Chapter 14

Banks' defences against investment fraud (2012)

14.3 Consolidated examples of good and poor practice

14.3.1 In addition to the examples of good and poor practice below, Section 6 of the report also included case studies illustrating relationships into which banks had entered which caused the *FSA* particular concern. The case studies can be accessed via the link in the paragraph above.

14.3.2 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.	• 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.
• 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 lacks a clear rationale for allocating resources to protecting customers from investment fraud.
• A bank has recognised subject matter experts on investment fraud supporting or leading the investigation process.	• A bank lacks documented policies and procedures relating to investment fraud.
• A bank seeks to measure its performance in preventing detriment to customers.	• There is a lack of communication between a bank's AML and fraud teams on investment fraud.
• 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.	

14.3.3 Risk assessment

Examples of good practice	Examples of poor practice
• 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.	• A bank has performed no risk assessment that considers the risk to customers from investment fraud.
• A bank performs 'horizon scanning' work to identify changes in the fraud types relevant to the bank and its customers.	• A bank's regulatory compliance, risk management and internal audit functions' assurance activities do not effectively challenge the risk assessment framework.

14.3.4 Detecting perpetrators

Examples of good practice	Examples of poor practice
• 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.	• A bank only performs the customer risk assessment at account set up and does not update this through the course of the relationship.
• 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 does not use account set up information (such as anticipated turnover) in transaction monitoring.
• A bank screens new customers to prevent the take-on of possible investment fraud perpetrators.	• 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.

14.3.5 Automated monitoring

Examples of good practice	Examples of poor practice
• A bank undertakes real-time payment screening against data about investment fraud from credible sources.	• A bank fails to use information about known or suspected perpetrators of investment fraud in its financial crime prevention systems.
• There is clear governance of real time payment screening. The quality of alerts (rather than simply the volume of false positives) is actively considered.	• A bank does not consider investment fraud in the development of monitoring rules.
• Investment fraud subject matter experts are involved in the setting of monitoring rules.	• The design of rules cannot be amended to reflect the changing nature of the risk being monitored.
• Automated monitoring programmes reflect insights from risk assessments or vulnerable customer initiatives.	
• A bank has 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.	
• When alerts are raised, a bank checks against account-opening information to identify any inconsistencies with expectations.	

14.3.6 Protecting victims

Examples of good practice	Examples of poor practice
• A bank contacts customers in the event they suspect a payment is being made to an investment fraudster.	• 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 places material on investment fraud on its website.	• A bank has no material on investment fraud on its website.

• A bank adopts alternative customer awareness approaches, such as mailing customers and branch awareness initiatives.	• Failing to contact customers they suspect are making payments to investment fraudsters on grounds that this constitutes 'investment advice'.
• Work to detect and prevent investment fraud is integrated with a bank's vulnerable customers initiative.	

14.3.7 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.	• 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's fraud statistics include figures for losses known or suspected to have been incurred by customers.	• A bank is unable to access information on how many of the bank's customers have become the victims of investment fraud.

14.3.8 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.	• Training material only covers boiler rooms.
• A wide-range of materials are available that cover investment fraud.	• A bank's training material is out-of-date.
• Awards are given on occasion to frontline staff when a noteworthy fraud is identified.	
• Training material is tailored to the experience of specific areas such as branch and relationship management teams.	

14.3.9 Use of industry intelligence

Examples of good practice	Examples of poor practice
• A bank participates in cross-industry forums on fraud and boiler rooms	• A bank fails to act on actionable, credible intelligence shared at industry

	and makes active use of intelligence gained from these initiatives in, for example, its transaction monitoring and screening efforts.	forums or received from other authoritative sources such as the *FCA* or City of London Police.
•	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.	