Chapter 4

Fraud

4

4.2 Themes

Preventing losses from fraud

4.2.1 G All firms will wish to protect themselves and their customers from fraud. Management oversight, risk assessment and fraud data will aid this, as will tailored controls on the ground. We expect a firm to consider the full implications of the breadth of fraud risks it faces, which may have wider effects on its reputation, its customers and the markets in which it operates.

The general guidance in FCG 2 also applies in relation to fraud.

Self-assessment questions:

- What **information** do senior management receive about fraud trends? Are fraud losses accounted for clearly and separately to other losses?
- Does the firm have a clear picture of what parts of the business are **targeted by fraudsters**? Which **products, services and distribution channels** are vulnerable?
- How does the firm respond when reported fraud **increases**?
- Does the firm's investment in **anti-fraud systems** reflect fraud trends?

Examples of good practice	Examples of poor practice
• The firm takes a view on what areas of the firm are most **vulnerable** to fraudsters, and tailors defences accordingly.	• Senior management appear **unaware** of fraud incidents and trends. No management information is produced.
• Controls adapt to **new fraud threats**.	• **Fraud losses are buried** in bad debts or other losses.
• The firm engages with relevant **cross-industry efforts** to combat fraud (e.g. data-sharing initiatives like CIFAS and the Insurance Fraud Bureau, collaboration to strengthen payment systems, etc.) in relation to both internal and external fraud.	• There is no clear and consistent **definition** of fraud across the business, so reporting is haphazard.
• **Fraud response plans and investigation procedures** set out how the firm will respond to incidents of fraud.	• Fraud risks are not explored when **new products** and **delivery channels** are developed.

Examples of good practice	Examples of poor practice
• **Lessons** are learnt from incidents of fraud.	• Staff **lack awareness** of what constitutes fraudulent behaviour (e.g. for a salesman to misreport a customer's salary to secure a loan would be fraud).
• **Anti-fraud good practice** is shared widely within the firm.	• **Sales incentives** act to encourage staff or management to turn a blind eye to potential fraud.
• To guard against **insider fraud**, staff in high risk positions (e.g. finance department, trading floor) are subject to enhanced vetting and closer scrutiny. 'Four eyes' procedures (see FCG Annex 1 for common terms) are in place.	• Banks fail to implement the requirements of the **Payment Services Regulations** and **Banking Conduct of Business rules**, leaving customers out of pocket after fraudulent transactions are made.
• **Enhanced due diligence** is performed on higher risk customers (e.g. commercial customers with limited financial history. See 'long firm fraud' in FCG Annex 1).	• **Remuneration structures** may incentivise behaviour that increases the risk of mortgage fraud.

Mortgage fraud – lenders

4.2.2 G This section applies to mortgage lenders within the supervisory scope of the appropriate regulator.

Self-assessment questions:

- Are systems and controls to detect and prevent mortgage fraud **coordinated across the firm**, with resources allocated on the basis of an assessment of where they can be used to best effect?
- How does your firm contain the fraud risks posed by corrupt **conveyancers, brokers and valuers**?
- How and when does your firm engage with **cross-industry information-sharing exercises**?

Examples of good practice	Examples of poor practice
• A firm's underwriting process can **identify** applications that may present a **higher risk** of mortgage fraud.	• A lender fails to report relevant information to the *FCA's* **Information from Lenders (IFL)** scheme as per *FCA* guidance on IFL referrals.
• Membership of a lender's **panels** of brokers, conveyancers and valuers is subject to ongoing review. Dormant third parties are identified.	• A lender **lacks a clear definition** of mortgage fraud, undermining data collection and trend analysis.

4

Examples of good practice	Examples of poor practice
• A lender **reviews existing mortgage books** to identify and assess mortgage fraud indicators.	• A lender's panels of conveyancers, brokers and valuers are **too large to be manageable**.
• A lender verifies that funds are being dispersed **in line with instructions** before it releases them.	• The lender does no work to identify **dormant parties**.
• A lender **promptly discharges** mortgages that have been redeemed and checks whether conveyancers register charges with the **Land Registry** in good time.	• A lender relies solely on the Financial Services Register when **vetting brokers**.
	• Underwriters' demanding work targets **undermine** efforts to contain mortgage fraud.

Mortgage fraud – intermediaries

4.2.3 G This section applies to mortgage intermediaries.

Self-assessment questions:

- does your firm satisfy itself that it is able to **recognise** mortgage fraud?
- When processing applications, does your firm consider whether the information the applicant provides is **consistent**? (For example, is declared income believable compared with stated employment? Is the value of the requested mortgage comparable with what your firm knows about the location of the property to be purchased?)
- What due diligence does your firm undertake on **introducers**?

Examples of good practice	Examples of poor practice
• Asking to see **original documentation** whether or not this is required by lenders.	• Failing to undertake due diligence on **introducers**.
• Using the *FCA's* **Information from Brokers** scheme to report intermediaries it suspects of involvement in mortgage fraud.	• Accepting all applicant information at **face value**.
	• Treating due diligence as the **lender's responsibility**.

Enforcement action against mortgage brokers

4.2.4 G Since the *FSA* began regulating mortgage brokers in October 2004, the *FSA* have banned over 100 mortgage brokers. Breaches have included:

- deliberately submitting to lenders applications containing false or misleading information; and
- failing to have adequate systems and controls in place to deal with the risk of mortgage fraud.

The *FSA* have referred numerous cases to law enforcement, a number of which have resulted in criminal convictions.

Investment fraud

4.2.5 G 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?

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 cover losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are informed by this assessment.	• A bank has performed no risk assessment that considers the risk to customers from investment fraud.
• A bank contacts customers if it suspects a payment is being made to an investment fraudster.	• A bank fails to use actionable, credible information it has about known or suspected perpetrators of investment fraud in its financial crime prevention systems.

4

Examples of good practice	Examples of poor practice
• A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules.	• 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.