

Fraud
Scap
Advisory
Panel

fraud Fighting Fraud:
advisory A Guide
panel for SMEs

Disclaimer

Whilst every effort has been made in the construction of this Guide, compliance with it does not guarantee that you and/or your business will not be a victim of fraud or criminality aimed against your business/PC systems.

The Fraud Advisory Panel and the contributors to this Guide accept no responsibility for any action taken by parties as a result of reading this Guide. Readers are strongly advised to seek and obtain the appropriate professional advice on the issues raised which affect them or their business.

fraud **Fighting Fraud:**
advisory **A Guide**
panel **for SMEs**

Acknowledgements

The Fraud Advisory Panel would like to thank Martin Robinson, Chairman of the Fraud Advisory Panel Education, Events and Training Working Group, Mia Campbell and Janine Aberly (Fraud Advisory Panel), together with Richard Kusnierz (Investigative Data Mining Ltd), Craig Adams (National Audit Office), John Armstrong (Aviva plc), Nathan Dony (Dony Consultants), Harvey Dyson (Square Mile Compliance Ltd), Susan Grossey (Thinking About Crime Ltd), Dominic McKeith (Nottingham University Business School), Gary Miller (Mishcon de Reya), and other members of the Working Group for their assistance in revising this publication. Special thanks also to the original authors of this Guide.

1. Introduction

Managing the risk of fraud should be high on the list of priorities for all businesses. Much has been written about fraud in big business but there is much less advice available to directors and managers of small and medium-sized businesses (SMEs). According to the Department of Trade and Industry (DTI)¹ there were an estimated 4.3 million business enterprises in the United Kingdom at the start of 2004 and 99.3% were small with fewer than 50 employees. Unfortunately, these organisations rarely have the luxury of internal controls and resources, such as internal auditors or human resource departments, which can help during the course of their other work in the fight against fraud.

The Fraud Advisory Panel has produced this Guide to help small and medium-sized businesses manage the risk of fraud. The Guide covers the policies, structures and procedures that a business should have in place if it is to be effective in preventing and detecting fraud.

The Fraud Advisory Panel is a registered charity comprising of volunteers drawn from the public and private sectors. Its role is to raise awareness of the immense social and economic damage caused by fraud and to help the public and private sectors, and the public at large, to fight back.

Anti-fraud strategies have often been inhibited by the difficulty of co-ordinating the wide range of business, professional and public sector responses. The Panel works to overcome these barriers via a robust multi-disciplinary approach.

2. What Is Fraud?

Fraud as a Business Risk

The management of business risk is one of the most important issues facing business. Any risk may be a serious threat to an organisation's well being. Fraud is a real threat to the financial health of an organisation and its image and reputation. Many SMEs fail to recover from fraud and cease trading.

Defining Fraud

In England and Wales there is no precise legal definition of fraud and no single criminal offence that can be called fraud. However, there is a common law offence of fraud in Scotland.

¹ Department of Trade & Industry, Small Business Service 'Statistical Press Release', press release. 25 August 2005.

Fraud is generally considered to involve theft (the removal of cash or assets to which the fraudster is not entitled) or false accounting (the falsification or alteration of accounting records or other documents). Assets include commercially sensitive information and intellectual property which would disadvantage its rightful owner if it were to fall into the hands of, or be sold to, a competitor.

The Fraud Bill currently before parliament defines fraud as:

- fraud by false representation;
- fraud by failing to disclose information; and
- fraud by abuse of position.

This legislation is expected to receive Royal assent in 2006. Its introduction will clarify the definition of fraud and hopefully make it easier to prosecute fraud offences.

Your business may be exposed to:

- **External fraud:** perpetrated by individuals outside the organisation (this includes your business being the target of organised criminals).
- **Internal fraud:** perpetrated by management or employees (within SMEs fraud is often perpetrated by owner managers or majority shareholders).
- **Collusion:** between someone within the organisation and an outsider.

Managing Fraud Risk

You need to understand the potentially damaging consequences of fraud on your business. You can then take steps to reduce the risk by developing an anti-fraud culture across your business, and introduce appropriate policies, controls and procedures. The key aspects of fraud management are:

- **Prevention:** implement a culture, supported by policies and procedures, to prevent your business from becoming a victim.
- **Detection:** implement systems and procedures to detect the early warning signs of fraud taking place. This may include staff training and awareness programmes, whistle-blowers' hotlines, spot audits and data mining.
- **Investigation:** prepare for fraud by having a fraud response plan that is kept up-to-date.
- **Insurance:** review the business's insurance policies such as Fidelity Guarantee Insurance and Directors' and Officers' Liability Insurance to ensure that they are consistent with current business risks. Insurance definitions are:

- (a) *Fidelity Guarantee Insurance (aka Crime Insurance)*: indemnifying and protecting employers against financial loss resulting from acts of dishonesty by employees. There are various types of cover that can be sought depending on the needs of the employer. These include:
- Collective policies: covering named employees for set amounts.
 - Floating policies: covering all employees up to a set limit.
 - Blanket policies: covering all employees in general.
 - Positions policies: provides cover for nominated positions, e.g. accountant, and not the employee by name.
- (b) *Directors' and Officers' Liability Insurance*: indemnifies directors and officers for losses arising from claims made against them by reason of a wrongful act related to their duties.

Identifying Types of Fraud

According to a study published in 2002², the most prevalent types of fraud by employees seem to be ones that impact on profit and loss as a result of **overstating expenses or understating income**. Individually these may be relatively small amounts and are difficult to spot, but when allowed to occur over a long period of time can amount to huge losses. Indications of fraud may exist (changes in cash flow patterns, variations in accounting ratios, stock shrinkage, customer complaints, etc) but these signs often go unrecognised. SMEs can be particularly vulnerable to fraud during a period of rapid expansion when the focus is on building the company and not what may be seen as secondary back office control mechanisms.

The study also suggests that the popularity of **outsourcing** may have widened the threat of fraud. The danger of outsourcing stems from a possible over-reliance on the third party's controls to protect the business's interests.

Family-run businesses may be more vulnerable to fraud committed by the majority shareholder. According to a postal survey conducted by the Federation of Small Businesses³ a number of small businesses have family involvement:

- 50% of respondents indicated shared ownership with a family member (generally a spouse).
- 38% of respondents share management responsibilities with a family member.

² Fraud Advisory Panel (2002) *Indications of fraud in SMEs*, London: Fraud Advisory Panel. Prepared by Dr Andrew Higson, Loughborough University Business School.

³ Federation of Small Businesses (2004) *Lifting the Barriers to Growth in UK Small Businesses: The FSB Biennial Membership Survey 2004*, London: Federation of Small Businesses. Prepared by Professor S Carter, Professor C Mason & Dr S Tagg, University of Strathclyde.

In such cases there may be resistance to accepting the obvious indicators of fraud and a reluctance to face facts and investigate a family member. There should be a mechanism to allow owners/managers to use their independent professional advisors, such as lawyers or accountants, as a 'sounding board' to discuss any concerns they may have. This process may allow an established working practice to be reviewed by an impartial party. Generally, as family businesses grow they employ 'outsiders' and open operations away from the family hub. This introduces new risks that should be carefully considered. The geographical distance between head office and a remote location (shops, distribution centres etc) often directly increases the opportunity for fraud as there may be a corresponding lack of supervision and an increased reliance on external parties. Most fraud includes a breach of trust.

Fraud may also involve the theft of information, such as trade secrets, customer databases and pricelists. Much of this sensitive information is stored on computers. The DTI gives advice on information security management on its website www.dti.gov.uk/industries/information_security. Organisations that consider themselves vulnerable to theft of confidential or sensitive information stored on computers may wish to ensure that:

- there are specific restrictions on IT systems whereby access to confidential information is restricted to specific individuals;
- the IT system is able to track who is accessing what and when;
- computers do not have the ability to copy information to an external or removable device such as memory stick or CDROM; or
- individuals do not have the ability to email large files of sensitive information to themselves at home or to competitors.

The Fraud Advisory Panel has published a specific guide to IT risks *Protecting Your IT Systems: A Guide for SMEs* which is available from their website, www.fraudadvisorypanel.org.

Most importantly you need to consider the business areas where your organisation may be most vulnerable to fraud. An impact risk assessment will quickly identify those areas.

3. Preventing Fraud

Responsibility for Fraud Prevention and Detection

Management has overall responsibility for ensuring the security and integrity of business assets by putting appropriate controls and review procedures in place. Management may in turn designate one person or department with specific responsibility for managing fraud prevention and detection. However, for your business to be effective in countering the threat of fraud, **everybody working within the business must take responsibility for the prevention and detection of fraud.**

There should be a visible, consistent, top-down approach to fraud prevention and detection together with a similar attitude to business ethics and professionalism. If the owners, majority shareholders and senior managers of a business give the impression that there are two sets of standards, then employees will have no loyalty to the company and fraud may become a problem.

Management has a responsibility to protect its business and employees. This includes a 'duty of care' to ensure its employees are not put in a position where they could be compromised by accepting inappropriate gifts or inducements. As part of its anti-fraud policies and procedures, your company should have a clear policy on the acceptance and giving of gifts and should maintain a hospitality register. Every business will have a different threshold for defining what is an unacceptable gift. This should be clearly documented and the policy should be circulated to employees, suppliers and clients.

Establishing Anti-Fraud Standards

The objective for every organisation should be to establish an anti-fraud culture covering working practices and business ethics culminating in formally documented procedures. However in small start-up companies where the focus is on growth and sales such documentation may be a low priority.

As a starting point clear fraud statements should be included in every employee's standard contract of employment setting out the minimum expectations of generally accepted business practices. This should cover the organisations response to theft, unauthorised business expenditure and use of assets.

A formal fraud policy statement indicates that the fight against fraud is endorsed and supported at the most senior level within your business. Organisations may wish to ensure all employees are aware of a zero-tolerance attitude to criminal breaches of business practices which may be reported to the police. The fraud policy statement should be communicated to all employees, contractors and suppliers.

A fraud policy statement should be simple, focused and easily understood. The content may vary from business-to-business but you should consider including the business's determination to:

- take appropriate measures to deter fraud;
- introduce/maintain necessary procedures to detect fraud;
- investigate all instances of suspected fraud;
- report all suspected fraud to the appropriate authorities;
- assist the police in the investigation and prosecution of suspected fraudsters;
- recover wrongfully obtained assets from fraudsters; and
- encourage employees to report any suspicion of fraud.

You may also wish to include the following:

- the allocation of responsibilities for the overall management of fraud; and
- procedures to be followed if a fraud is suspected.

A fraud policy statement should make clear that all employees have a responsibility for fraud prevention and detection. It is important the statement be actively and regularly promoted throughout the organisation to all employees, irrespective of grade, position or length of service. Examples of fraud policy statements may be found on the Fraud Advisory Panel website www.fraudadvisorypanel.org.

Managing the Prevention, Detection and Prosecution of Fraud

The management of fraud prevention should be integrated into the overall management programme rather than dealt with in isolation. Your anti-fraud controls should be designed to fit with the particular activities and circumstances of your business.

Organisations experiencing rapid expansion and diversification should regularly review fraud policies and conduct risk assessments to ensure that adequate controls are in place.

Key elements of fraud prevention may include:

- undertaking a comprehensive fraud risk assessment;
 - identify areas within the business most vulnerable to fraud
 - establish what processes are in place already

- identify extra or alternative controls needed to reduce the risk
- introduce these extra or alternative controls
- monitor the controls to check that they are in operation
- regularly assessing the effectiveness of the controls, particularly taking into account changing circumstances in the organisation; and
- ensuring that your strategy and procedures are workable and practical, supported by appropriate resources and regularly reviewed.

If your business is a financial services organisation regulated by the Financial Services Authority (FSA) you already have many obligations, including those related to anti-money-laundering systems and procedures. Your anti-fraud controls should link into those existing systems and procedures.

Case Study 1

A manufacturer and distributor of electronic products failed to implement adequate stock controls and audit procedures in its product repair shops. As a consequence, a senior member of the repair shop team was able to requisition original product spare parts over a number of years and replicate a repair shop environment in his home.



The losses over a 10-year period exceeded £1 million and could have been avoided through more efficient stock controls and audit procedures.

Case Study 2

A medium-sized travel company provided a refund cheque for £10 to a customer. This was intercepted in the post-room and fraudulently altered by amending the amount details to “£10,000” and altering the name of the payee. The company was alerted to the attempted fraud by the vigilance of their bankers. Following additional enquiries, it became clear the attempted fraud was part of a wider ring of organised fraud where refund cheques for small values were being altered in an attempt to secure higher amounts.



Generally an organisation should ensure that any outgoing post does not obviously contain cheques or other financial instruments. In this particular case, increased pre-employment screening and supervision within the post-room reduced the opportunity of cheques being intercepted in future.

Recruitment and Ongoing Personnel Guidelines

Unfortunately most fraud experienced by businesses is committed by its own staff. It is important to have an effective recruitment process designed to deter and prevent fraudsters seeking employment, and a system of personnel management designed to deter existing staff from committing fraud.

Your recruitment process must require that references be thoroughly checked and assessed. Temporary staff should be vetted as thoroughly as permanent staff, particularly in vulnerable areas such as finance. You should consider the need for further vetting or screening as employees are promoted, moved to higher risk/sensitive posts or gain access to privileged information. This can be helped by having a clear job application form requesting information that can be independently validated. Some CVs may contain false references, unexplained gaps and/or employment stretched to cover gaps. The job application form should be the starting point for validating the information provided by the prospective employee.

Recruitment agencies have a vested interest in placing employees. Consequently it is important to ensure that any arrangements with recruitment agencies include provision whereby:

- a) the agency will procure the applicant's consent that all information provided by the applicant can be passed onto the prospective employer; and
- b) obliges the agency to pass these details onto the prospective employer.


Ensure all contracts of employment have specific consents for:

- a) monitoring email and telephones for security and prevention and detection of crime (also check registration under the Data Protection Act);
- b) clear guidelines for the use of confidential and personal information;
- c) clear post-contract obligations such as returning all company property and the use of any company information; and
- d) the retention and recovery of pensions or bonus and incentive payments where fraud has been involved.

Consider having a consistent policy for the declaration of conflicts of interest. Depending on the business, all employees should positively declare that they and their immediate family (parents, in-laws, partners and children) have no commercial interest in clients, suppliers or competitors. It may be appropriate to have this declaration re-affirmed on an annual basis.


Case Study 3

A finance house needed an extra junior accountant for a short period of time. The company went to a reputable agency and employed an appropriately qualified person. The company relied on the agency's screening policy which had failed to uncover a series of discrepancies in the accountant's personal history, including a false address. The accountant removed a company chequebook from his work place and used it to make a series of high value purchases on his own behalf. The matter came to light when a routine enquiry was made with the finance house to verify the issue of one of the cheques. By this time the temporary accountant had left the company. He could not be traced and the matter was referred to the police.

 Don't rely on the recruitment agency's screening process. Every organisation should undertake some internal vetting of applicants. Access to chequebooks and manual cheques should be restricted to authorised personnel and kept securely stored when not in use. Such documents should be independently audited.

Case Study 4

An organisation employed a temporary accounts clerk to work in their shared service accounting centre. The organisation assumed the recruitment agency would perform adequate checks on the clerk's background. This did not happen. The clerk was able to use his access to the accounting system to divert supplier payments to his own bank account. After a week of such diversions, he left the company with over £150,000.

 Don't rely on the recruitment agency's screening process. An audit trail of changes to supplier's banking details should be reviewed independently of the department making the changes.

Implementing a Fraud Prevention Education/Training Programme

All new employees should be given a copy of the business's fraud policy statement. Fraud prevention and detection information should be included in your induction programmes and in continuous career training.

Reviewing Your Fraud Policy

Organisational structures are constantly changing. A control system which may have been effective on its introduction may no longer fit readily with the latest company structure or meet the organisation's changing circumstances or needs. Regular review is essential to ensure your systems still meet the current needs of your business, and that they address the risks facing your business today.

A Fraud Checklist for Directors and Senior Managers

Does your business:

- Treat fraud as a business risk?
- Identify the types of fraud to which it is most exposed?
- Ensure that at least one person or department is specifically identified as responsible for managing fraud risk?
- Make clear to all employees that fraud prevention and detection is the responsibility of everyone in the business?
- Have, and actively promote, a fraud policy statement?
- Have a strategy and procedures for managing the prevention, detection, investigation and prosecution of fraud?
- Have a fraud prevention education/training programme?
- Have a plan of action in the event that a fraud is detected?
- Have a clear whistle-blowing policy?
- Have recruitment and ongoing personnel policies that address the risk of fraud?
- Check that your fraud policies and procedures are complied with?
- Ensure that your fraud policies and procedures are regularly reviewed?

4. Detecting and Investigating Fraud

What to do When a Fraud is Detected

However comprehensive your fraud prevention controls may be, a determined and skilled fraudster may find a way around them. You need to have a contingency plan prepared in the event that a suspected fraud is uncovered. The scope and scale of this fraud response plan will depend, to a large degree, on the nature and size of your business.

Matters to consider for inclusion in a fraud response plan:

- Skills available in-house and contacts for external expertise such as specialist fraud investigators.
- Who will lead the investigation?
- When to obtain legal privilege and protection by instructing a criminal lawyer.
- When to inform the business's insurance carrier.
- How to investigate a suspected fraud.
- Ensure that policies exist to allow your business to use legitimate investigation techniques such as desk searches, covert interception of telephone conversations, use of CCTV surveillance, review of email and other forms of electronic communication, forensic imaging of computer and other electronic equipment (PDA, mobile telephones etc) and data mining.
- How to mitigate the threat of further fraud and the lessons learnt for improved controls.
- How to secure evidence without alerting the suspected fraudster at the outset.
- How to deal with suspects.
- How/when to involve the police.
- Public relations implications.

Your business's fraud response plan should be seen as a part of a much wider disaster recovery plan. It should be kept under constant review and regularly tested.

Enabling Employees to Report Fraud

As part of establishing an anti-fraud culture in your business you should make clear to all employees that whistle-blowing is an essential element in the fight against fraud.

According to the website for Public Concern at Work www.pcaw.co.uk, "Someone blows the whistle when they tell their employer, a regulator, customers, the police or the media about a dangerous or illegal activity that they are aware of through their work. Whistle-blowing can inform those who need to know about health and safety risks, potential environmental problems, fraud, corruption, deficiencies in the care of vulnerable people, cover-ups and many other problems. Often it is only through whistle-blowing that this information comes to light and can be addressed before real damage is done."


You should make it as simple and straightforward as possible for employees to report a suspected fraud and all employees should be aware of the fraud reporting lines. In a family-run business this may be difficult, but the business's solicitor or accountant could perhaps be called on to act as an independent third party. This should be discussed with the professional advisor and formally documented. You may wish to set up an internal, or external, fraud hotline that is willing to accept anonymous calls, or you may want employees to report fraud to their line manager. In this case though it should be possible for employees to by-pass their immediate line manager if they suspect that manager's involvement in fraud. Whatever fraud reporting mechanism you introduce, employees should be reassured that all reports will be treated confidentially. Where a report of a suspicion of fraud is made in good faith, the employee making the report is now normally protected in law under the Public Interest Disclosure Act 1998.

Complying with Fraud Policies and Procedures

Any system of controls can only be effective if the prescribed processes and procedures are complied with at all times throughout the business. Over time, controls can be eroded as short cuts are introduced or processes unofficially changed to meet new circumstances or dropped without approval. You should make sure regular checks are undertaken to confirm all the necessary controls are in operation throughout the business and remain effective, particularly taking changes in the business into account.

Case Study 5


A company involved in international trade where large amounts of cash were exchanged, allowed one senior manager to withdraw cash with sole authority. As a consequence, the manager was able to fraudulently withdraw small amounts of cash over a period of months without the withdrawals being spotted. In total, the manager stole over £80,000 from his company. An internal investigation and enquiry revealed that at least two signatures should have been required to withdraw cash and that there had been a complete failure of internal controls and procedures.

-  Organisations should review their mandate with their bank to ensure compliance. A risk assessment should identify high risk areas where a segregation of duties would reduce the opportunity for a single person to commit a fraud.

Case Study 6


A company nominated a single individual to deal with final salary adjustments for terminated employees. This individual controlled a cheque book to make final salary and expense payments. All cheques required a counter signature and the individual prepared a spreadsheet to document all such payments. Bank reconciliations took place on a regular basis and were performed by another department. Internal audit was satisfied the process was adequately controlled. The individual stole several million pounds over a number of years by circumventing the system. The mechanism involved:

- never letting anyone audit the cheque book or reconcile cheque stubs to the spreadsheet;
- making cheques to bogus employees;
- forging the second signature;
- altering the spreadsheet to reflect payments to real employees who were leaving; and
- preventing any detailed questioning about the large payments on the grounds of “privacy and the Data Protection Act”.

-  Always reconcile payments to employees and third parties against the original instructions. In this case a review of the cheque stub would have revealed the fraud.

Case Study 7

A long established family firm that had grown through four generations into a large company employed a chief accountant who stole over £300,000. Although the money was eventually recovered, the company went out of business with the loss of over 30 jobs.

 The board should regularly receive and review management accounts. In this case monthly financial reporting (versus quarterly) would have identified this fraud earlier.

5. Conclusion

Fraud is a major threat to any business but there are steps that can be taken to minimise the risks. A business that is **alert** to the risks, takes steps to put in place **appropriate controls and procedures**, **monitors** the operation of these controls and their ongoing effectiveness and maintains an **anti-fraud culture** will be better placed to deter, prevent, and at worst, detect fraud. Implementing these measures will help protect a business's bottom line, its image and its reputation.

Taking the fraud risk seriously can save your business

Indicators of Fraud Checklist

Possible behavioural indicators of fraud may include:

- Increased levels of stress without high workload
- Personal problems that cannot be shared
- Lifestyle not commensurate with income
- Reluctance to take annual holidays
- Personal financial problems
- Employees who always bend rules
- Employees subject to complaints
- Staff who work late
- Staff who refuse promotion
- New staff resigning quickly

Possible financial indicators of fraud may include:

- Cash only transactions
- Large variation in expenses between sites
- Poorly reconciled cash expenses
- Poorly reconciled customer accounts
- Customer complaints
- Rising costs with no explanation or that are not commensurate with an increase in revenue
- Large volume of cash refunds to customers

Useful Links

Association of British Insurers

www.abi.org.uk

British Bankers Association

www.bba.org.uk

CIFAS – the UK’s Fraud Prevention Service

www.cifas.org.uk

City of London Police

www.cityoflondon.police.uk

Companies House

www.companieshouse.gov.uk

Crimestoppers

www.crimestoppers.co.uk

Department of Trade and Industry

www.dti.gov.uk

Federation of Small Businesses

www.fsb.org.uk

Financial Services Authority

www.fsa.gov.uk

Fraud Advisory Panel

www.fraudadvisorypanel.org

Home Office

www.homeoffice.gov.uk

Information Commissioner’s Office

www.informationcommissioner.gov.uk

Law Society of England & Wales

www.lawsociety.org.uk

Law Society of Scotland

www.lawscot.org.uk

Metropolitan Police Service

www.met.police.uk

National Audit Office

www.nao.gov.uk

National Criminal Intelligence Service

www.ncis.gov.uk

North East Fraud Forum

www.northeastfraudforum.co.uk

Public Concern At Work

www.pcaw.co.uk

Serious Fraud Office

www.sfo.gov.uk

For more information on the Fraud Advisory Panel please contact:

Fraud Advisory Panel

Chartered Accountants' Hall, PO Box 433, Moorgate Place, London EC2P 2BJ

Tel: 020 7920 8721

Fax: 020 7920 8545

Email: info@fraudadvisorypanel.org

Or visit:

www.fraudadvisorypanel.org

Registered Charity No. 1108863

February 2006