Financial Services Authority

Banks' defences against investment fraud

Detecting perpetrators and protecting victims

June 2012

Contents

1 Executive summary

Introduction

1.1 Firms authorised by us have a regulatory duty to counter the risk they might be used to further financial crime. This report considers banks' efforts to counter fraud where a) their customer is the fraudster or b) their customer is the victim. We do this by examining measures banks take to counter a particular type of fraud: investment fraud. We have a regulatory remit to tackle investment fraud, which has prompted our particular interest in this area, although the lessons of this report can be applied to banks' handling of other types of fraud and criminal conduct affecting their customers.

CONSULTATION

The examples of good and poor practice found during the review are set out at the end of each chapter, and consolidated in section 11. As these examples constitute guidance from the FSA, we are consulting on them. Section 12 sets out the consultation process and how you can engage with it. After consultation, this material will be added to the FSA's publication, *Financial crime: a guide for firms*. This was published in December 2011, after the fieldwork for this review had begun.

Findings

1.2 Most banks argued investment fraud was not a significant issue, compared with other financial crime risks they and their customers faced. Such statements, however, were not supported by systematic analysis of the evidence; for example, we saw no assessments of financial crime risks that included investment fraud. It followed that:

- the processes for allocating resources to this issue appeared haphazard and not the result of purposive decision-making by senior management;
- we saw no clear assessments of whether controls to counter the risk of investment fraud were effective; and

- we saw little management reporting on how banks' customers had become victims of investment fraud, or of the volumes and trends.

1.3 In short, senior management appeared to have little interest in the issue and there was consequently little systematic governance of the specific risk of investment fraud.

1.4 We were disappointed with banks' ability to detect where their customers may be complicit in investment fraud (e.g. where a customer uses their account to receive payments from victims). Banks' customer due diligence measures did not, for example, use anticipated turnover information collected when commercial accounts were opened to inform subsequent transaction monitoring. Assessments of the risk posed by individual customers were heavily dependent on the knowledge of the staff member who was opening the account to collect the right information and challenge it as necessary. A lack of awareness of common investment fraud typologies could cause misclassification at this stage, which could affect how much attention the relationship subsequently received. Risk assessments on customers were not usually updated as the relationship with the customer developed over time. Ongoing monitoring of the customer was often the responsibility of customer-facing staff, who have many other responsibilities. These findings are relevant to banks' anti-money laundering measures more generally, so they raise serious concerns.

1.5 During our review, we observed a range of transaction monitoring technologies. One bank had had notable success in preventing customers falling victim to investment fraud through adding potential investment fraud perpetrators to its existing payment screening technology. Three banks had successfully used real-time payment screening to detect and prevent substantial volumes of payments to investment frauds by banks' customers. The success of payment screening, however, appears heavily dependent on the quality of the information used in the screening process.

1.6 None of the banks visited provided clear reporting to senior management on the level of investment fraud identified. This was in contrast to the reporting observed for other types of fraud, particularly fraud where the bank is financially exposed.

1.7 We saw several good examples of banks maintaining intelligence on investment fraudsters, although measures were inconsistent across the industry. Not all of the banks visited attended the industry forum on boiler rooms, and there appeared to be a reluctance to share experiences and intelligence formally, because of concerns over legal liability.

1.8 Communication with customers relating to investment fraud varied. Some banks had, or were considering, writing to customers they regarded as being at higher risk to warn of the dangers. But most banks' efforts were more limited. Many banks contact customers individually if they suspect a payment is being made to an investment fraudster. Some banks saw barriers to doing this that others had felt able to surmount.

1.9 While most of the management and staff interviewed understood the principle of investment fraud, the depth of understanding varied considerably. Some subject matter experts demonstrated an excellent understanding, but knowledge gaps among front-line staff could undermine the effectiveness of their ongoing monitoring of customer relationships.

Conclusion

1.10 While our review found individual staff members with a strong commitment to protecting customers, we saw little governance of the specific issue of investment fraud. Resource allocation was not based on documented risk assessments (which did not explicitly consider this risk) and was hence haphazard and not the result of purposive decision-making by senior management. As a consequence, it was not clear to us that the banks we visited had fulfilled this aspect of their regulatory obligation to counter the risk they might be used to further financial crime.

1.11 We were particularly disappointed with banks' ability to detect where their customers may be complicit in investment fraud. Ongoing monitoring of the customer was often the responsibility of customer-facing staff with many other responsibilities, who often lacked the knowledge to identify investment fraud. More positively though, we saw a range of transaction monitoring technologies, and some banks had used these successfully to preventing customers falling victim to investment fraud. We also saw good examples of banks maintaining intelligence on investment fraudsters, although measures were not consistent across the industry. Communication with customers relating to investment fraud also varied; some banks contacted potential victims individually, but others did not.

1.12 Although the review concentrated on investment fraud, it has wider relevance to how firms handle other types of fraud and criminal conduct affecting their customers. It is also relevant to how they fulfil their broader anti-money laundering responsibilities.

2 Introduction

Background

2.1 Financial firms have a regulatory obligation to counter the risk they may be used to further financial crime, including fraud. Financial firms have a long track record of taking measures to reduce their own losses from fraud. But how do they counter fraud where:

- the victim is their customer, or a third party; or
- the firm's customer is committing fraud?

2.2 We have considered this question in relation to a specific type of fraud that affects banks' customers: investment fraud. The lessons of this report can also be applied to how banks handle other types of fraud and criminal conduct causing detriment to their customers.

Investment fraud

2.3 We estimate UK consumers lose over £500 million every year to share sale frauds and other scams including, but not limited to, land-banking frauds, unauthorised collective investment schemes and Ponzi schemes. Our past investigations have shown there are usually UK-based bank accounts involved in these schemes: some belong to the victims; others receive the proceeds of these frauds. The main types of investment fraud are outlined in Table 1.

Table 1: Types of investment fraud[1]

Scheme	Description
Boiler rooms/share sale fraud[2]	Share scams are often run from 'boiler rooms' where fraudsters cold-call investors offering them often worthless, overpriced or even non-existent shares. While they promise high returns, those who invest usually end up losing their money. We have found victims of boiler rooms lose an average of £20,000 to these scams, with as much as £200m lost in the UK each year. Even seasoned investors have been caught out, with the biggest individual loss recorded by the police being £6m. We receive almost 5,000 calls each year from people who think they are victims of boiler room fraud.
Land banking[3]	Land banking companies divide land into smaller plots to sell it to investors on the basis that once it is available for development it will soar in value. However, the land is often in rural areas, with little chance of planning permission being granted.
Ponzi and pyramid schemes[4]	Ponzi and pyramid schemes promise investors high returns or dividends not usually available through traditional investments. While they may meet this promise to early investors, people who invest in the scheme later usually lose their money; these scheme collapse when the unsustainable supply of new investors dries up. Investors usually find most or all of their money is gone, and the fraudsters who set up the scheme claimed much of it for themselves.
Carbon credit schemes[5]	We are receiving an increasing number of reports from people who have been approached by firms promoting carbon credit trading schemes. Firms may try to sell carbon credit certificates or get investors to invest directly in a 'green' scheme or project that generates carbon credits as a return on their investment. Carbon credits can be sold and traded legitimately and there are many reputable firms operating in the sector. However, we are concerned an increasing number of firms are using dubious, high-pressure sales tactics and targeting vulnerable consumers.
Unauthorised Collective Investment Schemes	As well as land banking and carbon credit schemes, investors can also fall victim to other types of investment scam that are set up as an unauthorised Collective Investment Scheme.

2.4 Our own work to tackle investment fraud has raised concerns about how some banks handled customers who posed a high risk of perpetrating an investment fraud. Box 1 shows some case studies. Concerns over examples such as this is one reason for our focus on investment fraud in this review.

1 www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams
2 www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams/boiler_room
3 www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams/land_banking
4 www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams/ponzi_pyramid
5 www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams/carbon_credit

Box 1: case studies of banks' behaviour

These case studies were not generated by this review, but by our wider work to tackle investment fraud.

A carbon credit trading scam

In 2005, Bank Z opened an account for Business A, which said it was an IT contractor. Account opening data estimated annual turnover to be £200,000. Until late 2010, account turnover was negligible, but then rose markedly to be greater than £1m annually. The account received many transfers (by cheque, BACS and CHAPS) from a range of sources. This did not trigger any form of review by Bank Z. Business A was investigated by us as a carbon credit trading scam.

A land banking scheme

Bank P opened an account for Business B, which described itself as a commercial land agent. Account opening information estimated annual turnover to be £600,000, with retained income of £500,000. There was no explanation of how money would be generated by this business. Account activity showed many payments from retail customers, rather than commercial counterparties. Bank P did not submit a suspicious activity report on Business B, which subsequently opened an account with Bank Q, which did. This led us to take out a freezing order and restrain over £800,000 from this land banking scheme.

A 'get rich quick' scheme

Several accounts were opened at Bank Y by Business C that said it provided training for the financial services industry at locations throughout the country. Account opening information estimated annual turnover to be about £100,000. In fact, Business C received payments of £25m over four years. At its peak, this 'get rich quick' scheme received £1m from its 'investors' per month. About £20m was paid out over the same period covering business expenses, substantial payments to investors as well as payments to fund the lifestyles of the scheme's organisers. Bank Y did not submit a suspicious activity report on these accounts.

Method

2.5 We appointed a third party to review the systems and controls at eight deposit-taking institutions (seven banks and one building society). (For simplicity the term 'bank' is used throughout this document). The sample selected was designed to provide high coverage of the British retail banking market: 80% of the market was included. We set the parameters of the review and an FSA member of staff attended all visits. This document draws substantially on the third party's findings, although the judgements made here are ours.

Banks' regulatory obligations

2.6 Firms authorised by us have a regulatory duty to counter the risk they might be used to further financial crime. Our rules and guidance do not, however, articulate specific requirements related to banks' handling of the risks posed by investment fraudsters.

2.7 Several legal and regulatory obligations are relevant, both to the identification of a) customers who are potential victims, and b) customers who may be complicit in an investment fraud. Firms have obligations under the Proceeds of Crime Act 2002, the Money Laundering Regulations 2007 and our rules to:

- identify customers (and understand the nature of the business relationship);

- monitor account activity;
- report suspicious activity to the Serious Organised Crime Agency; and
- have policies and procedures in place to prevent activities related to money laundering and to counter the risk of being used to further financial crime.

2.8 What does this mean in practice? Our understanding of the measures banks take to counter the risks posed by investment fraudsters has previously been based on anecdotal accounts. We intend this thematic review, based on a systematic series of in-depth visits to our sample of banks, to help us build a picture of good and poor practice, and hence inform our expectations of what firms should achieve.

2.9 The examples of good and poor practice found during the review are set out at the end of each chapter, and consolidated at the end in Section 11. As these examples constitute guidance from the FSA, we are consulting on them. Section 12 sets out the consultation process and how you can engage with it.

2.10 After consultation, this material will be added to our publication, *Financial crime: a guide for firms*. This was first published in December 2011, after the fieldwork for this review had begun.

2.11 Some banks expressed concern that delaying a payment could lead to a breach of the Payment Services Regulations, which set requirements for the timing of payments (see 7.11). Those Regulations do, however, allow banks to delay payments in order to comply with other legal obligations, including regulatory requirements: the regulatory duty firms have to counter the risk they might be used to further financial crime will be relevant here. If there are strong grounds for suspecting a payee is a fraudster, these obligations are likely to be engaged; this means firms can delay payments while concerns about the payee are discussed with the customer.

2.12 Another aspect of our regulatory regime considered relevant by some firms is the general prohibition on providing investment advice (see 7.13). Some banks expressed concern that warning customers about a payment to a prospective investment fraudster could be considered investment advice, and is hence in breach of this prohibition. We believe it is perfectly possible to warn customers about the dangers of falling victim to investment fraudsters without providing investment advice. We routinely offer warnings to members of the public who have contacted us, and are comfortable with firms' staff doing the same.

3 Governance

Introduction

3.1 **This chapter is relevant to both banks' efforts to detect customers who are complicit in investment fraud, and to the detection and protection of customers who are victims.**

3.2 Our assessment of the banks' governance of financial crime risks relating to investment fraud included interviewing senior management, reviewing documented policies and procedures (where available) and reviewing documentation on the operation of the governance of financial crime and escalation of relevant matters. This included a review of minutes of the meetings cited by banks as integral to managing risks relating to investment fraud.

General observations

3.3 The banks generally had clear organisation structures in place for countering financial crime risks. These typically considered fraud and anti-money laundering (AML) separately, and reported performance against pre-agreed metrics for each area.

3.4 Most banks visited did not consider investment fraud to be a current significant issue to their customers or organisations, compared with the other financial crime risks they faced (see next section).

3.5 The banks visited were generally unable to demonstrate a mature and comprehensive framework for the governance of risks relating to investment fraud, whether as a specific issue, or as part of a broader anti-fraud framework.

3.6 Many banks argued investment fraud perpetrated by a customer of the bank was chiefly addressed through their existing anti money-laundering procedures.

3.7 In no bank did we see procedures that comprehensively addressed the risk of investment fraud perpetrated by a third party against the bank's customer. Approaches could differ between fraud teams and anti-money laundering units within the same organisation.

3.8 There appeared to be uncertainty at the banks visited about where within the organisation risks relating to investment fraud should be considered. A summary of who was responsible for detecting perpetrators and victims at each bank is outlined in Table 2 below.

Table 2: Summary of responsibility at the firms visited for detection of perpetrators and victims of investment fraud

	Detection of perpetrators	Detection of potential victims
Bank 1	AML Team	Fraud Team & AML Team
Bank 2	AML Team	Fraud Team
Bank 3	AML Team	AML Team
Bank 4	AML Team	AML Team
Bank 5	AML Team	AML & Payments Teams
Bank 6	AML Team	AML & Payments Teams
Bank 7	AML Team	AML Team
Bank 8	AML Team	Fraud Team

3.9 Several of the banks visited said they had a clear commitment to protecting their customers from financial crime. It was not clear how some of these banks delivered this commitment in respect of investment fraud.

One bank visited had developed a team to consider the risk to a customer arising from payments to boiler rooms. The team actively sought industry intelligence and used this to build a 'watch list'. Specially trained staff contacted customers where payments to potential boiler rooms were identified by payment screening filters and explained the risks of making the payment. This resulted in stopped payments of over £1m over three years.

3.10 There was no clear rationale expressed by the banks for allocating resources to managing investment fraud. While detailed metrics were in place for other types of fraud, we saw no measures that could be used by senior management to judge how much resource should be allocated to the issue. We noted most banks had invested resources to detect and mitigate investment fraud (in particular, relating to boiler rooms) in 2009, a time of heightened awareness of 'boiler room' activity.

A bank had a defined centre of excellence for investment fraud-related cases. The resource in this area demonstrated a particularly strong understanding of steps necessary to detect investment fraud activities. Employees at the firm were made aware that suspicions should be escalated to this team. The team also had a significant input to developing specific training for their colleagues on investment fraud, using cases they had investigated.

3.11 None of the banks visited clearly reported to senior management on the level of investment fraud observed within the banks. This was in contrast to the reporting we saw in place for other types of fraud, particularly fraud where the bank was financially liable.

The role of anti-money laundering teams

3.12 The anti-money laundering teams generally considered their roles to be to identify and escalate suspicion relating to the perpetrators of investment fraud. Most of the banks visited told us that, because they did not have an obligation to identify the exact nature of the activities reported to the Serious Organised Crime Agency, they could not report, either internally or to us as a part of the review, how many perpetrators of investment fraud had been identified.

3.13 A number of banks visited said their ability to protect customers from investment fraud was heavily dependent on the intelligence shared between banks on likely cases. None of the banks visited identified their own anti-money laundering monitoring as a potential source of intelligence. The absence of such investigations may be directly affecting the quality of intelligence shared between banks, and therefore the banks' ability to protect customers. This is considered in further detail in Section 11.

The role of fraud teams

3.14 Most of the fraud teams at the banks visited focused on fraud against the bank committed by customers or staff. While there was detailed and well-structured management reporting and monitoring of many types of fraud, we saw very few examples of clear reporting of customer losses resulting from investment fraud.

One bank, having told us that investment fraud was not an issue for their customers, presented cases that showed for a certain period the potential monetary losses from suspected investment fraud on their customers exceeded the combined value of the other types of fraud identified. Senior management at the bank had not considered this comparison before our visit.

3.15 While most respondents acknowledged that investment fraud is an international problem, we saw no examples of the larger banking groups using their international networks for intelligence or investigation.

One bank had invested significant time in 2009 to understand how their systems could be used to detect and prevent investment fraud. However, the specific recommendations and measures that had been identified had not been developed or implemented at the time of our visit. So, despite recognising that there were measures that could be taken to address investment fraud, the bank had not followed this up due to competing priorities.

3.16 We were concerned that communication between the AML and fraud functions on investment fraud was inadequate. The fraud team's role was often to identify whether a customer actually made a transaction, rather than to identify where the payment was to someone seeking to defraud the customer, and we saw little communication of concerns between the AML and fraud teams that a transaction could, once executed, become the proceeds of crime.

Conclusion

3.17 There appeared to be little effective governance of the specific area of investment fraud. We recognise banks have a number of financial crime-related risks to manage. Most banks argued investment fraud was not a significant issue, compared with other financial crime risks they and their customers faced. But these statements seemed based on supposition, rather than backed by an evidence-based assessment of the risks (see next section.) This may explain why, for example, resource allocation appeared haphazard.

3.18 We expect firms to be able to demonstrate that the level of resources allocated to investment fraud is the product of a purposive choice by management based on a sound assessment of the risks.

Governance: examples of good and poor practice

Governance	
Examples of good practice	**Examples of poor practice**
• A bank can demonstrate senior management ownership and understanding of fraud affecting customers, including investment fraud. • There is a clear organisational structure for addressing the risk to customers and the bank arising from fraud, including investment fraud. • There is evidence of appropriate information moving across this governance structure that demonstrates its effectiveness in use. • A bank has recognised subject matter experts on investment fraud supporting or leading investigations. • The monetary value of sums saved for customers are used as a performance indicator. • When assessing the case for measures to prevent financial crime, a bank considers benefits to customers, as well as the financial impact on the bank.	• A bank lacks a clear structure for the governance of investment fraud or for escalating issues relating to investment fraud. Respective responsibilities are not clear. • A bank lacks a clear rationale for allocating resources to protecting customers from investment fraud. • A bank lacks documented policies and procedures relating to investment fraud. • There is a lack of communication between a bank's AML and fraud teams on investment fraud.

4 Risk assessment

Introduction

4.1 **This chapter is relevant both to banks' efforts to detect customers who are complicit in investment fraud, and to the identification and protection of customers who are victims.**

4.2 We expected to review the management of risk relating to investment fraud by looking at:

- risk assessments of investment fraud risks (whether as stand-alone pieces of work or wider exercises); and
- assessments of the adequacy of controls in this area.

4.3 However, as outlined below, we saw no comprehensive examples of investment fraud having been considered explicitly in a manner that informed the bank's wider financial crime risk assessment.

Observations

4.4 We saw no clear connection between a bank's assessment of the threat of investment fraud and the measures that had been implemented to detect or prevent investment fraud at any of the banks visited.

4.5 While we saw several good examples where the threat of investment fraud had been considered, it was not clear that these had informed the organisation's risk assessment. It was therefore difficult to conclude that the general response of banks visited in this area was risk-based. We consider this to be the root cause of several concerns identified as a part of this review.

One bank had performed a detailed threat assessment that considered investment fraud explicitly. This threat assessment evidently considered both internal and external intelligence on investment fraud. However, the bank was unable to show evidence of a link between this assessment and their fraud risk assessment. Consequently, we found that the bank's reaction to investment fraud was not consistent with this threat assessment.

4.6 Senior management at many of the banks visited stated that the issue was not a significant problem for their firm. In the absence of a well-considered risk assessment, it was difficult for senior management to demonstrate how they had reached this conclusion.

4.7 There was some evidence of 'horizon scanning' in respect of investment fraud. This means that some firms were reviewing the available published material, press stories and market information to educate themselves about possible future investment scams. Some of the banks visited had clearly initiated activity following our communication notifying them of our intention to visit.

Prior to learning of our review, one bank had a system in place to assess and keep track of emerging risks as well as the actions put in place to address them. This had identified the FSA's past communications on investment fraud, and had brought them to the attention of senior management.

4.8 A summary of banks' efforts in respect of risk assessment, horizon scanning and whether these initiatives focused on investment fraud is outlined in Table 3 below:

Table 3: Summary of initiatives observed for risk assessment, horizon scanning and whether these initiatives explicitly considered investment fraud

	Risk Assessment incl. investment fraud	**Horizon scanning identifying investment fraud**	**Clear connection from risk to control**	**Assurance activity on investment fraud**
Bank 1	No	No	No	No
Bank 2	No	Yes	No	No
Bank 3	No	Yes	No	No
Bank 4	No	Yes	No	No
Bank 5	No	Yes	No	No
Bank 6	No	No	No	No
Bank 7	No	Yes*	No	No
Bank 8	No	Yes**	No	No

* Performed in 2009 – a time of heightened awareness of 'boiler room' activity
** Performed immediately prior to our visit

4.9 While some banks had considered financial crime risks by channel of business, no banks we visited had 'stress tested' this assessment against investment fraud as a known type of fraud.

4.10 The regulatory compliance and risk assurance functions had not looked at the risk of investment fraud in any of the banks visited. We also noted that internal audit had not considered the risk or challenged their firm's risk framework to ensure it was taken into account.

4.11 One bank visited had a robust process in place for identifying customer payments to suspected boiler rooms. But there was little evidence that other types of investment fraud had been considered. The management responsible felt the team currently dealing with boiler room fraud lacked the experience or knowledge to investigate other types of investment fraud.

Conclusion

4.12 We saw no systematic risk assessments that included investment fraud. Furthermore, we saw no clear assessment of whether the controls that had been implemented in relation to investment fraud, or wider fraud controls, were effective in mitigating the risks posed by investment fraud. This may be a consequence of the lack of organised governance in this area, as outlined in section 3.

4.13 In addition, while we saw some examples of both internal audit and regulatory compliance functions focusing on financial crime, these units had not considered the risk of investment fraud. The lack of a risk assessment had not been challenged by these functions.

Risk assessment: examples of good and poor practice

Risk assessment	
Examples of good practice	**Examples of poor practice**
• A bank has assessed the risk to itself and its customers of fraud including investment fraud and other frauds where customers and third parties suffer losses rather than the bank. Resource allocation and mitigation measures are informed by this assessment. • A bank performs 'horizon scanning' work to identify changes in the fraud types relevant to the bank and its customers.	• A bank has performed no risk assessment that considers the risk to customers from investment fraud. • A bank's regulatory compliance, risk management and internal audit functions' assurance activities do not challenge the risk assessment framework effectively.

5 Detecting perpetrators

Introduction

5.1 **This chapter is primarily relevant to banks' efforts to detect customers who are complicit in investment fraud. It also has more general relevance to the steps banks take to meet the requirements of the Money Laundering Regulations 2007.**

5.2 Accounts held at UK-based banks have been used to receive payments from victims of investment fraud. These 'collection accounts' are controlled by the fraudsters. What can banks do when opening accounts to help identify this? What can they do afterwards?

5.3 Our review in this area focused on the opening and subsequent monitoring of commercial accounts that could be used to perpetrate investment fraud. We recognise that other account types could also be used by investment fraudsters.

5.4 We had expected to observe controls that showed evidence of reviews of the type of business being opened, its ownership structure and anticipated business performance. We expected to see links between account opening information and the banks' ongoing monitoring of relationships with their customers.

5.5 Our review in this area comprised:

- Interviews with those responsible for opening, and monitoring, commercial accounts.
- Reviews of commercial account opening files, with specific focus on how potential collective investment schemes were reviewed.
- Understanding of the connection between the information provided by the commercial customer at account set-up and subsequent monitoring.

Observations

5.6 All banks visited had procedures for opening commercial accounts. These included documentation requirements and an assessment of the risk of the customer, based on the proposed business type, location and structure.

5.7 We saw strong evidence of sufficient information being collected at opening stage to enable ongoing monitoring of commercial bank accounts that could detect customers perpetrating investment fraud. This includes information on the type of business and expected turnover. However, few banks ensured that this information was followed through to subsequent transaction monitoring (see section 6).

5.8 None of the banks visited included the anticipated turnover of the commercial account in their automated transactional monitoring. This data was captured at application stage, but had not been included within the scope of the transaction monitoring.

5.9 All banks performed risk assessments of customers at account opening stage. The frequency of account reviews varied considerably. One bank, for example, performed an annual review of accounts, while another reviewed accounts only if there was a change to the nature of ownership of the customer. Some banks performed reviews more frequently for higher risk customers and in the case of certain triggers such as the raising of a suspicious activity report. Most banks did not update their risk assessment for the customer as a result of these reviews.

5.10 The levels of scrutiny of business accounts varied according to how they were managed by the bank. Most subjected higher value customers (for example. with an expected turnover greater than £1m) to more detailed scrutiny. Those business managers responsible for smaller customers could have 500 or even 1,000 accounts to monitor. Consequently, we are sceptical of the business managers' ability to monitor these customers effectively without support.

5.11 Some banks used an internally generated 'watch list' to screen new applicants to prevent the bank taking on possible investment fraud perpetrators. Others are using the list of potential investment fraud perpetrators published by the FSA for this purpose, or external commercial fraud databases. This screening was usually integrated with the banks' monitoring for politically exposed persons and so required little investment in technology. Few of the banks screened for trigger words such as 'land', 'plot' or 'carbon'.

5.12 A summary of whether each of the banks visited systemically reviewed new accounts against suspected investment fraud perpetrators is in Table 4 below.

Table 4: Summary of firms' efforts to scan new and existing customers against suspected investment fraud data.

	Scan new customers against investment fraud data	Scan existing customers against investment fraud data
Bank 1	No	No
Bank 2	No	Yes**
Bank 3	Yes*	Yes**
Bank 4	No	No
Bank 5	No	No
Bank 6	No	No
Bank 7	No	Yes 1
Bank 8	Yes 1	Yes 1

* Scanning based on FSA's published list of investment fraud perpetrators
** Scanning based on internally maintained intelligence

5.13 None of the banks visited had procedures to ensure that commercial account applications rejected as being possible investment fraud cases were fed consistently into either their own intelligence database or industry-wide intelligence efforts.

At a number of the banks visited, we found the staff opening commercial accounts had a limited level of understanding of which types of businesses should be regulated by the FSA. For example, our testing identified one case where a commercial account had been opened for a business that apparently required authorisation by the FSA, but there was no evidence the bank had checked the FSA's Register. The bank's procedures relied on the applicant disclosing they were authorised by the FSA before performing this check.

However, we also saw one example where a relationship manager escalated an application for a possible carbon credit company because he did not feel he understood the business sufficiently well. The firm rejected the application. This case demonstrated the benefit of educating front-line staff about investment fraud risks.

5.14 We saw few examples of a connection between the process banks had in place to exit a relationship and the risk assessment performed when accounts were opened. We would have expected the termination of a relationship with a customer through the account exit process to provide a rich source of intelligence for ensuring the account opening risk assessment was operating as designed.

Conclusion

5.15 None of the banks visited used anticipated turnover collected when commercial accounts are opened to inform subsequent transaction monitoring. Therefore, there is no way to systematically assess whether a commercial account shows far higher turnover than expected.

5.16 While some risk assessments that did consider the type, structure and location of the applicant, this was heavily dependent on the knowledge of the staff member who was opening the account to collect the necessary information and challenge effectively. A lack of awareness of common investment fraud typologies could cause misclassification at this stage, which could affect the degree of due diligence the account undergoes.

5.17 Quality assurance processes were focused on ensuring appropriate customer due diligence evidence was collected, but it was not clear that they focused on the adequacy of the firm's assessment of the risk posed by the customer.

5.18 Risk assessments of customers were not usually updated as the relationship with the customer developed over time. Ongoing monitoring of the customer was often the responsibility of customer-facing staff, who may be incentivised to bring in or retain business.

5.19 We had expected banks to consider the risk posed by their customers on an ongoing basis, and to feed this information through to the measures they had in place to mitigate these risks, such as automated transaction monitoring. This was not the case for most of the banks visited. As this finding is relevant to banks' anti-money laundering measures more generally, this was a finding of particular concern.

Detecting perpetrators: examples of good and poor practice

Detecting perpetrators	
Examples of good practice	**Examples of poor practice**
• A bank's procedures for opening commercial accounts include assessing the risk of the customer, based on the proposed business type, location and structure. • Account opening information is used to categorise a customer relationship according to its risk. The bank then applies different levels of transaction monitoring based on this assessment. • A bank screens new customers to prevent the take-on of possible investment fraud perpetrators.	• A bank only performs the customer risk assessment at account set up and does not update this through the course of the relationship. • A bank does not use account set up information (such as anticipated turnover) in transaction monitoring. • A bank allocates excessive numbers of commercial accounts to a staff member to monitor, rendering the ongoing monitoring ineffective. • A bank allocates responsibility for the ongoing monitoring of the customer to customer-facing staff incentivised to bring in or retain business.

6 Automated monitoring

Introduction

6.1 **This chapter is relevant both to banks' efforts to detect customers who are complicit in investment fraud, and to the detection and protection of customers who are victims.**

6.2 How can banks' ongoing monitoring of customer transactions detect where customers are complicit in investment fraud, or where customers may be about to fall victim? Automated transaction monitoring and screening activities relevant to investment fraud typically fall into the following categories:

- Account name screening: screening accounts (on opening or periodically thereafter) according to a predefined 'watch list' of customers the bank regards as high risk. The 'watch list' often used either intelligence gained from the bank's experience or the FSA's published list of investment fraud cases.
- Ongoing real time (or near-real time) fraud monitoring: this is usually designed to identify cases where an account holder did not make a particular transaction (so, for example, account takeover or card fraud).
- Post-event AML monitoring: the review of specific transactions or account activity across a period (for example, over a month) to identify unusual activity that could indicate that the bank is processing the proceeds of crime.
- Real-time payment screening: screening SWIFT and CHAPS payments against a predefined 'watch list' of investment fraudsters. The 'watch list' often used either intelligence gained from the bank's experience or the FSA's published list of investment fraud cases.

6.3 A summary of the technology adopted by each bank is in Table 5 below.

Table 5: Summary of transaction monitoring technologies used by each firm visited

	Account name screening*	Real time fraud monitoring	Post event AML monitoring	Real-time payment screening (investment fraud)
Bank 1	No	Yes◊	No◊◊	No
Bank 2	Yes	Yes**	Yes	Yes
Bank 3	Yes	Yes◊	Yes	No
Bank 4	No	Yes**	Yes	No
Bank 5	No	Yes**	Yes	No
Bank 6	No	Yes**	Yes	No
Bank 7	Yes	Yes◊	Yes	Yes
Bank 8	Yes	Yes◊	No◊◊	Yes

* Per Table 4
** Card transactions only
◊ Card and account transactions
◊◊ Integrated monitoring system with fraud monitoring

6.4 One bank had a governance forum to review the design and effectiveness of transaction monitoring rules. This forum had considered rules to identify land banking, but dismissed the possibility of transaction monitoring because of its perceived complexity.

6.5 Some banks regard their system detection rules to be commercially sensitive, and were reluctant to share their approach with other banks.

One bank had implemented a transaction monitoring system some years previously, but was unable to change the rules used to generate alerts. The rules had been defined by the vendor on set-up, and the bank had neither the knowledge nor the capability to change these to reflect their perception of the risk being monitored.

Account name screening

6.6 Some banks used an internally generated 'watch list' to screen new applicants to prevent the possible investment fraud perpetrators opening accounts. Others are using the list of potential investment fraud perpetrators generated by the FSA for this purpose, or externally purchased fraud databases. This monitoring was usually integrated with the banks monitoring for politically exposed persons and so required little investment in technology.

One bank had previously carried out sweeps of their customer database against the FSA list of known investment frauds and for 'carbon credit' in account names. Another screened account names every week against an internal 'watch list' of potential

investment fraudsters to help manage the risk that customers (both new and existing) are perpetrating investment fraud.

Real-time fraud monitoring

6.7 Ongoing real-time monitoring may detect victims or perpetrators of investment fraud. In respect of victims, the monitoring was designed to identify whether a customer did make a particular transaction, rather than whether they ought to make a transaction. We saw few examples of specific consideration of investment fraud and how this could be detected by real-time or post-event transaction monitoring.

Post-event AML monitoring

6.8 Post-event AML monitoring did not appear effective in identifying perpetrators of investment fraud. Most of the cases identified by the banks appeared to originate from suspicions raised by customer-facing staff. However, it was interesting to note that some of these cases had previously been identified by transaction monitoring, and a suspicious activity report raised, but the incident was not categorised as investment fraud.

Real-time payment screening

6.9 Payment screening appeared to be the most effective means of identifying potential victims of investment fraud. Three of the banks visited used payment screening for this purpose. One of these three had prevented in excess of £1m in payments to potential boiler rooms over the previous three years.

6.10 One bank used the FSA list of potential investment fraudsters to screen for payments, but showed little success in identifying relevant payments.

6.11 One bank was in the process of implementing technology to monitor the pattern of external payments, rather than just the information contained in individual payments. This was a good example of how technology was developing in this area.

Conclusion

6.12 The banks visited demonstrated they had implemented a range of transaction monitoring technologies.

6.13 The design of these transaction monitoring solutions rarely explicitly considered the risk of investment fraud to a bank or its customers. Rules were defined generically on the assumption that they would detect a range of fraud types. While this may be the case, there was no clear documentation demonstrating banks had applied known fraud typologies to the configuration in place to ensure they would be detected. This is consistent with our observation in the risk assessment section of this report that the banks did not 'stress test' their risk and control frameworks against known fraud typologies.

6.14 Many of the automated measures used to address the risk of investment fraud directly used existing technology and did not require significant investment in systems. For example, one bank has been able to demonstrate notable success in preventing customers falling victim to investment fraud through adding potential investment fraud perpetrators to its existing payment screening technology.

6.15 It was disappointing that some of the banks visited dismissed the use of payment screening technology as impractical to prevent payments to investment fraudsters. Three of the banks visited had successfully implemented procedures in this area: their real-time payment screening had been able to detect and prevent some payments to investment fraudsters by banks' customers.

6.16 However, the success of payment screening appears heavily dependent on the quality of the information used to screen against. Basing the screening on out-of-date, incomplete or inappropriate information has led to an increased false detection rate at one bank, which can undermine the basis for the monitoring and lead to wasted resources.

Automated monitoring: examples of good and poor practice

Automated monitoring	
Examples of good practice	**Examples of poor practice**
• A bank undertakes real-time payment screening against a well-formulated watch list. The bank actively contacts customers if suspect payments are identified (see next section). • There is clear governance of transaction monitoring rules. The quality of alerts (rather than simply the volume of false positives) is actively considered. • Investment fraud subject matter experts are involved in the setting of transaction monitoring rules. • Transaction monitoring programmes reflect insights from risk assessments or vulnerable customer initiatives. • A bank has transaction monitoring rules designed to detect specific types of investment fraud e.g. boiler room fraud. • A bank reviews accounts in a timely fashion after risk triggers are tripped (such as the raising of a suspicious activity report). • High-risk accounts are screened against adverse media reports. • When alerts are raised, a bank checks against account-opening information to identify any inconsistencies with expectations.	• A bank fails to use information about known or suspected perpetrators of investment fraud in its financial crime prevention systems. • A bank does not consider investment fraud in the development of transaction monitoring rules. • The design of rules cannot be amended to reflect the changing nature of the risk being monitored.

7 Protecting victims

Introduction

7.1 **This chapter is primarily relevant to banks' efforts to protect victims.**

7.2 In this section of our review, we have considered how banks help to protect customers from investment fraud, and how they educate their customers. The ability of banks to protect their customers from investment fraud is greatly aided by customers being able to recognise fraud and report this to the appropriate authorities. There are already several sources of public information on investment fraud, including Action Fraud[6] and the FSA's website.

Guidance to customers

7.3 Not all the banks visited placed guidance on their websites to help customers who suspected they were falling victim to investment fraud. Where this advice was provided, the advice on whom to contact varied: some recommended contacting the bank itself; others recommended the FSA, the City of London Police or Consumer Direct.

Who to contact

We advise that banks should refer victims of investment fraud to Action Fraud on 0300 123 2040. Customers who have been approached by a suspected investment fraud may wish to use our online form[7] or contact our consumer helpline on 0845 606 1234. Customers seeking more information on investment fraud may wish to consult our 'Scams and swindles' page.[8]

7.4 The content of the banks' website communications with customers often simply replicated our guidance, even when the bank had invested in developing extensive internal awareness materials.

6 www.actionfraud.police.uk/ and www.fsa.gov.uk/
7 www.fsa.gov.uk/pages/doing/regulated/law/alerts/form.shtml
8 www.fsa.gov.uk/scams

7.5 A summary of the investment fraud advice observed on the websites of banks, whether they had mailed or planned to mail customers and a comparison against communication relating to other types of fraud (internet banking fraud used as an example) is contained in Table 6 below.

Table 6: Summary of customer communication initiatives relating to investment fraud

	Investment fraud on website	Proposed contact point for customers	Mailings to customers	Internet banking on website
Bank 1	No	N/A	No	Yes
Bank 2	Yes	FSA	Has taken place or is planned	Yes
Bank 3	No	N/A	No	Yes
Bank 4	No	N/A	Has taken place or is planned	Yes
Bank 5	Yes	Bank and FSA	Has taken place or is planned	Yes
Bank 6	Yes	FSA and City of London Police	No	Yes
Bank 7	Yes	Bank	No	Yes
Bank 8	Yes	Consumer Direct	No	Yes

7.6 While not all banks warned customers of the dangers of investment fraud, most offered guidance to help prevent customers from falling victim to fraud where the bank was potentially liable (internet banking fraud, for example).

7.7 One of the banks had contacted their customers using mailshots that warned of the dangers of investment fraud. Two banks planned to do this during 2012. One of the banks visited also planned to work with victims of investment fraud to help encourage others to report the issue. In addition, some of the banks visited worked with charities to help promote the issue.

7.8 Some banks participated in industry initiatives to help raise awareness of investment fraud.

Contacting customers

7.9 Some banks had set procedures for contacting customers if they suspected a payment was being made to an investment fraudster. At these firms, defined procedures and scripts were in place to help ensure that a consistent and clear message was relayed to customers.

7.10 Several banks had initiated a vulnerable customers initiative, and considered that this helped protect customers from investment fraud. However, few banks had considered

the types of customer that could be vulnerable to investment fraud, and the definition of a 'vulnerable customer' varied significantly between banks.

The vulnerable customers initiative run by one of the banks included in-branch preventative action such as raising alerts to the fraud team and providing support to victims through phone calls and meetings. In addition, incentive schemes had been used to reward branch staff for identifying potential victims of investment fraud and preventing payments being made to the perpetrators.

7.11 Some banks expressed a perceived conflict between their obligation to detect where customers were the victim of investment fraud and their legal obligations to the customer to process a payment on time. For example, several banks noted that there was a conflict between meeting the timing requirements of 'faster payments' and the risk that a payment could be made to a possible investment fraudster (see 2.11).

7.12 Some banks also noted that customers often insisted on payments being made even after having the potential risks of investment fraud explained to them in some detail. One of the banks visited had a process for calling customers a set number of times to explain the possible risk. Another bank went as far as to meet customers in person.

7.13 Some banks expressed a concern they could be considered to be providing investment advice through calling a customer to warn them a payment is to a prospective investment fraudster. Some banks managed this risk through the use of predefined call centre scripts and staff training (see 2.12).

Conclusion

7.14 Most banks' external communications relating to investment fraud was either thin or non-existent. We anticipated banks would use their experience of reacting to investment fraud to provide rich, relevant and practical examples of how it could affect customers, that could, in turn, inform compelling advisory material aimed at the public. However, this was not the case at most of the banks visited.

7.15 The 'signposting' for customers concerned about potential investment fraud is inconsistent between banks. There is currently no common single point of contact suggested by banks. This is a matter for all interested bodies to consider so that consumer awareness can be improved and intelligence-sharing can be enhanced.

7.16 Many banks contacted customers if they suspected a payment was being made to an investment fraudster; some met customers in person to warn of the dangers. While visiting potential victims goes beyond our regulatory expectations, some banks saw barriers to initiating any contact with customers.

7.17 Banks should consider the examples of good and poor practice below when taking steps to protect customers from investment fraud.

Protecting victims: examples of good and poor practice

Protecting victims	
Examples of good practice	**Examples of poor practice**
• A bank contacts customers if it suspects a payment is being made to an investment fraudster. • A bank places material on investment fraud on its website. • A bank adopts alternative customer awareness approaches, including mailing customers and branch awareness initiatives. • Work to detect and prevent investment fraud is integrated with a bank's vulnerable customers initiative.	• Communication with customers on fraud just covers types of fraud for which the bank may be financially liable, rather than fraud the customer might be exposed to. • A bank has no material on investment fraud on its website. • A bank fails to contact customers it suspects are making payments to investment fraudsters on grounds that this constitutes 'investment advice'.

8 Management reporting and escalation of suspicions

Introduction

8.1 **This chapter is relevant both to banks' efforts to detect customers who are complicit in investment fraud, and to the detection and protection of customers who are victims.**

8.2 There were separate management's reporting processes for victims and perpetrators of investment fraud at the banks visited.

8.3 We focused our review on:

- Staff and management understanding of their obligations in respect of investment fraud, particularly in relation to escalating suspicions that a customer of the bank is a perpetrator of investment fraud.
- The quality and detail included in the investigation report for a suspicion.
- The timeliness of the process for filing suspicious activity reports (SARs).

8.4 We had expected management reporting to show evidence of senior management responsibility and to both reflect and inform the risk management framework adopted for investment fraud.

Management reporting

8.5 None of the banks visited provided clear reporting to senior management on the incidence and level of investment fraud perpetrated either on or by their customers. This was in contrast to the reporting observed as being in place for other types of fraud, particularly fraud where the bank is financially liable.

8.6 Only one bank reported information to senior management about customers who were prevented from becoming the victim of investment fraud. However, the reporting was focused solely on boiler rooms.

8.7 Given this lack of management reporting, it is difficult to understand the basis on which the senior management of some banks had decided that investment fraud posed little threat to the bank's customers (see our sections on governance and risk assessment).

8.8 Few banks were able to access information easily on cases where their customers had fallen victim to investment fraud. There were rarely procedures in place to record this information.

Escalation of Suspicious Activity Reports

8.9 There were generally good processes in place for investigating suspicions raised within the banks visited, and for subsequently reporting these to Serious Organised Crime Agency. The investigators typically understood the principles of investment fraud, though at some banks this understanding was biased towards boiler rooms, with other typologies such as carbon credits and land banking poorly understood.

8.10 Some banks raised suspicious activity reports where they identified a victim of investment fraud. However, the majority did not, because they did not consider they held the proceeds of crime.

8.11 Where a bank identified a perpetrator of investment fraud, they would typically raise a suspicious activity report. But there was no systematic reporting of perpetrators of investment fraud at any of the banks visited. One bank had a specialist team to investigate potential perpetrators of fraud in further detail to allow the firm to make an informed decision on whether to exit the relationship with the customer.

8.12 At one bank, much of the work done to show evidence of progress in this area, including raising suspicious activity reports, was performed in the weeks prior to our visit. In particular, a number of the reports were made to the Serious Organised Crime Agency shortly before our visit even though some cases had been identified some time before and, in one case, in 2009.

Conclusions

8.13 We expected to see clear reporting to senior management of how the bank's customers were exposed to this risk. This was not the case at the banks visited.

8.14 Management reporting of fraud focused on events for which the bank would be financially liable. We saw little management reporting where the bank's customers had become victims of investment fraud. This was particularly evident when we requested information on cases of investment fraud the bank had identified. Few banks were able to provide this information without additional investigation across their systems, as these had not been configured to recognise this issue.

8.15 The suspicious activity report processes appeared to be formal and consistent, with strong detail documented in the reports. However, given that the purpose of the process is to report suspicion, it is of concern that many banks were unable to inform us of the number of possible investment fraud perpetrators they had identified among their customers.

Management reporting and escalation of suspicions: examples of good and poor practice

Management reporting and escalation of suspicions	
Examples of good practice	**Examples of poor practice**
• A specific team focuses on investigating the perpetrators of investment fraud. • A bank's fraud statistics include figures for losses known or suspected to have been incurred by customers.	• There is little reporting to senior management on the extent of investment fraud (whether victims or perpetrators) in a bank's customer base. • A bank is unable to access information on how many of the banks customers have become the victims of investment fraud.

9 Staff awareness

Introduction

9.1 **This chapter is relevant both to banks' efforts to detect customers who are complicit in investment fraud, and to the detection and protection of customers who are victims.**

9.2 Staff awareness is important in ensuring that systems and controls are properly designed, and implemented in a manner that effectively mitigates the risks posed by investment fraud. For example, some banks' ongoing monitoring of customers relied heavily on frontline business managers spotting where things were amiss.

9.3 Our assessment of awareness consisted of meetings with staff and management at each of the banks visited. In addition, we reviewed training documentation and internal awareness material (where this existed) to ascertain how the banks ensured their employees were aware of emerging investment fraud issues.

Awareness

9.4 Most of the employees interviewed were aware of investment fraud, although awareness focused mainly on boiler rooms, rather than other types of investment fraud, particularly at senior management level.

9.5 Some banks had subject matter experts on investment fraud who were able to demonstrate an excellent understanding of many of the types of investment fraud they had seen.

At one of the firms visited, we observed case notes indicating that a business relationship manager observed the characteristics of a potential Ponzi scheme. Despite describing these explicitly to the investigator in an email, the relationship manager's conclusion was that the activity was not necessarily suspicious. A suspicious activity report was nonetheless raised by the investigator.

9.6 One of the banks outsourced elements of transaction monitoring and customer contact. Customer-facing staff at the outsourcer were made aware of investment fraud. In addition, there was an emerging compliance monitoring programme designed and operated by the firm to ensure the outsourced service provider was meeting the bank's control requirements in this area.

Training

9.7 Some fraud training was carried out at all firms, and this included material on boiler room fraud. Fraud investigation teams at some of the banks visited received specific training designed to educate them on the risks of unauthorised business.

9.8 But the general quality of internal training provided to staff was variable. For example, one bank had used a variety of training materials, including newsletters and DVDs to explain the types of investment fraud to which the bank could be exposed. Others relied on including a general notice in their periodic financial crime training.

Conclusion

9.9 While most of the management and staff interviewed understood the principle of investment fraud, the depth of understanding of investment fraud typologies varied. While we recognise there are a broad range of topics on which a bank employee must receive training, we are concerned the material we saw did not always reflect the customer experience in relation to investment fraud. Much of the material is theoretical in nature and describes fraud typologies. While this is a good starting point, some of the rich customer experience described to us, particularly by banks with specialist teams able to investigate this type of issue, could be used to improve the effect of this training material.

Staff awareness: examples of good and poor practice

Staff awareness	
Examples of good practice	**Examples of poor practice**
• Making good use of internal experience of investment fraud to provide rich and engaging training material. • A wide range of materials covering investment fraud is available. • Incentives for branch staff to support vulnerable customers. • Training material is tailored to the experience of specific areas such as branch and relationship management teams.	• Training material only covers boiler rooms. • A bank's training material is out-of-date.

10 Use of industry intelligence

Introduction

10.1 **This chapter is relevant both to banks' efforts to detect customers who are complicit in investment fraud, and to the detection and protection of customers who are victims.**

10.2 One of the challenges in implementing an effective regime to prevent and detect investment fraud is the management and distribution of current, relevant and detailed industry intelligence.

Observations

10.3 Timely and detailed intelligence on the typology of investment fraud and the firms perpetrating this were cited by most banks as being critical to implementing effective investment fraud prevention procedures.

10.4 There are a number of sources available for building up a watch list for investment fraud including:

- Intelligence from the FSA or City of London Police about unauthorised businesses or the names of suspect shares.
- Intelligence from other banks e.g. from the banks' boiler room forum.
- Lists published on the FSA website of UK and overseas unauthorised businesses.
- Lists published by other organisations e.g. the International Organisation of Securities Commissions publishes an 'Investor Alert' list on its website covering a number of different jurisdictions.

10.5 Many of the banks visited regularly send representatives to a forum on boiler rooms and other investment frauds. This forum discusses emerging boiler room and investment fraud typologies, and shares intelligence on current investment fraudsters the banks have identified However, there seemed to be some uncertainty among banks about their own obligations and those of the regulator and other relevant bodies (such as Action Fraud or the Serious Organised Crime Agency).

10.6 While several banks are identifying potential perpetrators of investment fraud, there appears to be reluctance on behalf of banks to share intelligence because of concerns over legal liability.

10.7 We have seen little evidence of banks using empirical evidence of investment fraud from their own portfolios. In particular, where firms had international operations, we saw little evidence of collaboration between the UK and overseas parts of the group on investment fraud.

One firm produced its own 'watch list' of potential investment fraudsters using intelligence gathered from the Serious Organised Crime Agency, the City of London Police and other police forces, the FSA, the banks' boiler room forum and internal sources. Another had management resource dedicated to maintaining an internal 'watch list' from the boiler room forum and informal industry connections.

Conclusion

10.8 We saw several good examples of firms maintaining intelligence of investment fraudsters. However, these measures were not consistent across the industry. Not all of the banks visited attended the industry forum on boiler rooms, and there appeared to be a reluctance to share experiences and intelligence, because of concerns over legal liability.

10.9 We believe it desirable that the transaction monitoring rules banks have found effective in detecting investment fraud are shared with other firms on a confidential basis. Clear guidelines for submitting intelligence could be established to help address perceived liability issues.

Use of industry intelligence: examples of good and poor practice

Use of industry intelligence	
Examples of good practice	**Examples of poor practice**
• A bank participates in cross-industry forums on fraud and boiler rooms and makes active use of intelligence gained from these initiatives in, for example, its transaction monitoring and screening efforts. • A bank takes measures to identify new fraud typologies. It joins up internal intelligence, external intelligence, its own risk assessment and measures to address this risk.	• A bank fails to act on information shared at industry forums or intelligence received from other authoritative sources such as the FSA or City of London Police.

11 Consolidated examples of good and poor practice

11.1 This section consolidates examples of good and poor practice identified by this thematic review. These examples form the guidance material we are consulting on as part of this review. The next chapter states how this consultation will work. We welcome any comments you may have.

11.2 Following consultation, we anticipate our final guidance on banks' handling of investment fraud will form a new Chapter 14 in Part 2 of *Financial crime: a guide for firms*.[9] Consequently, we have set the material out in a format consistent with the format used in that publication. Once published it will be accompanied with brief introductory text setting out the context of this thematic review.

11.3 *Financial crime: a guide for firms* sets out our expectations of firms' financial crime systems and controls and provides examples of the steps firms can take to reduce the risk of being used to further financial crime. We are committed to keeping the guide up to date. And we are required to consult on changes to 'guidance on rules' in the guide, such as relevant examples of good and poor practice from financial crime thematic reviews, which have not already been subject to consultation.

11.4 Readers may find it helpful to consider these examples of good and poor practice in conjunction with the 'About the Guide' section of *Financial crime: a guide for firms*. Among other things, this says 'Guidance in the Guide should be applied in a risk-based, proportionate way. This includes taking into account the size, nature and complexity of a firm when deciding whether a certain example of good or poor practice is appropriate to its business'.

9 http://fsahandbook.info/FSA/html/handbook/FC/link/PDF

Governance	
Examples of good practice	**Examples of poor practice**
• A bank can demonstrate senior management ownership and understanding of fraud affecting customers, including investment fraud. • There is a clear organisational structure for addressing the risk to customers and the bank arising from fraud, including investment fraud. There is evidence of appropriate information moving across this governance structure that demonstrates its effectiveness in use. • A bank has recognised subject matter experts on investment fraud supporting or leading the investigation process. • The monetary value of sums saved for customers are used as a performance indicator. • When assessing the case for measures to prevent financial crime, a bank considers benefits to customers, as well as the financial impact on the bank.	• A bank lacks a clear structure for the governance of investment fraud or for escalating issues relating to investment fraud. Respective responsibilities are not clear. • A bank lacks a clear rationale for allocating resources to protecting customers from investment fraud. • A bank lacks documented policies and procedures relating to investment fraud. • There a lack of communication between a bank's AML and fraud teams on investment fraud.

Risk assessment	
Examples of good practice	**Examples of poor practice**
• A bank has assessed the risk to itself and its customers of fraud including investment fraud and other frauds where customers and third parties suffer losses rather than the bank. Resource allocation and mitigation measures are informed by this assessment. • A bank performs 'horizon scanning' work to identify changes in the fraud types relevant to the bank and its customers.	• A bank has performed no risk assessment that considers the risk to customers from investment fraud. • A bank's regulatory compliance, risk management and internal audit functions' assurance activities do not effectively challenge the risk assessment framework.

Detecting perpetrators	
Examples of good practice	**Examples of poor practice**
• A bank's procedures for opening commercial accounts include assessing the risk of the customer, based on the proposed business type, location and structure. • Account opening information is used to categorise a customer relationship according to its risk. The bank then applies different levels of transaction monitoring based on this assessment. • A bank screens new customers to prevent the take-on of possible investment fraud perpetrators.	• A bank only performs the customer risk assessment at account set up and does not update this through the course of the relationship. • A bank does not use account set up information (such as anticipated turnover) in transaction monitoring. • A bank allocates excessive numbers of commercial accounts to a staff member to monitor, rendering the ongoing monitoring ineffective. • A bank allocates responsibility for the ongoing monitoring of the customer to customer-facing staff with many other conflicting responsibilities.

Automated monitoring	
Examples of good practice	**Examples of poor practice**
• A bank undertakes real-time payment screening against a well-formulated watch list. The bank actively contacts customers if suspect payments are identified. • There is clear governance of transaction monitoring rules. The quality of alerts (rather than simply the volume of false positives) is actively considered. • Investment fraud subject matter experts are involved in the setting of transaction monitoring rules. • Transaction monitoring programmes reflect insights from risk assessments or vulnerable customer initiatives. • A bank has transaction monitoring rules designed to detect specific types of investment fraud e.g. boiler room fraud. • A bank reviews accounts after risk triggers are tripped (such as the raising of a suspicious activity report) in a timely fashion • High-risk accounts are screened against adverse media. • When alerts are raised, a bank checks against account-opening information to identify any inconsistencies with expectations.	• A bank fails to use information about known or suspected perpetrators of investment fraud in its financial crime prevention systems. • A bank does not consider investment fraud in the development of transaction monitoring rules. • The design of rules cannot be amended to reflect the changing nature of the risk being monitored.

Protecting victims	
Examples of good practice	**Examples of poor practice**
• A bank contacts customers if it suspects a payment is being made to an investment fraudster. • A bank places material on investment fraud on its website. • A bank adopts alternative customer awareness approaches, including mailing customers and branch awareness initiatives. • Work to detect and prevent investment fraud is integrated with a bank's vulnerable customers initiative.	• Communication with customers on fraud just covers types of fraud for which the bank may be financially liable, rather than fraud the customer might be exposed to. • A bank has no material on investment fraud on its website. • A bank fails to contact customers it suspects are making payments to investment fraudsters on grounds that this constitutes 'investment advice'.

Management reporting and escalation of suspicions	
Examples of good practice	**Examples of poor practice**
• A specific team focuses on investigating the perpetrators of investment fraud. • A bank's fraud statistics include figures for losses known or suspected to have been incurred by customers.	• There is little reporting to senior management on the extent of investment fraud (whether victims or perpetrators) in a bank's customer base. • A bank is unable to access information on how many of the banks customers have become the victims of investment fraud.

Staff awareness	
Examples of good practice	**Examples of poor practice**
• Making good use of internal experience of investment fraud to provide rich and engaging training material. • A wide range of materials are available that cover investment fraud. • Incentives for branch staff to support vulnerable customers. • Training material is tailored to the experience of specific areas such as branch and relationship management teams.	• Training material only covers boiler rooms. • A bank's training material is out-of-date.

Use of industry intelligence	
Examples of good practice	**Examples of poor practice**
• A bank participates in cross-industry forums on fraud and boiler rooms and makes active use of intelligence gained from these initiatives in, for example, its transaction monitoring and screening efforts. • A bank takes measures to identify new fraud typologies. It joins up internal intelligence, external intelligence, its own risk assessment and measures to address this risk.	• A bank fails to act on information shared at industry forums or intelligence received from other authoritative sources such as the FSA or City of London Police.

12 Consultation

12.1 The previous chapter consolidates examples of good and poor practice identified by this review, which forms the guidance material on which we are consulting. Please see the Guidance Consultation[10] published simultaneously with this document for more details.

12.2 Please respond by 23 August 2012.

12.3 You can send your response by email to: jody.ketteringham@fsa.gov.uk

12.4 Alternatively, responses can be sent by post or telephone:

Jody Ketteringham
Financial Crime and Intelligence Department
Financial Services Authority
The North Colonnade
London E14 5HS
Telephone: 020 7066 3490

10 www.fsa.gov.uk/library/policy/guidance_consultations/2012/gc1207

The Financial Services Authority
25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000 Fax: +44 (0)20 7066 1099
Website: www.fsa.gov.uk