Financial Services Authority

Firms' High-Level Management of Fraud Risk

February 2006

Introduction

There is no doubt that fraud is a major, and growing, problem in the UK. The overall size of the problem is very difficult to calculate, but a recent estimate by Norwich Union, collated from a variety of surveys covering different elements of the fraud problem, put the figure at approximately £16bn in 2004. Furthermore, KPMG's latest annual Fraud Barometer, which is derived from UK court cases involving losses of more than £100k, showed that the value of those cases reached £942m in 2005 – nearly three times the value of cases in 2004. KPMG attributed the increase not only to more fraud cases, but also to a greater willingness to prosecute. The two biggest classes of perpetrators, KPMG added, were managers and organised crime, which together accounted for almost 90% of cases.

Within the financial sector, the upward trend of fraud losses was readily apparent until 2004, when, according to the Association for Payment Clearing Services (APACS), total plastic card fraud in the UK reached £505m (an increase of 20% on 2003 and equivalent to £1.4m per day). However, card fraud reduced in the first half of 2005, particularly on lost and stolen cards and counterfeit card fraud – the two types of fraud that are currently being tackled directly by the introduction of Chip & PIN technology. As predicted, fraud has migrated and 'card not present' fraud is now the largest card fraud type, accounting for £151m in 2004. Similarly, cheque fraud losses totalled £46m in 2004, up nearly 3% on 2003. That said, the banking industry has had some success in identifying and stopping more than 90% of all fraudulent cheques as they pass through the clearing system, thus preventing customer loss. Industry savings on preventing cheque fraud rose by 20% – from £556m in 2003 to £665m in 2004.

We announced our new policy on fraud in a speech by our Financial Crime Sector Leader - Philip Robinson – on 26 October 2004. This recognised that there is a strong financial incentive for firms to tackle fraud. So our approach emphasises industry collaboration, information-sharing and leadership (by trade bodies and firms' senior management) and a better understanding of fraud risks and how to tackle them.

Against this background, we decided to undertake a review of high-level management of fraud risk within a sample of 16 firms (mainly larger financial services groups) during the second half of 2005 to assess how firms' senior management were managing this risk.

As part of the review, we met with leading consulting firms, industry bodies (APACS and the Association of British Insurers [ABI]) and law enforcement. This report sets out our findings.

This report does not constitute formal guidance from the FSA given under section 157 of the Financial Services and Markets Act.

The report is published for information but should you wish to provide us with comments please address them to:

James Hastie or John Ellis
The Financial Services Authority
25 The North Colonnade
London E14 5HS

Email: james.hastie@fsa.gov.uk or john.c.ellis@fsa.gov.uk
Telephone: 020 7066 1796 or 020 7066 0976

Executive Summary

1. Overview

- The following points, set out under the same headings as we have used in the main body of this report, summarise the key findings of our review. These include observations of good practice firms have adopted, as well as areas of weakness. We have also highlighted important issues and risks.
- We do not require firms to comply with detailed rules and guidance on fraud management. However, SYSC 3.2.6R requires firms to 'take reasonable care to establish and maintain effective systems and controls….for countering the risk that the firm might be used to further financial crime'.
- These key findings reflect our overall expectation that firms' senior management should be proactive in taking responsibility for identifying and assessing fraud risk and the adequacy of existing controls, and ensure that, if necessary, appropriate additional controls are put in place. We expect a firm to consider the full implications of the fraud risks it faces, which may have wider effects on its reputation, its customers and the markets in which it operates.
- By highlighting examples of good practice adopted by some firms within our sample, we aim to focus the attention of the wider population of regulated firms on areas where many could improve their existing approach to fraud management. While we observed examples of improvements in fraud management that had made a meaningful difference to some firms' success in fighting fraud, firms could do more to ensure they are managing fraud risk effectively.

2. Governance

- Overall we observed good high-level sponsorship of fraud management at executive level, in response to what is perceived as a growing problem.
  - This was by CEOs or other members of the most senior executive committees, and in some cases by Board committees. Boards were informed of fraud incidents and trends but not involved in anti-fraud strategic developments.
  - Developing and monitoring of fraud strategies and tactics were typically the responsibility of high-level management committees, such as risk committees or fraud 'steering groups', and approved by executive members of Boards.

- However, approval of anti-fraud strategies and plans was in some cases informal.
  - In these cases, it was not always apparent under what authority approval was given. As a result, director-level accountability for the delivery of plans and strategies was unclear.

3. Roles, Responsibilities & Resources

- In response to rising levels of fraud, large retail banks and insurers we spoke to have taken steps to improve their fraud management capabilities. These changes will take time to bed down and it is important that senior management maintain an ongoing focus on ensuring their approach is appropriate for the risks faced by the business.
  - This reflects recognition by senior management within these firms that the increasing threat of fraud needs to be managed in a more integrated and effective way.
  - At some firms, mounting fraud losses have driven a more urgent and fundamental reorganisation of fraud management, whereas at others these developments have been more evolutionary. Firms with well established anti-fraud strategies and plans were in a better position to follow the latter approach, i.e. were less absorbed by 'fire fighting' issues as they arose.
  - Although devolved fraud management structures were most common, partly due to the sheer scale of the businesses, we saw the alternative centralised model operating at some firms which could have benefits such as the sharing of best practice and quality control.
- Some other firms, including investment banks, asset managers and some building societies have taken a fresh look at their existing control environment. In particular, they have looked at the assurance provided by operational risk, security and internal audit to ensure their vulnerability to fraud is adequately mitigated.
  - This has been done either through raising the profile of fraud risk within existing reporting and control frameworks, such as making it a standing agenda item at committees or within risk assessments, or through 'steering groups' of senior managers from different parts of the business which are established specifically to consider fraud issues.
  - This approach requires more discipline, and ongoing sponsorship by senior management, to ensure the focus on fraud risk is maintained over the longer term. Where volumes of detected frauds are low, but nonetheless could have a very significant impact on the firm, there is a risk that senior management could 'take their eye off the ball'.

- Some firms have successfully adopted an integrated and comprehensive approach to fraud management.
  - This is where front line business areas are engaged in anti-fraud initiatives which are 'embedded' in the business and supported by a central team (the 'hub and spoke' model).
- We noted some unclear or inappropriate allocation of anti-fraud responsibilities within firms.
  - Anti-fraud responsibilities form an inherent part of many people's responsibilities within a firm, but if accountabilities for these are not clearly defined, they may be de-prioritised in favour of other business needs. An operations area, for example, may place operational efficiency above the need to pause and investigate unusual customer activity.
  - The 'hub and spoke' approach adopted by many firms (see paragraphs 23-25 below) was successful in ensuring that responsibilities and priorities of dedicated central fraud departments were aligned with those of business units.
- In general, firms assessed all proposed anti-fraud investment against the same required rates of return as other investment proposals.
  - As fraud received no 'special treatment', it was acknowledged that fraud managers often faced a difficult task when seeking to justify why they should be allocated additional resources in preference to, say, a marketing initiative that was expected to generate good returns.
  - There is a risk that the full implications of the fraud risks faced by firms – in particular any wider effects on the reputation of the firm, its customers and the markets it operates in – may not be considered when the case for anti-fraud investment is assessed.

4. Fraud Data & Reporting

- Without accurate and detailed fraud data and analysis, firms are not in a position to assess where and why they are at risk of fraud.
  - For example, if fraud losses are 'hidden' within other costs such as bad debts and insurance claims, the underlying causes (and costs) of fraud will be unclear and management will not be in a position to change processes or allocate resources to directly mitigate the risk.

- We saw recent examples of initiatives to 'strip out' and report such losses. However, these initiatives tended to be more reactive (to concerns over the magnitude of crystallised losses) than proactive responses to emerging risks. Firms would clearly be in a better position to manage fraud risk if they were able to establish systems and controls to detect mounting fraud threats at an early stage. There was evidence of this being done in some business units and product lines, but of weaknesses in others.
- At firms that recognise they suffer high volumes of fraud, fraud managers required more detailed and immediate fraud data and analysis to respond to emerging threats. We saw some good examples of this type of management information, but also noted that there were some examples of gaps in the firm-wide coverage of this data.

5. Risk Assessment & Risk Appetite

- Generally we observed improving fraud risk identification, assessment, mitigation and reporting. However, some of this is quite recent and needs to be sustained. Firms tended to define their risk appetite for fraud in terms of budgets and targets for 'expected' losses.
  - Firms are reporting and reviewing fraud risk within operational risk management reporting channels, where these exist, but this information is high level.
  - Only a few firms were developing formal fraud risk assessment processes beyond that required for operational risk purposes, and these were at the early stages of development. As a result, firms tended to respond to fraud risk in a more tactical, incident-driven manner.
  - Firms need to assess the fraud risk that they are exposed to and ensure that appropriate controls are in place to mitigate this risk. For example, a retail firm is likely to require a control environment that is relatively more focused on the risk of identity theft than a wholesale firm, whose controls may be more focused on addressing transaction fraud risk.
  - Firms decided on resources for anti-fraud work more on an incremental basis than driven by a clear cost benefit or risk appetite analysis. Some firms, however, claimed that their mechanisms for determining an appropriate level of resources were more structured than this.

6. Business Engagement, Systems & Controls and 'Know Your Employee'

- Firms that under-invested in anti-fraud systems, controls and processes suffered relatively high levels of fraud losses.

- In business units with high expected fraud losses, investment in systems and controls and a focus on robust anti-fraud operational processes was key to effective fraud mitigation.
- Fraud threats are very dynamic. As fraudsters constantly devise new techniques and exploit the easiest targets in the financial services sector, firms should continue to invest in more effective systems and controls. And they should manage their responses to fraud to avoid being targeted as a 'weak link' in the sector.
- Despite devolving responsibility for fraud management to its major geographical centres and business units, one major firm has recognised the importance of adopting a strategic approach in developing anti-fraud technology by giving these responsibilities to its central group fraud team.

- Focused management of internal (staff) fraud risk and fraud risk in product design are important parts of fraud risk management. As the fraud threat is likely to continue growing, firms will have to be more imaginative and flexible in devising new detection and prevention techniques in these areas, covering the threat from existing as well as new employees.
  - Internal fraud and associated organised crime activity is recognised as one of the main threats to firms and is growing fast. Firms are taking this seriously through, for example, enhanced vetting, high profile arrests, and communication and awareness. Firms realised they needed to employ multiple strategies for countering this threat to overcome the inherent difficulties of tackling the problem, e.g. most fraudsters do not have previous criminal records.
  - It is important for fraud risk identification to take place at an early stage in product development. Firms acknowledged this and we saw reasonable evidence of this happening in practice, but it sometimes came too late in the product development process.

7. External Liaison & Communication

- There are encouraging signs of increased industry cooperation and strong support within firms for this. Nevertheless, more needs to be done in this area – not only to share 'raw' data but also to exchange information on the perpetrators of fraud.
  - Firms see this as critical to the success of anti-fraud measures. In particular there is strong support for various trade associations taking the lead and initiatives, such as information sharing between firms, coming out of this.
  - Firms believe their anti-fraud efforts would benefit significantly from being able to obtain information relevant to frauds from government departments.
  - Legal barriers to effective information sharing are seen by firms as significant but not insurmountable.

- Firms' experience of Law Enforcement's response to reports of fraud was mixed.
  - Firms recognised that some parts of Law Enforcement were better resourced than others to deal with fraud investigations, partly driven by the lack of fraud targets. But major firms who can 'package up' cases (and show a link to organised crime) were generally more successful in engaging Law Enforcement.
- Small firms tended not to have considered fraud risk in a holistic way and gained comfort from the low volumes of detected fraud they had experienced in the past.
  - These firms typically cited the existence of 'core' business controls such as asset reconciliations and compliance monitoring, and management's 'hands on' approach, as providing adequate assurance against fraud risk. But we did not see any evidence that the full range of potential fraud risks had been considered by senior management in a joined-up way.
  - The impact of an individual fraud event could potentially be more damaging to a small firm, and there are inherent difficulties in maintaining a segregation of duties and avoiding conflicts of interest in these firms. Given this, we would expect firms to consider the fraud threats to their business in a more structured way which reflects their vulnerability to fraud.
  - We noted one medium-sized firm that showed how fraud risk could be addressed without onerous extra resource requirements. It did this by clearly allocating anti-fraud responsibilities and using existing risk management and audit processes to ensure key risks are identified and mitigated.

8. Educating Customers

- There are limits to how far firms are prepared to go in implementing anti-fraud measures if there is a risk of causing inconvenience to customers.
  - The degree to which customer experience is expected to be negatively affected by an anti-fraud initiative is a significant factor in determining whether to proceed with the initiative. The position competitors adopt will obviously influence firms' decisions in this respect. But we were also informed that more important factors, such as the need to maintain confidence in an online banking system, may dictate how strong anti-fraud controls should be.
  - For example, in relation to internet banking customer authentication, firms are wary of putting customers off by implementing controls which are more stringent than those of their competitors. At one firm, the marketing department had prevented fraud warning notices being placed on its website for the reason that use of the website should be restricted to marketing purposes.

– In our recently published Financial Risk Outlook[1], we noted that Two-Factor authentication[2] may not yet be cost effective for banks, but it may be adopted if seen as necessary to maintain confidence in online banking or as a unique selling point. However, the industry is looking to establish a pilot using this technology for 'card not present' (telephone order) fraud and this extension to other channels should make the business case more attractive.

1 http://www.fsa.gov.uk/Pages/Library/corporate/Outlook/fro_2006.shtml

2 'a security process in which the customer provides two independent means of identification. Usually this involves 'something you have' and 'something you know' – for example a keyring-sized security device and a password.'

Findings

Overview

1. Fraud is more than just a financial crime issue, it is a reputational one for individual firms and industry as a whole. Our review indicated that senior management of many large firms recognise fraud is presenting a growing challenge and reputational risk to their business. This is attributable to various factors, including mounting fraud losses in some product areas, greater competitive pressures to drive costs down, and increased regulatory attention on fraud issues.

2. As financial services margins continue to be squeezed, the costs of fraud have become more apparent to senior management and reductions in these fraud costs have a more material effect on firms' bottom lines. The extensive and growing publicity given to fraud in the media and concerns about the extent of fraud within the UK in general also mean that senior management are more focused on fraud issues than in the past. However, wider commercial concerns and cost/benefit issues continue to make raising fraud issues an uphill task.

Governance

3. While firms' anti-fraud policies and statements might be issued under the authority of their Boards, we did not find examples of Boards being directly involved in the formulation and monitoring of anti-fraud initiatives. However, on balance, we did not consider this a major issue as, within the retail banks and insurers in particular, CEOs, Chief Operating Officers (COOs), Audit committees and Risk committees were to varying degrees taking responsibility for developing and monitoring these initiatives. We found no examples of a Board Director being assigned specific responsibility for financial crime risk.

4. Boards or Board committees received reporting on fraud losses and trends but, in practice, Board committees tended to be the highest level fora at which fraud issues were discussed in any detail and with any regularity. At large retail institutions which experienced high volumes of fraud, Boards did receive regular standardised loss reports. At the investment banks, asset managers and the small retail firms we visited, the low volumes of detected fraud meant that these reports were relatively infrequent. The most senior executive with ultimate responsibility for fraud management – typically the Finance, Risk or Security Director – was usually responsible for delivering fraud reports to the Board.

5. It was for the responsible Board or executive committees to decide lessons learnt, and approve mitigating controls, if necessary, arising from significant fraud incidents. Boards generally relied on their executives to develop an overall anti-fraud policy or strategy, supported by sound infrastructure and by swift, effective, corporate communication when problems arose. These strategies and policies were typically approved by the most senior executive committee or a member of this committee. The formality of these approval processes varied between firms. In some cases, this was given under clear delegated authority from the Board, but in other cases approval was more informal. As a result, high-level accountability for plans and strategies was less clear. For firms without dedicated anti-fraud resource, policies and strategies were either presented to senior executives for information only or did not exist.

6. In the past, fraud management was driven at the product level. Major firms are now beginning to consider fraud at a strategic level. These strategies and plans were typically developed by heads of risk, financial crime or fraud functions. And they were monitored by senior executive committees, such as risk or security groups, or fraud 'steering groups' which were relatively new bodies set up to look at fraud on a more holistic basis. These groups were typically chaired by heads of risk, financial crime, audit or, at an insurer, claims.

7. The level of seniority and range of responsibilities of people who sit on these groups or committees was a key factor in ensuring coordination and effective implementation of anti-fraud strategies and of decisions and actions taken in response to fraud issues. At one major firm, this group was chaired by the COO and included the heads of major product and controlling functions.

8. However, at one firm we visited, we saw a lack of clarity over how the firm's anti-fraud strategy was articulated. Senior management expressed contradictory views on this. Some were under the impression that their firm's fraud policy document constituted a fraud strategy but others considered the strategy was embodied in the 'totality' of the control environment.

Policies and Procedures

9. Because of the diversity of the large firms, developing a set of group fraud policies and standards was seen as the first step in building an integrated approach to fraud risk management.

10. Within the retail banking and insurance sector, every firm we visited had in place some form of high-level Fraud Prevention Policy or Fraud Policy Statement. These documents typically stated the firm's clear commitment to preventing and detecting fraud and set out, in broad terms, fraud definitions, responsibilities (for example between the centre and the business units), internal reporting procedures and investigating processes.

11. In general, these Policies or Statements set out minimum standards, leaving the Divisional Fraud teams, where they exist, the discretion to determine their individual fraud strategy. These individual documents were overseen and subject to challenge by the Group. More detailed guidance covering, for example, the firm's Fraud Response Plan, was generally readily accessible via an intranet site.

12. The high-level policy documents were owned by group fraud departments, which were responsible for ensuring the (minimum) standards were adhered to throughout the groups. They were often subject to regular (usually annual) review and in some cases sign-off by Boards.

13. In other financial sectors, including investment banking and asset management, where volumes of fraud were very low (although the potential impact of fraud could be high), there was no one high-level anti-fraud document. Rather, all the controls and procedures, in place to protect the firm's and its customers' assets, together constituted the firm's fraud prevention policy (see paragraph 60 below).

14. Some firms had conducted an exercise to review these controls and procedures, to ensure that they provided sufficient coverage of potential fraud issues, even if these issues might not be specifically 'labelled' as fraud related, and produced an overarching high-level policy document.

Roles and Responsibilities

Structures

15. High volumes of fraud experienced by retail banking and insurance firms have typically led these firms to adopt relatively well-defined anti-fraud roles and responsibilities. Fraud management within these firms is becoming more integrated in order to tackle the threats more holistically, for example by transferring best practice in relation to ATM or credit card fraud quickly from part of a group to another.

16. Where the incidence of fraud is relatively low, such as in the investment banking and asset management sector, large firms rely on various control procedures which are not specifically labelled as anti-fraud measures. For example, these relate to physical security, procurement and whistleblowing, to provide assurance that fraud risk is being mitigated. While these firms have implemented some projects and other initiatives to assess their vulnerability to fraud, they continue to divide responsibility for fraud management between different business functions. Without formal, integrated anti-fraud responsibilities and structures, these initiatives may be more difficult for firms to sustain on an ongoing basis.

17. However, one relatively small asset management firm proved that it was possible to install formal and robust fraud control mechanisms which linked in with its existing control environment but did not entail significant additional resource or effect on business efficiency. These initiatives included clear allocation of responsibility to individuals and committees, relevant management information and controls focused on the areas of greatest risk.

18. The allocation of anti-fraud responsibilities within firms varied and, in some cases, was very new. We saw some fraud departments located in risk management or joined with the anti-money laundering teams within a financial crime department. In some cases, security and fraud functions were combined, but most security departments (both physical and IT) were located separately from the fraud area.

19. Overall, we observed that the allocation of responsibilities for the day-to-day management of fraud risk was clear. In large groups, fraud managers typically had dual reporting lines, to local business management and more senior fraud management, which ensured that their work was integrated with, and aligned to, the priorities of the business. At one group, there was clear evidence that a previous lack of clarity and direct accountability over anti-fraud responsibilities had significantly impaired the organisation's ability to tackle fraud threats. Some firms had reallocated responsibilities between the business units and a central fraud function to improve accountability for, and a focus on, fraud. They did this either by devolving more responsibility to business units or by centralising activities that had previously been given insufficient priority in the business.

Fraud vs AML

20. Many firms saw the integration of fraud and anti-money laundering (AML) as beneficial for operational reasons, in particular for processing suspicious activity reports and liaising with third parties such as law enforcement. Financial crime managers did, however, recognise that there were important differences between fraud management and AML, particularly in the way they affected firms' profit and loss accounts and the degree to which they were governed by statutory and regulatory requirements.

21. As a result, the relationship between fraud management and AML at firms varied considerably between firms. Within investment banks and asset managers, where volumes of detected fraud were low and anti-fraud responsibility was not allocated to dedicated fraud managers, responsibilities for AML were typically closely aligned with compliance. In retail banks and insurance firms, where significant resource was dedicated to anti-fraud measures, responsibilities for these at the operational level (and sometimes at the senior management level) tended to be separate from those relating to AML.

22. Firms recognised there could be benefits from combining AML and anti-fraud teams – for example from synergies arising from using common monitoring systems and sharing intelligence. However, differences in the legal and regulatory requirements around these two areas and operational responses to issues meant that firms had to consider carefully whether combining the two might reduce the focus and effectiveness of either function.

Embedding in the business

23. The importance of embedding specialist anti-fraud responsibilities in the 'front line' of businesses, with these responsibilities reflected in job descriptions, was seen by several major firms as key to successful fraud mitigation. Given the diversity of the product base, and therefore the potential fraud risks faced by major firms, the knowledge and skills within the customer-facing and operational parts of the business were a vital resource for identifying and mitigating fraud risk and reacting quickly and effectively to fraud threats. This model was typically part of a 'hub and spoke' approach whereby support was provided to the 'front line' by a central team whose primary responsibilities were developing and enforcing policies and standards, monitoring, reporting and highlighting threats and sharing best practice.

24. At one insurance firm, a good example of this 'hub and spoke' approach took the form of fraud managers being appointed in each branch to ensure fraud reporting was consistent with the firm-wide definitions. These people were supported by assistants and fraud coordinators in each team. The fraud coordinators' role was part-time and involved coordinating a team's anti-fraud activities and spreading best practice.

25. The sheer scale of some firms dictated that fraud be managed according to this type of 'hub and spoke' model. However, this model was not universally followed. There were more centralised approaches – where fraud responsibility was 'passed through' the business to a central team, adopted in some cases for reasons such as operational efficiency and the effective exchange of information, or where the business was not large enough to support a devolved structure.

26. At an investment bank, a different approach was adopted: business unit risk officers had a generic responsibility for independent risk control, including all aspects of security risk, to ensure that risks had been identified and that policies and standards had been established. They and, where applicable, their security risk control specialists were responsible for, among other things, signing off security risk aspects of all 'new business' proposals, and regularly assessing the adequacy of fraud prevention measures, in particular:

    - the extent and effectiveness of segregation of duties;
    - monitoring and investigating security incidents, including fraud, and determining or recommending necessary actions; and

- recording all security incidents and initiating reviews ('back tests') of security risk operating standards in response to significant incidents or near misses.

27. Firms also recognised that central responsibility for anti-fraud measures had a role to play in countering threats that were increasingly common across products and geographical locations – for example, in relation to internet banking and ATM fraud. In addition, where some major firms chose to run separate brands for specific product lines, there was a trend towards integrating anti-fraud operations for these products. This was expected to lead to a reduction in fraud losses through applying fraud management best practice to all products with similar characteristics and the availability of more and better resources (technology, skills, intelligence).

28. Law enforcement agencies emphasised to us the importance of 'embedding' anti-fraud responsibilities (particularly in relation to new product approval) within the business so these are seen as part of the day-to-day management of the business, and of assessing risk as widely and as early as possible in product development. For example, there were numerous fraud cases during the late 1990s when firms expanding rapidly into the PEP/ISA market did not address anti-fraud deficiencies in their business processes. These deficiencies allowed applicants to withdraw funds before the initial cheque deposits cleared.

29. In credit and debit card businesses, the size of fraud losses has a consistently large effect on the businesses' profitability, expected patterns of loss are relatively clear and the speed of response is critical to the mitigation of fraud losses. Here, we found that anti-fraud management is better developed than for other financial products. It appeared to be most effective when it operates closely with the business. For example, a firm could pick up intelligence on trends from its fraud response telephone operators. In this way, effective strategic and tactical responses to rapidly changing risks and threats can be agreed and implemented quickly. These responses include changing the parameters and rules for monitoring systems or making changes at short notice to a marketing strategy, while at the same time striking the right balance between fraud mitigation and customer relations.

Fraud Data and Reporting

Internal

30. Overall, we found a good level of fraud reporting (although it was evolving and at a relatively early stage of development) to the appropriate senior management decision makers.

31. Within this, the regularity – and nature – of fraud reporting to senior management varied between firms. Generally, the relevant Board committee would receive reports of fraud losses, trends and issues at least half-yearly and often quarterly, while the Board itself would be informed only of major fraud events, typically via a regular risk report. At executive management level, reporting was often more frequent.

32. It was common for senior executive management in large firms to receive regular reporting of direct fraud management costs (i.e. dedicated anti-fraud teams and systems), fraud losses and estimated 'savings' made by fraud mitigation initiatives (e.g. declining fraudulent applications and/or detection of fraudulent transactions before funds are paid away), but no firm had attempted to quantify and report the full costs of fraud mitigation. While the costs of dedicated anti-fraud teams and systems could be easily identified, the 'embedded' cost of anti-fraud work by the business as a whole was considered impossible to strip out from day-to-day 'business as usual' costs.

33. One major bank, which monitored its fraud experience daily, kept the Board informed with a monthly management information (MI) pack that covered not only significant fraud risks and issues but also relevant regulatory developments. A similar approach was followed by a fund manager, whose Board did not receive MI specifically related to fraud but, rather, received papers prepared by the firm's Controls Group, which dealt with issues relevant to fraud prevention. Another major bank supplemented its quarterly reporting of significant fraud issues to the Audit Committee with weekly financial crime 'flash' reports by the Head of Financial Crime to the bank's Executive Committee, covering high-level fraud loss and operational performance trend and variance data.

34. The large firms collected and reported fraud data to senior management as part of their overall operational risk management process. Typically, the Operational Risk Management (ORM) function would collect information on all operational risk events, including fraud and theft among the cause categories. ORM would be responsible for producing monthly reporting packs, which identified the value, number and causes of losses suffered in the reporting period. These reports might also include analysis of lessons learnt from fraud incidents and the position on recoveries or simply high level aggregated data showing details of different categories of fraud (e.g. internal and external). One firm applied thresholds to its reporting, namely, capturing all events with an impact of £25k or more, and providing a detailed post mortem on events with an impact exceeding £500k.

35. Fraud data reported through the ORM process was provided by fraud management and operational departments, which typically also reported to senior management through separate channels. This separate fraud reporting tended to provide a more granular and timelier analysis of fraud incidents, trends, issues and mitigation initiatives. The difficulties of putting in place data feeds from different business units was apparent at one firm which was not yet able to report a consolidated picture. One major bank had responded to this issue by implementing a consolidated fraud data collection system, which provided a complete set of aggregated fraud data for management reporting purposes and acted as a group wide case management system.

36. Recognising the significant amount of fraud previously 'hidden' within credit losses, a major retail banking group recently conducted a major review to 'cleanse' accounts and identify fraudulent activity. Following on from this, the group was intending to develop its own fraud scorecards for credit applications.

37. The way in which fraud losses were allocated within firms varied. Some firms viewed the allocation of fraud losses to individual business units as important in order to match costs with responsibility for management of those costs. Where fraud management was more centralised, firms tended to favour booking fraud losses centrally, although this is less common than in the past.

External

38. We found strong support from firms for industry-wide initiatives, notably by APACS (taking over from the British Bankers' Association [BBA], in this regard), the ABI and the Building Societies Association (BSA), to collect consistent fraud data based on common definitions and share that data between trade association members. Individual firms were keen to compare their own fraud experience with aggregated sector information, so they could assess the effectiveness of their fraud prevention efforts.

39. APACS has been helping its members share intelligence on a number of fraud types including account takeover. It also plans to explore the options available to share intelligence on internal frauds. Meanwhile, limited information on internal investigations (which provides relevant information without naming the fraudster) is already being provided to APACS. Sharing of intelligence on major payment and lending fraud cases via APACS has been going on since about June 2005, using APACS's existing 'closed user group' internet system. Participating banks are able to match against others' data, e.g. on a personal loan fraud ring, to see if they are being attacked by the same people.

In October 2005, an individual was jailed for five and a half years for conspiracy to defraud. He was described as the ringleader in a sophisticated operation that involved two accomplices, who were also jailed for fraud and money laundering offences.

The fraudster used forged passports and utility bills to open bank accounts, built up credit on those accounts and then defaulted on his debts. His method was to work in stages, creating false identities, opening accounts and gaining the trust of the banks, before applying for extra credit facilities on which he defaulted. He eventually had 473 separate accounts, including 200 with one high street bank and 85 with another. He set up 112 separate mail redirection facilities so that the banks would be unable to trace him. He operated the accounts to avoid giving rise to suspicion, giving the banks and building societies the impression that he was an ordinary customer receiving a regular income.

40. The insurance industry has collaborated to set up the Insurance Fraud Bureau (IFB). The IFB will improve insurers' ability to detect and prevent organised insurance fraud. At present, industry capability to manage that risk is constrained because insurers acting individually find it difficult to detect linked events. The IFB will use existing shared data from three of the major insurance databases. The data will be cross-interrogated for suspicious activity using specialist data-mining techniques and any such activity reviewed to identify possible fraudulent claims that might warrant further investigation. The pilot test identified potential fraud savings of at least £50m a year: with improved data quality and refinement of detection techniques, total savings could reach £200m a year. The IFB will start operating in 2006.

41. Insurers are cooperating in other ways too. The ABI is developing its techniques to measure the scale of general insurance claims fraud. In 2006, it will extend this measurement to internal, life and health (clients and care providers) fraud. The ABI has set up a series of workshops to help spread good practice between firms and, in particular, to reduce the vulnerability of small insurers to fraud.

42. Benchmarking fraud data is very difficult, because of different definitions and completeness issues, e.g. fraud versus 'gone away' claims, and, most importantly, because each firm's book and risk profile/appetite are different. In 2004, the ABI began to collect claims fraud savings data from firms under consistent definitions. This is used to make broad assessments of fraud costs and to feed data back to members on how they compare to the industry average. However, there may be good reasons for the firm to be below the average. The ABI stressed there was a tension between simplicity and avoiding subjectivity when reporting, while also noting that a major challenge is to estimate what is not being declared and identified. If successful, data sharing should highlight examples of potential under-reporting.

A recently published (November 2005) report by Norwich Union, entitled 'The Fraud Report – shedding light on hidden crime', drew attention to the involvement of criminal gangs in organised motor insurance fraud. These gangs, the report said, 'seek to defraud insurers and consumers by submitting high volumes of false motor insurance claims for damaged vehicles, personal injury and associated losses of earnings and suffering'. A particularly worrying feature of induced accidents is that the criminals' preferred targets include unaccompanied women and the elderly, who are considered the drivers most likely to admit liability on the spot. The Norwich Union report states that this is the fastest growing area of organised motor fraud.

43. Many firms cited the importance of having an effective mechanism for communicating fraud news, warnings, trends and mitigation initiatives as a vital component of an effective anti-fraud strategy. This would be both within groups with direct responsibility for fraud management and, on a wider front, throughout organisations as a whole.

44. Most firms applied judgemental criteria, usually determined by compliance and legal departments, to assess whether frauds were 'significant' under the FSA's rule SUP 15.3.17 and therefore reportable to the FSA. However, some applied fixed thresholds to determine whether to report. Recent proposed revisions to these reporting requirements should provide firms with more useful guidance on what to report and align the requirements clearly with our financial crime objective, as well as with concerns relating to firms' financial soundness.

Risk Assessment & Risk Appetite

Risk appetite

45. Few firms have been able to formally articulate their overall risk appetite for fraud or measure risk at a high level. A more common approach was for fraud loss (and savings) targets or budgets to be set, based on previous experience or from benchmarking against industry data.

46. Senior management was also able to demonstrate its risk appetite on an ad hoc basis, through its willingness to provide the resources necessary to deal with fraud incidents or through its other decision-making. For example, we were told by a major insurer that the UK CEO had been influential in changing the firm's risk appetite, exiting unprofitable lines of business and only underwriting business where the firm fully understood the risks. This had an immediate impact on claims fraud the car rental business suffered because of staged accidents.

Risk assessment

47. Fraud risk data were generally being reported and monitored through firms' operational risk frameworks. In some cases, control self assessments conducted for the purposes of meeting Sarbanes Oxley requirements also gave firms assurance on the adequacy of fraud controls. However, the management of operational risk was, to some extent, work in progress because risk registers, maps and profiling were still under construction, in part to meet the requirements of Basel II. And this assurance was provided at a relatively high level or in relation to one part of the overall fraud control environment, e.g. financial controls.

48. Firms which suffered regular fraud losses saw the need for significant additional detailed risk analysis and monitoring by dedicated anti-fraud teams. Some major firms had recently started to produce more detailed fraud risk assessments (including key risk indicators) at business unit and product level that fed into operational risk assessments. However, overall, specific detailed fraud risk assessment processes were at an early stage of development.

49. Where businesses were producing fraud risk profiles, we found that group fraud risk departments reviewed these and were able to challenge the risks documented by divisional fraud teams. One major bank required all its business areas to undertake one full risk assessment each year and to update their risk profiles quarterly with any significant changes.

50. At a major insurer, fraud risk self assessments were being rolled out across the business to form part of an overall financial crime risk assessment. Once these are fully developed, they will be combined with the AML risk profiles. The risk profiles were initially produced on a judgemental rather than empirical basis, i.e. the views may be correct but they are difficult to prove, and a process would follow to assess the judgements objectively.

51. Where fraud risk profiles were being developed, group and divisional fraud risk departments had, or were in the process of devising, suites of Key Risk Indicators designed to provide the Board with a high-level view of the management of key fraud risks across the Group. We saw that some divisional fraud teams have developed reports to highlight current fraud trends and potential future fraud exposures. This information was used, among other things, to devise new anti-fraud procedures and strategies and in refining detection systems. However, we found one example of fraud risk reporting not including all business units within the firm that were considered to be vulnerable to fraud.

52. Some firms without dedicated anti-fraud departments had set up working groups, led typically by senior risk or internal audit functions and including representatives from the main business units and support areas. These groups conducted gap analysis of the adequacy of 'business as usual' controls against fraud including, for example, hiring practices; information security and privacy; physical security; sourcing and procurement; and treasury controls.

53. In the smaller firms we visited, fraud risk tended not to have been addressed in a systematic manner. Fraud issues were likely to be less frequent than for the large firms but nonetheless could potentially pose significant risk to the firm. Fraud events were likely to be dealt with in an ad hoc fashion depending on the specific circumstances of a case.

54. In general, we found that fraud risk identification and control featured in the review process for new products and delivery channels. However, this did not always take place at a sufficiently early stage in the development process.

Business Engagement, Systems and Controls

55. Among retail banks and insurers, we found a variety of fraud prevention and detection systems and controls operating successfully. We also found that under-investment in such systems and controls, to create a sustained anti-fraud capability, was likely to render a firm a soft target for fraudsters.

56. For credit and debit card businesses, where the threat of fraud is high and long established, anti-fraud management and techniques were typically most well developed and sophisticated. One major banking group was using two different systems for transaction monitoring of its unsecured credit portfolios. Both rules-based systems were considered to have been exceptional investments as they had significantly increased the group's ability to identify fraudulent activity on plastic cards (e.g. a new PIN requested in a short space of time or a flurry of transactions occurring at a high-risk retail outlet). Even so, both were kept under constant review for possible enhancements to performance, with the result, for example, that a lot of customers could be contacted quickly about a suspect transaction and with minimal staff.

57. The same banking group had also achieved major fraud savings, in the corporate banking area, through its pioneering introduction of a system for identifying fraudulent cheques. In its general insurance business, the group had successfully used Voice Risk Analysis (VRA) to screen customer telephone conversations and identify claims worthy of further investigation. We were informed that fraud savings had doubled as a result of the introduction of VRA and had not significantly affected renewal rates. In addition, the group had developed its own, very cost-effective, proprietary software for claims investigation under household and travel insurance policies. This provided a basic assessment of the reported loss against generic industry-wide information concerning the degree of fraud risk for that particular type of product.

58. We noted, however, that two major insurers were less convinced of the merits of VRA. One firm had found that its own cognitive interviewing techniques out-performed the VRA software, which was also very expensive. The other firm also considered such lie detection technology as no more effective than its existing anti-fraud measures and also as incompatible with the business's customer service model. This second firm had initiated a project to develop automated scorecards, as the next phase of anti-fraud 'optimisation'. These scorecards would be based on several risk factors, derived from the insurer's claims database, for use in identifying potentially suspicious claims.

59. Firms recognised that their ability to meet emerging fraud threats as quickly as possible critically depended on good analytics in their anti-fraud operations. Some anti-fraud systems had measurements in place to manage the 'false positive' ratio and refine the system rules accordingly. The lower the ratio the more effective a particular rule is in identifying fraud, indicating better fraud detection rates and improved customer service. As an example, when several debit cards from one bank were stolen from a Royal Mail sorting office, rapid detection of the theft through analysing transaction patterns and new fraud claims allowed a new prevention rule to be implemented, within 24 hours, that identified stolen cards at an earlier stage. This reduced the impact on, and inconvenience to, customers (who didn't know their cards had been stolen) and resulted in savings of £1.3m.

60. For large firms that experienced very few frauds but could be seriously damaged by the impact of a single fraud event – like investment banks, fund managers and custodians – senior executive management tended to rely on a key set of general control practices in their various business lines to manage fraud risk effectively. Typically, these would include: robust client/firm instruction authentication; segregation of duties; restricted system access; dual control over cash and securities transfers; daily reconciliation of movements of cash and securities; and a rigorous exceptions management process. At a higher level, these controls would be supported by what one firm termed 'Core Controls'. These are Hiring Practices; Information Security & Privacy; Physical Security; Sourcing and Procurement; and Treasury – Bank Account Controls. Given the size of the potential fraud risk in custody operations, the two fund managers in our visit sample exercised considerable due diligence in the appointment and monitoring of custodians.

Whistleblowing

61. All but one of the firms we visited had established whistleblowing procedures which were readily accessible to staff (often on the intranet) and usually managed by the firm's Compliance, Legal or HR Departments and in some cases by corporate security. In a few cases, the procedure gave staff the option of contacting an external agency to make an anonymous report. One major insurer operated a global whistleblowing hotline that was operated by an external agency which provided a multilingual contact centre open 24 hours every day.

62. One major retail bank had received 48 disclosures in the last year, 10% of which were fraud related. But this was an exception, with the number of whistleblowing reports made annually typically being small and very few relating to fraud. Instead, reports tended to concern HR matters (e.g. time-keeping), abuse, malpractice (e.g. use of a firm resource for personal purposes) and management style and conduct.

63. This low level of reporting did not appear to be attributable to any lack of staff awareness of the whistleblowing process. One firm displayed a large poster in every workplace; another included whistleblowing as part of the compliance department's annual regulatory testing of all staff; and a third firm reminded staff of the availability of the 'hotline' at least annually.

64. The small numbers of reports were neither a surprise nor a concern to any of the firms. Most were confident that they had an open culture, in which staff felt able to raise malpractice issues with their line manager, and get them resolved, without fear of being penalised. Several firms mentioned that the term 'whistleblowing' had unfortunate connotations of 'snitching' on colleagues, which might make staff reluctant to use the formal procedure. Consequently, some firms preferred to use the term 'professional standards' or 'ethics', rather than 'whistleblowing'.

65. In general, senior management were kept informed of the (lack of) use of whistleblowing procedures and had evinced no concerns. In the case of the bank that received the most reports, the Audit Committee conducted a half-yearly review of reports received and looked at actions outstanding. A recent whistleblowing audit had rated it as 'amber', the main concern being awareness and use of the procedure. As a result, the policy was to be re-launched to raise its profile bank-wide, and possibly re-named as a Professional Standards line.

66. A common view expressed by firms was that, to foster an environment in which staff were prepared to make reports, whistleblowing procedures should be considered as one of several options available to staff who wished to disclose sensitive issues. Encouraging staff to make reports in whatever way they feel comfortable, by fostering an open and ethical culture and encouraging staff to report issues, if appropriate, through their line management or HR departments was seen as equally important.

Recruitment (Know Your Employee)

67. Major firms and Law Enforcement consider insider fraud, whether arising from coercion, collusion, infiltration or existing employees' own initiatives, to be one of the most serious fraud threats faced by financial institutions. Evidence of this threat, which is growing very rapidly, can be seen from the increase in payment fraud and account take-over relative to more 'traditional' threats such as cheque fraud (although the latter is also now increasing as criminals seek alternatives to credit card fraud in response to the introduction of Chip & PIN).

In December 2005, a postman was jailed for six and a half years for masterminding a £20m chequebook and credit card fraud. He worked at a sorting office in North London, where he stole chequebooks while sorting the post for his Golders Green round. He then farmed out the chequebooks to a gang of around 220 people across the UK. They would take one or two cheques from each book, pay them into both legitimate and bogus bank accounts, and then destroy the remaining cheques. The fraudsters managed to avoid detection by only cashing cheques for values between £800 and £1,200. Some victims were unaware that they had been defrauded, and it was only when the police received an average 12 reported thefts per day that an investigation was launched.

In total, 45 people were arrested in raids around the country, 23 of them were convicted of a range of offences including handling stolen goods, forgery and deception. Most of the defendants were sentenced to between six months and three years in jail.

68. In addition to issues about the security of data within firms, the banking sector is increasingly concerned about the security of data held by third parties outside the financial sector. If standards here are weak, banks are vulnerable. Recent media 'scares' about the security of customer data seem to have resulted from information 'leakage' at non-financial companies.

69. Examples of staff being approached by criminals nearby their place of work (whether a branch, call centre or other operational area) and offered money to sell confidential customer information were cited by firms and Law Enforcement as the most common incidents of this type of fraud. What an employee may initially see as an easy way of earning extra money, and maybe 'getting even' with an employer, can easily end in blackmail and violence if the employee tries at a later stage to end the relationship with a criminal.

70. Criminals who get customer information in this way will often pass it on to others who can gain the most benefit from it by collating data obtained from various sources. Indeed, fraudsters will often ask different employees to obtain different pieces of information on the same customers. The sustained nature of some fraud attacks was illustrated to us by examples of fraudsters repeatedly contacting the same customers and their banks in attempts to deceive them into revealing different components of the customers' security details.

In September 2005, a cashier at a high street bank branch in Cosham, Portsmouth, was sentenced to two years for helping fraudsters steal almost £500,000 from customers' accounts. She served customers at the branch and then trawled through their accounts to check whether they had made any large deposits in the past. She then passed on their details to a criminal gang.

Equipped with information such as balances, last transactions, and direct debits on the accounts, gang members walked into branches in London and Cardiff and asked to change address details and to set up online banking facilities. They then used the internet to transfer funds to their own accounts.

The cashier claimed she had been intimidated by two people she met at a Portsmouth nightclub and insisted that she herself had gained nothing from the fraud. The police said it was clear she had been targeted by professional criminals.

71. To counter the rising threat of internal fraud, particularly in the retail banking sector, a number of firms were tightening up their employee vetting procedures to keep fraudsters out. Several firms had decided to use specialist external agencies to undertake pre-employment screening and thereby identify potentially untrustworthy employees.

72. The intensity of the vetting process varied between firms and was not always applied to temporary as well as to permanent staff. One major firm's practice was to have new employees vetted at two levels, depending on whether the new recruit was to perform an FSA-regulated role. At another firm with a substantial proportion of contract and temporary staff, the increased risk had resulted in a major drive to improve employee vetting.

73. Another firm applied seven levels of employment screening, the degree of due diligence depending on whether the individual was a junior administrator or a senior manager. The external agency acting for that firm undertook a series of detailed checks on the recruit's background and employment history. It then analysed the results compared with known deception profiles, as well as highlighting any gaps and discrepancies in the information provided by the recruit. Any negative information discovered led to the firm automatically rejecting the candidate. This firm had rejected five potential new hires in the preceding year, mostly for stating false academic or professional qualifications, which constituted a very small percentage (unspecified) of total hires in that period. However, another firm told us that its failure rate currently stood at 8% of all potential recruits checked out by the agency.

74. One large investment bank began vetting key suppliers within the last two years. Each contractor must screen its own employees to a standard agreed by the bank, which will shortly be putting in place random sampling via unannounced visits, to check that its contractors are actually carrying out appropriate levels of screening.

75. We were told by one major retail bank that it was working with the Metropolitan Police on insider profiling, which allowed the bank to compare new recruits against those profiles. The profiles showed that fraudsters were often over-qualified for their role and that 73% were not on the Electoral Roll.

76. Firms saw the current CIFAS and APACS initiatives (see paragraph 99 below) to develop databases of staff dismissed for fraud or dishonesty as a very positive development to reduce the risk of known fraudsters being re-employed within the financial services sector.

77. All firms are exposed to the risk that they might hire people who have previously been dismissed for fraud-related issues. Furthermore, firms need to be alert to indications that existing employees may begin fraudulent activity.

Anti-Fraud Training

78. The approach adopted by firms to staff training and the importance attached to this varied. Some firms combined fraud awareness and anti-money laundering training, while others covered fraud issues as part of a more wide-ranging 'security awareness' training package. Generally, fraud awareness training was given to new staff as part of their overall induction training and a number of firms regularly sent out newsletters or alerts to staff about fraud risks and fraud attempts. Most firms relied on computer-based training packages of some kind.

79. One major firm we visited had evolved a new training strategy, predicated on the need to help all its employees recognise 'red flags' that might indicate an increased risk of fraud (e.g. unexplained wealth or financial problems, reluctance to take leave, pressure to make performance targets, autocratic line management, client complaints and high staff turnover) and also the categories of controls that were most effective in detecting and preventing fraud (e.g. authorisation and approval, reconciliations, and segregation of duties). This firm had hired an external provider specialising in e-training to build a stand-alone training module that all staff had to take. The module incorporated a test with a pass-mark of 80%, with any staff member failing to achieve that score having to re-take the test.

80. A somewhat different, but no doubt equally effective, approach adopted by a major banking group was to have in place good practice guidelines, set by its Group Fraud Risk department, for fraud awareness training at divisional level. This document defined the requirements of fraud awareness training (as described in the Group Fraud Policy Statement); the roles and responsibilities at group, divisional and individual level; the methods of delivering training; and the documentation and record keeping that are required. Each division then created its own fraud awareness training for staff, tailored to support that division's needs, objectives and risk profiles and to meet its own preferred training methods.

81. As an example, the retail fraud team at one bank had developed a fraud investigator programme that has been delivered to the branch network in North London to assist internal investigations. Early results show improved fraud prevention and awareness, as well as reduced losses. All new employees in the retail division receive anti-fraud training and all staff receive ongoing information, e.g. via newsletters, on current trends and issues.

82. Similarly, we found that major insurers tended to tailor their anti-fraud training to the needs of individual business units. Such training was essential for staff handling claims, for example, who might also receive more specialist training in cognitive interviewing.

Resources for Tackling Fraud

83. We found that the size of dedicated anti-fraud teams, and specialist anti-fraud staff within business units, in several firms had increased in the last few years. For example, the fraud team at one major building society had more than doubled (from four to nine full time employees) over the past three years. And a major insurer had plans to redeploy staff from its central fraud unit to individual business units, and also recruit new specialist fraud handlers, equating to an overall increase of about 25% in anti-fraud resource.

84. Some firms informed us that additional fraud resource could easily be justified by the fraud cost savings that would result from this. However, the pattern of recent year-on-year increases in resource appeared to have occurred in more of an incremental fashion rather than being driven by a fundamental re-appraisal within organisations of the optimal level of resource required.

85. Awareness of financial crime generally, and fraud risks in particular, had increased significantly in recent years. This was attributed to a variety of factors, not least our statutory financial crime objective and the profile of fraud being raised in a speech by our Financial Crime Sector Leader, Philip Robinson, in October 2004. This prompted at least one firm to conduct a formal 'gap analysis' to see how it measured up.

86. However, a consistent message we received across all financial sectors was that, whether additional resources were needed by way of staff or for technical development, there must always be a clear business case made to senior management to gain approval. These financial considerations, i.e. an acceptable level of return, seemed to outweigh more qualitative concerns, such as reputational risk. In general, this resulted in relatively high hurdle rates being applied to proposals for new anti-fraud investment. When faced with a choice between investment in anti-fraud controls or, for example, a revenue-enhancing marketing campaign or customer management system, management naturally would have to think carefully before deciding against the revenue investment option.

87. It was not always clear what would constitute an acceptable return, partly because anti-fraud expenditure tended to show diminishing returns over time. At one extreme, we heard a major insurer's view that a £10m investment in anti-fraud measures would need to generate £30-40m of savings a year to be justified. However, another insurer was satisfied with a position whereby its central fraud team generated recoveries that exceeded the annual running costs of that team. The cost-benefit ratio was too difficult to quantify for business units, because their staff often had other responsibilities in addition to fraud risk management.

88. A more clear-cut example of the need for a sound business case, in the area of technical development, concerned Two-Factor authentication procedures for access to internet banking. We were told that several banks already had such procedures in place for corporate banking but the key strategic investment decision was whether to extend these procedures to retail customers. That decision would critically depend on the extent to which a bank had been specifically targeted by fraudsters (e.g. 'phishing'[3] and keystroke logging attacks have usually originated abroad and been aimed at banks who are well known internationally) and the degree of concern about possible loss of consumer confidence in internet banking.

Fraud Investigations

89. Large retail and insurance firms allocated responsibility for significant or complex fraud investigations to specialist departments. We found these departments to be appropriately skilled. At other firms, responsibility for fraud investigations was given to corporate security or audit departments (although one insurer had recently moved this from internal audit to avoid potential conflicts). We saw no evidence of inadequate resources being applied to investigations. However, these departments were selective in taking on cases which appeared to offer the best chances of success. As part of their devolved fraud management structure at the insurers, most suspected claims fraud cases were dealt with in the claims teams by using the experience of local fraud 'champions', based on guidelines issued from the centre. This model placed anti-fraud responsibility with those closest to the customers who were best placed to assess the majority of cases as efficiently as possible.

90. We saw examples of fraud investigation teams within large organisations being able to conduct investigations to criminal investigation standards (including computer forensics). The view of firms that were able to do this was that this significantly increased the chances of law enforcement taking on a case.

3 'Phishing' attacks are where criminals send spoof emails misrepresenting corporate identity to trick individuals to disclose personal financial data such as account numbers and PINs. They create websites that mimic the trusted brands of well-known financial firms.

91. We found that firms experienced mixed responses from the police when reporting frauds. The response typically depended on factors like: a possible link to organised crime (e.g. drugs trafficking) or terrorist financing; the individual police force's ability and inclination to investigate (e.g. the force having a specialist financial investigation team and a fraud target); police knowledge of the type of fraud (banking frauds were thought to be more familiar to the police, and easier to prove, than insurance frauds); and whether a firm could package the information it passed to the police in a 'police-friendly' way. But sometimes firms found that progress with investigations could be hampered by cases being passed from force to force, without any one financial investigation team accepting 'ownership'.

92. We were also told that the criminal justice system was partly to blame for the difficulties in taking forward fraud investigations and prosecutions. The Crown Prosecution Service was perceived to be reluctant to prosecute fraud, given the current state of the law and the risk of investing a huge amount of time in pursuing a case with a very uncertain (or inadequate) outcome in the courts. While audit trails can make fraud relatively easy to prove, factors such as the cost of data retrieval and the potential unpredictability of the jury system when applied to fraud trials create difficulties for law enforcement. In addition, the incentive for forces to investigate frauds is diminished by the absence of Home Office targets for dealing with this type of crime. As a result, fraud squads can be seen as a spare resource which can be used for other purposes.

93. In spite of these difficulties, firms tended to seek criminal prosecutions wherever possible or, failing that, civil restitution. These actions, together with arresting staff in their office environment – with the message communicated forcefully in a firm's anti-fraud policy statement – were viewed as significant deterrents. This was particularly the case for staff fraudsters, who stood to lose not only lost their jobs but also their pension rights, if caught.

In June 2004, a PA at a large investment bank, was jailed for seven years for stealing £4.3m by forging cheques on her bosses' bank accounts. She had been given considerable freedom to make out cheques for paying their business and personal expenses and abused their trust to transfer money to her own accounts and spend it on luxury cars, villas and designer jewellery over a period of nearly two years.

94. As e-fraud threats are becoming more and more sophisticated, with fraudsters hiding behind many computers and operating out of foreign jurisdictions (most hacking originates from Eastern Europe and Russia and very little is sourced from the UK), the task of investigating these attacks and even determining their source is becoming more difficult for fraud investigators. Without an audit trail linking the fraud incident to the point where the firm's systems or controls were originally compromised, for example the place where customer details were initially obtained, investigators are unlikely to make much progress.

95. We observed, following suspected incidents of fraud, Corporate Audit at one firm frequently performed 'post mortems' to identify and analyse root causes and develop actions to reduce the possibility of recurrence. These findings were frequently reported to senior management.

External Liaison & Communication

96. In addition to the fraud data sharing work carried out by several trade associations (see paragraphs 38-39 above), we found that there was much useful dialogue between firms in the bank, building society, fund management and insurance sectors to share both anti-fraud best practice and relevant information. This dialogue took place by several different means: through various fraud steering groups and committees established by APACS, the BBA, BSA, ABI and IMA; through bodies like the North East Fraud Forum and its counterpart in the South West; and through informal networks of CEOs, Heads of Internal Audit, Fraud Managers and Risk Officers.

97. However, the variety of channels through which fraud issues could be discussed and taken forward was also seen by some as an inefficient structure that meant progress in taking forward initiatives was too slow. The lead on anti-fraud initiatives taken by APACS (see below) was universally welcomed as an example of a measure that would 'streamline' responsibilities.

98. The APACS Council has stated that fraud is now a major issue. The increased priority being given to this risk by the banking industry is evident from the work of the APACS Fraud Control Steering Group (on which the BBA is represented), through which APACS has taken the lead for the banking industry on strategic anti-fraud initiatives for all non-card fraud to add to its existing responsibilities for card fraud. This has helped to simplify anti-fraud responsibilities within the banking industry and, as such, is a welcome response to the criticism that anti-fraud initiatives within the financial services industry lack effective coordination.

99. Various intelligence sharing programmes had also been developed. APACS members had been sharing intelligence on major cases since June 2005 (see paragraph 39 above). Furthermore, we were told that several major banks also provided intelligence to the Metropolitan Police on insider fraud cases. This has allowed the police to identify links between individual cases and to target geographical hot-spots. APACS aims to launch a database which will allow its members to share information on all staff fraud cases. CIFAS is also looking to implement a similar initiative.

100. In addition to initiatives on intelligence sharing, staff fraud and chequebook stockpiling, one of the Fraud Control Steering Group's current projects is to develop a 'dashboard' of high-level industry-wide fraud losses, which APACS hopes to be able to share with third parties including Law Enforcement and the FSA. While retail banking is currently the focus of the group, the intention is to develop closer links with the insurance and other sector bodies. The APACS work does not at this stage go as far as developing formal pictures of best practice. However, as and when the data provided is considered robust, detailed analytical reviews will be undertaken for benchmarking and best practice development.

101. Information sharing initiatives within the building society and insurance sectors, based on agreed common definitions of fraud categories and losses, were progressing well. The BSA has been collecting data on fraud from its members since January 2005. It collects this each quarter to monitor trends, detect emerging problems and provide strategic direction for sector initiatives. The association also shares intelligence via the BSA Financial Crime Prevention Panel and issues updates in the Financial Crime Prevention Manual.

102. The ABI not only provides a useful forum for its members to discuss anti-fraud measures but has also initiated a 'Cheatline'. Operated by an individual ABI member for one year at a time, this took about 200-300 calls in 2005. Much of the information received tends to be low quality, but there have been some big successes too, resulting in significant savings.

103. There had been some significant improvements recently in relations between the financial sector and the police. For example, the North East Fraud Forum had enabled bankers and policemen to get round the table to discuss their 'top 20 gripes'. While the banks recognised the constraints on police, with fraud not in the public eye in the same way as muggings and burglaries, nevertheless there had been some good cooperation. A good example of this is the Dedicated Cheque and Plastic Card Unit in the City Police, which is funded by the financial services industry. Also, Operation Vanguard, an initiative proposed by Kent Police, has been a very positive development. Kent Police proposed sharing - with several major general insurers - information about thefts and burglaries. This has enabled the insurers to fast track the payment of genuine claims, and has provided good publicity for both the Police and the insurance industry. The firms concerned see it as 'a tremendous step' that the initiative came from the police.

Educating Customers

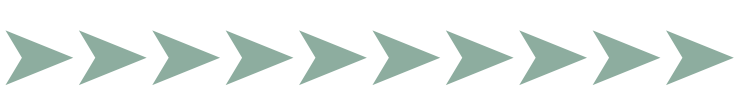
104. As weaknesses in customers' personal computer security are increasingly being exploited by fraudsters as a way of getting access to firms' own systems, customer education and awareness of security issues is becoming more important for the industry as a whole.

105. Firms generally believed that customer education and awareness of fraud risk were vital; however, they did not always appear to be allocating significant resources towards achieving that objective. In one case, a firm's marketing department prevented a fraud risk warning from appearing on that firm's website. The department insisted that the site be used only for marketing purposes and pointed out that the firm benefited from others' activities in raising public awareness of fraud risk.

106. We saw evidence of competing priorities within firms between fraud mitigation and 'customer experience'. There are clearly limits to how far firms are prepared to go in implementing anti-fraud measures if there is a risk of causing inconvenience to customers, for example in relation to internet banking customer authentication. Firms are wary of putting customers off by implementing controls which are more stringent than those of their competitors.

107. One major insurer told us that the risk of publicising the prevalence of insurance fraud was that it might prompt more policyholders to attempt a fraudulent claim themselves. The firm's own approach was to announce on its website that it checked the claims history of anyone making a claim. This was believed to be a more effective anti-fraud message.

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: http://www.fsa.gov.uk



FSA®