Guidance consultation

Examples of good and poor practice in 'Banks' defences against investment fraud'

June 2012

1 Consultation

1.1 Our thematic review, Banks' defences against investment fraud, explains the findings of our visits to seven retail banks and one building society to assess the systems and controls in place to contain the risks posed by investment fraudsters. In that document, which is published simultaneously with this guidance consultation, we set out examples of good and poor practice we identified. These examples are consolidated in Section 11 of *Banks' defences against investment fraud*, and are reprinted below for your convenience. These examples of good and poor practice, as well new text for the fraud chapter of *Financial crime: a guide for firms* drawn from those examples, forms the guidance material on which we are consulting. We have not previously consulted on any of this material; it is all subject to consultation now.

1.2 This document discusses how this consultation will work, as well as setting out our analysis of the costs and benefits of this guidance material. We welcome any comments you may have.

Consultation process

1.3 We invite your views on:

(a) the examples of good and poor practice we propose to include in Chapter 14 in Part 2 of Financial crime: a guide for firms (see pages 5 to 7);

(b) our proposed new text for the fraud chapter of Part 1 of Financial crime: a guide for firms (see page 8); and

(c) our cost benefit analysis of this proposed guidance (see pages 2 to 4).

1.4 Please respond by 23 August 2012.

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

2 Cost benefit analysis

2.1 This section sets out an estimate of the costs and an analysis of the benefits of the guidance in *Banks' defences against investment fraud*. The estimates below are based on information about costs and about the staff time allocated to taking measures to meet our expectations we gained from previous consultations. We welcome comments on this analysis.

2.2 It is necessary for us to perform cost benefit analysis on proposed guidance when we consider a) it is likely to change behaviours of firms in a way that is not already accepted in the market and/or b) where the guidance is not reasonably predictable from an existing FSA rule. We believe both conditions to be true of the examples of good and poor practice set out in *Banks' defences against investment fraud*.

2.3 It is also necessary for us to consider guidance if we consider our proposed guidance may materially affect market structures, although we do not believe this to be the case for this guidance, which in our judgement will not, for example, affect the types or number of businesses that offer retail banking services in the United Kingdom.

Costs

2.4 **Costs to the public**: we do not anticipate the good and poor practice set out in this review has cost implications for the public.

2.5 **Costs to firms:** firms will incur costs as a consequence of considering our examples of good and poor practice. We have set out some estimates below:

(a) **Governance:** firms will wish to consider if organisational arrangements (including the allocation of responsibilities and designation of subject matter experts) need to be revised in light of the proposed guidance. Some banks may consider that policies and procedures may need to be updated. We estimate this review will be done by fifty firms that have a) retail depositors who may be affected by investment fraud or b) commercial or retail customers who may be complicit in such fraud, and would occupy one full-time equivalent (FTE) for thirty working days at each firm. Assuming a cost (including all overheads) for one FTE of £290 a day[1], this amounts to a one-off cost across the industry of £435,000.

[1] This figure is drawn from the cost benefit analysis in Consultation Paper 11/12 from last year; see: http://www.fsa.gov.uk/pubs/cp/cp11_12.pdf

(b) **Risk assessment:** our review found firms had not assessed the risks to themselves and their customers of fraud (including investment fraud and frauds where customers and third parties suffer losses rather than the firm). We anticipate preparing these risk assessments will be a cost for firms, and that this cost will be of a similar magnitude as the cost of considering the adequacy of governance arrangements: a one-off cost across the industry of £435,000.

(c) **Detecting perpetrators:** having performed their risk assessment, firms will consider whether the resources allocated to detecting customers who may be complicit in fraud is appropriate. Some may conclude that, given the risks, their existing resource-allocation is adequate. Others may decide they require more resources: we anticipate a half of firms (so twenty-five of our fifty deposit takers) will employ the equivalent of one extra FTE as a consequence of this decision. If one FTE costs £290 a day, this suggests an annual cost of £1.69m across the industry.

(d) **Automated monitoring:** We anticipate firms may use our examples of good and poor practice to consider whether their existing automated monitoring systems could be used more effectively, by, for example, refining transaction monitoring rules. We estimate twenty firms will use resources the equivalent one FTE for twenty working days to consider what measures are appropriate and then implement them. This would be a one-off cost to industry of £116,000. We do not anticipate firms will make substantive systems changes, or procure new systems as a consequence of considering our guidance.

(e) **Protecting victims:** after considering our examples of good and poor practice, and performing the risk assessment discussed above, firms may wish to revise how they communicate the dangers of fraud to their customers, and how they engage with individual victims. We understand firms renew the material on their website and other information aimed at customer on a periodic basis to ensure it remains current, and we anticipate this would form one aspect of that ongoing review: as a consequence, we do not anticipate this will lead to significant incremental costs. Some firms may conclude they need to engage with prospective victims more directly. If one third of our fifty deposit-takers decide to employ the equivalent of one third of an FTE's time for this task, it would cost £383,000 annually across the industry.

(f) **Management reporting and escalation of suspicions:** firms will wish to consider whether their internal reporting arrangements are adequate, and whether the basis on which internal fraud data are gathered needs to be revised. If this initial review occupies the equivalent of one FTE at fifty deposit-taking firms for ten working days this would be a one-off cost to industry of £145,000. If it is determined that extra fraud data needs to be gathered, and doing so uses the equivalent of one FTE for ten days a year, this would be an additional annual ongoing cost of £145,000 to the industry. Firms may wish to consider whether their current investigatory arrangements aimed at detecting customers who may be complicit in fraud are suitable, although these costs arguably would fall under those set out in heading (c).

(g) **Staff awareness:** we anticipate that firms will consider whether our examples of good and poor practice contain lessons for their own internal training arrangements. We understand firms update training materials on a regular cycle in any event, and have ongoing arrangements for periodically reviewing whether staff's training and competence remain adequate, so we anticipate firms will not experience significant extra costs beyond those that would otherwise be incurred.

(h) **Use of industry intelligence**: we anticipate some firms will allocate more time to engagement in cross-industry information-sharing exercises as a consequence of considering our guidance, and on work to ensure intelligence gathered in this way was used effectively. If a third of our fifty deposit-takers (so seventeen firms) opted to use the equivalent of one FTE for one month a year in such work this would cost the industry £98,600 a year.

2.6 We estimate the industry will face a one-off initial cost of £1.1m and an ongoing annual cost of £2.3m, with the largest component being the ongoing allocation of increased resources to the detection of customers who are complicit in investment fraud.

2.7 **Costs to the FSA**: we do not anticipate the good and poor practice set out in this review will have cost implications for us.

Benefits

2.8 **Benefits to the public**. We estimate UK consumers lose over £500 million every year to investment fraudsters. If firms take our examples of good and poor practice into account when considering whether their systems and controls are appropriate, we anticipate this will lead to fewer members of the public falling victim to investment fraud. We also anticipate it will lead to more customers who are complicit in investment fraud being detected. Preventing this fraud stops the illegitimate transfer of funds from UK consumers to those engaging in investment fraud. By do so society avoids the costs of investigating and prosecuting cases of investment fraud.

2.9 **Benefits to firms:** We believe consumers' concerns about fraud undermine their confidence in engaging with the financial services industry more generally: firms' efforts to tackle fraud against the customer may help lessen this fear. While consumers' losses to investment fraudsters may be small relative to the size of deposit-takers' retail funding, banks and building societies may nonetheless have self-interested reasons to wish to retain those deposits.

3 Consolidated examples of good and poor practice

3.1 This section consolidates examples of good and poor practice identified by *Banks' defences against investment fraud*. These examples form the guidance material we are consulting on as part of this review. We welcome any comments you may have.

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

[2] http://fsahandbook.info/FSA/html/handbook/FC/link/PDF

3.3 *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 have 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.

3.4 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.* Amongst 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".

Examples of good practice	Examples of poor practice
Governance	
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	
A bank has assessed the risks to itself and its customers of all types of fraud, including investment fraud, and including 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	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.

Examples of good practice	Examples of poor practice
customers.	
Detecting perpetrators	
A bank's procedures for opening commercial accounts include an assessment of 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 updating 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	
A bank undertakes real-time payment screening against a well-formulated watch list. The bank actively contacts customers in the event 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 after risk triggers are tripped (such as the raising of a SAR) 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	
A bank contacts customers in the event they suspect a	Communication with customers on fraud just covers types of fraud for which the bank may be financially

Examples of good practice	Examples of poor practice
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.	liable, rather than fraud the customer might be exposed to. A bank has no material on investment fraud on its website. Failing to contact customers they suspect are making payments to investment fraudsters on grounds that this constitutes "investment advice".
Management reporting and escalation of suspicions	
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 bank's customers have become the victims of investment fraud.
Staff awareness	
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	
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.

3.5 In addition to the examples of good and poor practice above in a new Chapter 14 in Part 2 of *Financial crime: a guide for firms,* we propose to make changes to the fraud chapter in Part 1; we intend to remove the existing text in Box 4.5 that discusses investment fraud and replace it with the material set

out below. The amendments draw upon the examples of good and poor practice above, but also set out three self-assessment questions. We will also update cross-references elsewhere in that chapter. We would welcome your comments on these proposals.

Box 4.5: Investment fraud

UK consumers are targeted by share-sale frauds and other scams including land-banking frauds, unauthorised collective investment schemes and Ponzi schemes. Customers of UK deposit-takers may fall victim to these frauds, or be complicit in them. We expect these risks to be considered as part of deposit-takers' risk assessments, and for this to inform management's decisions about the allocation of resources to a) the detection of fraudsters among the customer base and b) the protection of potential victims.

Self-assessment questions:

- Have the risks of investment fraud (and other frauds where customers and third parties suffer losses) been considered by the firm?
- Are resources allocated to mitigating these risks as the result of purposive decisions by management?
- Are the firm's anti-money laundering controls able to identify customers who are complicit in investment fraud?

Good practice[3]	**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 contacts customers if it suspects a payment is being made to an investment fraudster. A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules.	A bank has performed no risk assessment that considers the risk to customers from investment fraud. A bank fails to use information about known or suspected perpetrators of investment fraud in its financial crime prevention systems. Ongoing monitoring of commercial accounts is allocated to customer-facing staff incentivised to bring in or retain business. A bank allocates excessive numbers of commercial accounts to a staff member to monitor.

[3] These examples of good and poor practice are drawn from Chapter 14 of Part 2 of this guide, which provides further examples drawn from our thematic review *Banks' defences against investment fraud.*