work in these areas and more by following the links below.

As always, we would greatly appreciate your feedback on our newsletter, to help us ensure that the content is relevant and tailored to your needs. You can help us by completing this **short survey**.

Index

News articles

- Boiler rooms: raising consumer awareness
- Tackling mortgage fraud
- Stakeholder perceptions survey
- Small firms project update
- Data security: customer communications

News in brief

- Home Office identity theft initiatives
- APACS card fraud figures
- Enforcement actions: Aon Ltd and – Syndicatum Holdings
- Philip's BBA speech



Philip Robinson – Director
Financial Crime and Intelligence Division

Share scams: raising consumer awareness

We held the first ever International Boiler Room Conference in London in November 2008. The event brought together international law-enforcement, securities regulators and industry stakeholders from over twenty countries, to show that together we can be more creative and more persistent than our opponents.

The topic was discussed frankly and openly, in a constructive atmosphere, with plenty of ideas generated for improving international co-operation. Overall it was considered a success.

A share scam (also known as a 'boiler room') is one where potential investors are cold called (often from overseas) and pressured into buying worthless shares which often prove to be non-existent. We have estimated the size of the problem at £200 million in the UK every year, others have estimated that it is as high as £500 million.

Our Consumer Helpline receives around 5,000 enquiries per year about share scams. At the conference, Jonathan Phelan, Head of Retail Enforcement at the FSA explained our approach to tackling this menace.

Our strategy has three elements (known as the 3Ds)

- 1 Deterrence** – to share scams deter boiler rooms and those contemplating helping them.
- 2 Disruption** – to disrupt the activities of the criminals who operate the share scams.
- 3 Discouragement** – to discourage consumers from dealing with unauthorised firms.

Deterrence: We believe that our enforcement activities make a real impact to the problem posed to the public by share scams. Because of the international nature of this activity, jurisdictional and resource limitations prevent us from taking court action in every case. However, we have had success in this area, working with the British Columbia Securities Commission, the Ontario Securities Commission and the US Attorney's office we were able to secure \$2m in compensation for consumers.

Disruption: Our disruption tactics include working with web hosts to take down the websites of share scams, naming suspected share

scams on our website and alerting local regulators to the problem.

Discouragement: Because of jurisdictional problems, we believe that the most effective strategy is to warn consumers about the dangers. We recently notified around 11,000 UK shareholders that their personal details are on a 'suckers list' shared by fraudsters, which we received from the Canadian authorities.

In addition to our significant media work (over 120 appearances in the last year) to warn consumers about share scams, we continue to develop new initiatives, such as:

- **warning leaflets** to companies, registrars and FSA regulated firms, for them to send to shareholders and customers; and
- publishing a list of known unauthorised overseas firms on our **corporate** and **consumer** websites.

If you would like to join the fight against boiler rooms and help warn people, ask your customers and stakeholders to please use this material.

Finally, if you become aware of a share scam please complete our **online reporting form**. We would also encourage you to report the matter to the City of London Police **Operation Archway**, the national reporting system for share scams.

Tackling mortgage fraud

In July, we set out a programme of work to **tackle mortgage** fraud which emphasised the need for a coordinated response from the mortgage community.

The key elements of our approach include:

- a programme of targeted supervisory visits to assess firms' financial crime systems and controls;
- strengthened engagement and enhanced information sharing, with partners including law enforcement, regulators, the National Fraud Strategic Authority (NFSA), regulated firms, and within the industry itself; and
- a review of the role of the Approved Persons regime as it relates to mortgage intermediaries.

We are already seeing the benefits of this enhanced approach. There has been a steady increase in the number of lenders participating in the Information

From Lenders (IFL) scheme and a corresponding increase in the amount of intelligence we've received. This has allowed us to take tough regulatory action – this year we have prohibited 26 individuals and issued fines of over £500,000. We have also passed cases to the police for criminal prosecution, reinforcing our message of credible deterrence to those who may be tempted to abuse the system. We've subsequently announced a new system to encourage mortgage brokers to report information to us.

More details, including a link to the reporting forms, are available on our new **webpages for smaller firms**.

We said in July that our approach forms part of the UK's wider response to the issue and focuses on greater partnership working with the National Fraud Strategic Authority (NFSA), regulators, trade associations and law enforcement agencies.

Last month the NFSA published the **UK's wider strategy to tackling the problem**. The report follows a series of workshops and analysis that involved lead players in the mortgage sector.

In publishing the report, the Attorney General, Baroness Scotland, lead government minister on fraud, pointed to the encouraging range of industry initiatives already in place but endorsed the call for greater action.

Four key areas of improvement were identified:

- 1 Designing-out the fraud risks inherent in different mortgage products and processes.
- 2 Instigating preventative safeguards and controls within firms at the right level to make mortgage fraud easier to spot and stop.
- 3 Ensuring professional integrity amongst key professional sectors.
- 4 Driving-up the risk to perpetrators through more effective detection and prosecution.

We will continue with our concerted drive to enhance defences against mortgage fraud. Intelligence sharing is a key part of this strategy. In addition to putting in place formal arrangements for us to share intelligence with key partners, we will be reviewing whether mandatory participation from lenders in the IFL project is appropriate.

Stakeholder perceptions survey results

We have now published the results of our follow-up survey to gauge industry perceptions of financial crime trends and threats and our performance in tackling them since 2006. The results help inform policy making, and contribute to our formulation of emerging risks. You will see these outlined in our Financial Risk Outlook (FRO) and Business Plan documents to be published later this quarter.

Overall, the findings from this year's survey show many consistencies with 2006. Generally financial crime continues to increase, albeit at a slower rate, and the overall ease of making a business case for resources for financial crime has remained largely the same. In terms of specific risks, firms identified data security as their main priority, followed by money laundering. Large firms were much more likely to have increased the priority of corruption and terrorist financing, compared to small firms.

It is an encouraging sign that senior management in the majority of large firms are making tackling financial crime an increasing business priority, and so are more likely to invest in resources. This could be linked to their slightly more pessimistic outlook on the likelihood of financial crime increasing in the future.

Smaller firms are more likely to believe that financial crime is decreasing, or is remaining at the same level. They are also less likely to see financial crime as a priority and invest resources into strengthening their defences, preferring instead to adapt or change existing processes. This lends further weight to our current focus on smaller firms' anti-financial crime controls and the major thematic project outlined later in this newsletter.

In terms of our performance, the overall picture is mainly consistent. There have been some small but significant improvements with small retail firms and our rating by the larger firms is slightly less polarised. Large retail firms continue to be the group most critical of our performance, with small retail firms being the most approving.

We are still perceived as marginally more effective at combating money laundering than fraud. This could be linked to the perceived amount of guidance on implementing a risk-based approach available; firms feel strongly that there is much

more available on money laundering than there is on fraud. Although the overall perception is that we have improved our levels of guidance on the latter.

Views on the effectiveness of the new money laundering regime remain mixed. However, those views appear to be linked to how easy or difficult a firm finds the implementation of the risk-based regime. Either way, the message is clear: firms are against the introduction of more detailed rules.

Finally, the vast majority of respondents continue to be of the view that we should keep a role on financial crime in the future. In particular, to share intelligence and provide clarity on best practice.

We would like to extend sincere thanks again to those who took part in the study. You can find a link to the full results at <http://www.fsa.gov.uk/pubs/other/perceptions.pdf>.

Small firms thematic review – update

We are over halfway through the visit programme in the review of financial crime systems and controls in small firms and we thought that you may find it helpful to know a bit more about the background to the project.

The review was commissioned in response to findings detailed within the Financial Action Task Force (FATF) mutual evaluation of the UK, which indicated that we have, in the past, placed more focus on supervising the larger firms.

This is the largest review of small firms' anti-financial crime controls ever undertaken by us, around 200 small firms being selected for review as a representative sample from the regulated population. The review is being led by our Financial Crime Operations team, with support from the Small Firms and Contact Division and Wholesale Small Firms Division.

Planning for the review began in early 2008 and visits to the 200 small firms sampled began in May, with all visits anticipated to be completed by the middle of 2009.

Our visit teams are discussing their findings with the firms and we intend to publish a full analysis of the review findings late 2009. As with previous financial crime thematic work, the results will provide a summary of good and poor practices

identified during visits, which firms can use to benchmark and improve their own practices.

Data security: customer communications

Think about when you send out communications, such as promotional offers and annual statements to your customers. Do you take appropriate steps to reduce the risk of your customers becoming victims of identity fraud and other crimes? Our research indicates that the answer may well be 'no'.

In April 2008 we published the findings of a major piece of thematic work looking at firms' controls around personal data. The key findings of this work identified that poor data security is a serious and widespread problem throughout the financial services industry.

As a follow-up to this work, we have been reviewing the way that firms disclose personal data in the various communications they have with their customers. Our work has identified some worrying examples, where firms have used personal data unnecessarily or with greater frequency than really needed. For example, a large fund-management firm sent out monthly statements that included answers to the security questions a caller would need to provide to access the account and effect transactions (including the only piece of non-public authentication information). This compromised the security of the accounts.

Further information on this subject and steps that you can take towards enhancing your data security procedures are available on our [website](#).

News in brief:

Home Office identity theft initiatives

Latest figures published by the Identity Fraud Steering Committee (IFSC) show the new estimate for the cost of identity fraud to the UK economy to be £1.2 billion – that's £25 for every adult in the UK.

To help tackle identity fraud and drive down the cost to the economy, two initiatives are being introduced for the first time.

- Death records are to be released to vetted organisations, such as credit-checking agencies. This should make it much easier to detect fraudulent activity, such as the takeover of a recently deceased person's identity to open bank or credit card accounts.
- New identity cards for foreign nationals are to be rolled out as part of the National Identity Scheme from 25 November. The card will contain a biometric chip to make it more secure against forgery and abuse.

For further information refer to the Home Office websites: **UK Border Agency** and **Identity and Passport Service**

APACS release card fraud figures

APACS, the UK payments association, have released their **card fraud figures** for the first half of 2008.

The figures show that total card fraud losses increased by 14% to £301.7m compared to the same period in the previous year. More than 40% is the result of fraud abroad – typically criminals exploiting countries that have yet to upgrade to chip and PIN.

The figures show that chip and PIN has certainly made it more difficult for fraudsters to commit card fraud in the UK. Overall fraud on lost and stolen cards has fallen by 38% in the past three years to £27.3m and is now at its lowest level for ten years.

However, criminals continue to target UK-issued cards, copying the magnetic stripe data and creating counterfeit magnetic stripe cards that can potentially be used fraudulently in countries that

haven't yet upgraded to chip and PIN. This has caused a 190% increase in losses abroad over the last three years, which now total £121.2m. This type of fraud will become more difficult to commit when the European banking industry meets its target to complete its chip card rollout by 2010.

Online banking fraud losses have seen the biggest increase, totalling £21.4m during the six months to June 2008, a 185% rise compared to 2007. The increase is largely due to increased phishing and spyware scams. Losses from phone, internet and mail order shopping fraud have also increased year on year and now stand at £161.9m, 54% of all card fraud losses.

APACS has urged shoppers to protect themselves when banking and shopping online by installing up-to-date anti-virus software on their computer, only using secure websites and registering with MasterCard SecureCode and Verified by Visa when prompted.

Help and advice about preventing all types of online banking fraud is available at www.banksafeonline.org.uk.

Enforcement action – Aon Ltd

On Thursday 8 January 2009, we fined Aon Ltd £5.25 million for failing to take reasonable care to establish and maintain effective systems and controls to counter the risks of bribery and corruption.

As a result of Aon Ltd's weak control environment, the firm made various suspicious payments, amounting to approximately US\$7 million, to a number of overseas firms and individuals.

This is the largest financial crime related fine imposed by the FSA to date and sends a clear message to the UK financial services industry that it is completely unacceptable for firms to conduct business overseas without having in place appropriate anti-bribery and corruption systems and controls.

We are currently conducting a thematic review into the adequacy of the systems and controls in place at a number of commercial insurance intermediary firms for preventing illicit payments and inducements particularly through the use of overseas third parties. Following the results of

that project we will consider whether to undertake any wider thematic work.

Enforcement action – Sindicatum Holdings

On 29 October 2008, we fined Sindicatum Holdings Ltd (SHL), a corporate advisory firm, £49,000 for failures relating to its anti-money laundering systems and controls and for not adequately verifying and recording its clients' identities.

We also fined Michael Wheelhouse, SHL's money laundering reporting officer, £17,500 in relation to his failures in overseeing and implementing the anti-money laundering systems and controls at SHL.

In particular, we found that:

- SHL failed to implement adequate procedures for verifying the identity of its clients;
- SHL failed to verify adequately the identity of a significant number of its clients;
- SHL failed to keep adequate records to verify of the identity of its clients; and
- Mr Wheelhouse failed to take reasonable steps to implement adequate procedures for verifying the identity of the Firm's clients.

Both fines reflected a 30% discount for settling with the FSA. The penalty also reflected the limited financial resources of the firm and its ability to pay the fine.

This is the first time the FSA has fined an MLRO for weak anti-money laundering controls and it is a warning to firms and individuals about the importance of complying with our requirements in this area.

Philip Robinson BBA speech

Philip Robinson spoke at the BBA's 6th Annual Financial Crime Conference, setting out our agenda for fighting financial crime in 2009. In the speech, Philip outlined the financial crime risks that we are seeing in the current economic climate and the subsequent areas of regulatory focus. Philip also emphasised the need for the anti-financial crime community to work together in order to stay ahead of the criminals and the importance of senior management setting the right culture for their organisation: one which focuses on operational

risks such as financial crime, in addition to prudential and financial stability issues.

You can read the full speech [here](#).

Upcoming events

Our Annual Financial Crime conference will take place on Monday 27 April 2009. Details will follow shortly and in the meantime don't forget to mark the date in your diary.

Contact details

If you would like to be added to our distribution list to receive this newsletter, or have any questions about the content please email us at financial.crime@fsa.gov.uk