Summary of feedback received

November 2012

Consultation title	*Banks' defences against investment fraud* Proposed guidance and amendments to '*Financial crime: a guide for firms'*
Date of consultation	June 2012
Summary of feedback received	We received four responses to our consultation. Their comments have been summarised below. We are grateful for the constructive engagement we received. **Comments on how we issue guidance** Two respondents believed our guidance would not be applicable to all deposit-takers in all cases, with one noting we visited a relatively small sample of firms that was not necessarily representative of the entire industry. A ''one-size-fits-all'' approach would not be appropriate. One respondent highlighted the dangers of statements of good practice being used as an inflexible ''ticklist'', while another voiced concern that collecting together all findings from previous thematic reviews in Part 2 of *'Financial crime: a guide for firms*' has led to that section becoming unwieldy: they argued for this to be restructured. *We believe the ''*About the Guide''*' statement on page 6 of '*Financial crime: a guide for firms*' makes it clear that guidance should be applied in a manner that reflects the size, nature and complexity of a firm. Part 2 contains all past guidance in one place – this is intended to ensure the Guide is a comprehensive ' 'one-stop shop". We indicate where past text is no longer current.* **Comments on how we conducted the review** One respondent felt our review placed too much emphasis on deposit-takers' efforts to detect customers who are complicit in perpetrating investment fraud, at the expense of considering how they look at customers as victims. Another suggested greater engagement by the FSA with stakeholders during the planning of this review would have allowed a sharing of experience and expertise that could have informed our findings. That respondent also disputed the accuracy of our finding that firms were unable to express a clear rationale for the basis on which they allocated resources to managing investment fraud risks.

We note these comments.

Comments on cooperation between public and private bodies

Three respondents emphasised the importance of cooperation and coordination between public bodies and the private sector to tackle investment fraud, arguing there was room for improvement; all respondents said information provided by the FSA could be enhanced. One respondent argued that firms would welcome more information from the FSA about the nature and extent of investment fraud to help inform their risk assessments and efforts to detect and prevent investment fraud, and data from government could assist ‘‘horizon scanning’’ by firms seeking to identify new risks. Another suggested FSA ‘‘watchlists’’ would be more usable if they were electronic and had regularly scheduled updates.

We note these comments.

Comments on other types of fraud

One respondent argued the guidance should be recast so it explicitly applies to firms’ efforts to detect and prevent other types of fraud and criminal conduct affecting customers. Another warned of danger of a ‘‘silo’’ approach to investment fraud, which is just one of the many types of fraud to which customer can fall victim.

Our report considered investment fraud as an example of a type of fraud to which banks’ customers can either fall victim, or be complicit. It said, ‘*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.*’

Comments on the clarity of our use of language

One respondent cautioned that the terms ‘ ‘investment fraud’’ and ‘‘unauthorised businesses’’ are not in common currency amongst the public or business. They put forward ‘‘mass-marketing fraud’’ and ‘‘investment scam’’ as more commonly used phrases.

We agree there is scope for confusion. We will include new glossary entries in the guide.

Comments on the need to balance other regulatory commitments

One respondent argued the review does not give sufficient weight to the complexity deposit-takers face balancing the requirements of the payment services regulations, data protection legislation, and the objective to prevent financial crime.

We acknowledged these issues in Section 2 of our report.

Comments about customers who are wrongly suspected of fraud

One respondent argued the FSA should do more to protect

consumers who are wrongly suspected of fraud by their bank, and disadvantaged as a consequence. This respondent suggested detailed steps the FSA could take in this regard.

We note these comments, which fall outside the scope of this piece of work.

Comments on our guidance on ‘‘Governance’’

Our guidance gave this as an example of good practice: ‘There is a clear organisation structure for addressing the risk to customers and the bank arising from fraud, including investment fraud.’

Two respondents argued it should be made clearer that the organisation structure should reflect the size and complexity of the business.

*We believe the ‘‘*About the Guide’*’ statement on page 6 of ‘*Financial crime: a guide for firms*’ makes it clear that guidance should be applied in a manner that reflects the size, nature and complexity of a firm.*

‘The monetary value of sums saved for customers are used as a performance indicator’.

Three respondents expressed doubt whether ‘‘sums saved’’ is an appropriate measure. One suggested ‘‘losses prevented’’ might be better, but warned this figure might not offer much insight. Another wanted guidance on what figures this might include, suggesting it was difficult to estimate what future payments might have been prevented, and that some customers insisted on payments going through, despite their banks’ efforts.

We have made this statement more general in nature: ‘A bank seeks to measure its performance in preventing detriment to customers’.

Comments on our guidance on ‘‘Risk assessment’’

Our guidance gave this as an example of good 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.’

One respondent believed this text is open to misinterpretation, and could be read to suggest losses suffered by the bank are less important. Alternative text was suggested.

We have drawn on the alternative text suggested to rephrase this example: ‘A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management framework. The risk assessment does not only cover situations where the bank could suffer losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures

are also informed by this assessment.'

Comments on our guidance on ''Detecting perpetrators''

Our guidance gave this as an example of good practice: 'A bank screens new customers to prevent the take-on of possible investment fraud perpetrators.'

A respondent suggested such screening should seek to prevent any type of fraudster.

We note this comment but will not alter this example of good practice.

Comments on our guidance on ''Automated monitoring''

Our guidance gave this as an example of good practice: 'A bank undertakes real-time payment screening against a well-formulated watch list.'

A respondent cautioned that preparing watch lists is hampered by a paucity of information.

We have changed ' 'well-formulated watch list" to ' 'data about investment fraud from credible sources''.

Our guidance gave this as an example of good practice: 'The bank actively contacts customers if suspect payments are identified'.

A respondent queried if this duplicates guidance in the following section.

We agree, and will remove this text from this location.

Our guidance gave this as an example of good practice: 'There is clear governance of transaction monitoring rules. The quality of alerts (rather than simply the volume of false positives) is actively considered.'

One respondent sought clarity about the meaning of 'transaction monitoring rules'. *We have changed 'transaction monitoring rules' to 'real-time payment screening', and have sought to clarify this elsewhere in this section.*

Our guidance gave this as an example of good practice: 'High-risk accounts are screened against adverse media.'

Several respondents sought clarification of what we mean by 'adverse media.' A respondent suggested 'reasonably selected information sources'. Another suggested the press and internet were a more realistic source of information at account take-on, rather than part of automated monitoring.

We have removed this text, believing it is covered by the reworded first example in this section.

Comments on our guidance on 'Protecting victims'

Our guidance gave this as an example of good practice: 'A bank contacts customers if it suspects a payment is being made to an investment fraudster.'

One respondent was concerned this approach could lead to a bank breaching its mandate with customers by failing to execute their instructions; this could lead a bank to be exposed to legal action by customers or referrals to the Financial Ombudsman Service. It also suggested an increase in use of the consent regime under the Proceeds of Crime Act could result, resulting in costs for firms and the authorities.

We will include this as an example of good practice because we saw examples of banks that do routinely contact customers, and presumably feel able to balance the legal risks that this may entail. It is not clear to us that Suspicious Activity Reports (SARs) seeking consent would be appropriate in such cases, because the funds the customer is seeking to transfer are arguably not yet the proceeds of crime, and there would be no basis on which the authorities could seek to have the funds restrained. We would consequently be surprised if there was an increase in consent SARs as a result of this guidance. We agree though that other types of engagement with law enforcement may be appropriate in these situations.

Our guidance gave this as an example of good practice: 'A bank adopts alternative customer awareness approaches, including mailing customers and branch awareness initiatives. '

Two respondents suggested that direct mailings are, in their experience, not the most effective method of communicating the dangers of investment fraud. One said it had tried a range of other methods including the use of social media, leaflets in branches and material on the internet.

We gave mailshots as an example of a communication method that we are aware has been used, although we are happy to clarify this was not an endorsement of that approach in preference to others. We have changed 'including' to 'such as'.

Comments on our guidance on 'Management reporting and escalation of suspicions'

Our guidance gave this as an example of good practice: 'A specific team focuses on investigating the perpetrators of investment fraud.'

A respondent argued this is not always appropriate in all circumstances. Another warned this could lead to investment fraud being considered in isolation and a 'silo' mentality.

We will keep this text, although agree a dedicated team will not be appropriate in all cases.

Our guidance gave this as an example of good practice: 'A bank's

fraud statistics include figures for losses known or suspected to have been incurred by customers.'

A respondent suggested 'suspected fraud' was of little use in management information.

We saw examples of banks considering how to gather such data, so will include this as an example of good practice, although we accept that all statistical indicators have their strengths and weaknesses.

Comments on our guidance on 'Staff awareness'

Our guidance gave this as an example of good practice: 'Incentives for branch staff to support vulnerable customers.'

Three respondents objected to 'incentives' in such cases, suggesting these can lead to unspecified adverse incentives and vulnerable customers being treated differently and hence unfairly.

Our use of the term 'incentives' was perhaps unhelpful. Drawing from an illustrative example given by a respondent, we changed the text to 'Awards are given on occasion to frontline staff when a noteworthy fraud is identified'.

Comments on our guidance on 'Use of industry intelligence'

Our guidance gave this as an example of good 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.'

One respondent queried if we anticipated all banks should take part in these forums.

There are many banks, for example those without sizeable retail customer bases, for whom attendance at these forums will not be appropriate. But we believe it is good practice for a bank whose customers may be exposed to this risk to seek to engage with such initiatives.

Our guidance gave this as an example of poor practice: '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.'

A respondent suggested actionable intelligence is not always available from such sources.

We have clarified we are referring to 'actionable, credible intelligence'. It now reads 'A bank fails to act on actionable, credible intelligence shared at industry forums or received from other authoritative sources such as the FSA or City of London Police.'

Comments on our cost benefit analysis

We estimate the industry will face a one-off initial cost of £1.1m and an ongoing annual cost of £2.3m. Three respondents gave views on our cost benefit analysis. One said our methodology was unclear and consequently found it difficult to determine whether our estimate is accurate, although suggested costs are likely to be significantly greater than estimated. Respondents suggested we overlooked several significant sources of cost:

- The ongoing cost of customer contact, case investigation and reporting to the authorities that would be necessary if a firm introduces new initiatives to combat investment fraud.
- The cost of claims to the Financial Ombudsman Service if there is an increased number of customer complaints about banks delaying payments.
- The cost of an increase in the number of consent SARs if greater numbers of suspicious payments are identified.
- The ongoing cost of analysing and refining automated monitoring rules.
- The ongoing cost of periodic risk assessment.
- The one-off cost of preparing and delivering training on investment fraud: the respondent suggested this would occupy one full-time equivalent member of staff for 30 working days at each firm.

We note these comments.

You can access the full text of the guidance consulted on here