

Fraud hotspots in smaller businesses

Small and medium-sized businesses (SMEs) are particularly vulnerable to fraud in times of economic downturn; many lack the controls found in larger organisations and do not necessarily have the resources to combat certain types of fraud. This factsheet highlights some of the key areas of fraud risk.

What is fraud?

The term 'fraud' is commonly used to describe the use of deception to deprive, disadvantage or cause loss to another person or party. This can include theft, the misuse of funds or other resources, or more complicated crimes such as false accounting and the supply of false information.

Individuals can be prosecuted under the Fraud Act 2006 if they make a false representation, fail to disclose information or abuse their position.

Areas of fraud risk

All types and sizes of businesses are vulnerable to fraud. Smaller businesses can be susceptible to a very broad range of fraud risks and a small workforce can mean that it is difficult to segregate duties.

Fraud can be committed by employees (sometimes called 'internal fraud' or 'employee fraud'), third parties (such as suppliers and customers) and even by business owners themselves. Some of the most common fraud 'hotspots' are summarised below.

Customers

Card fraud: A fraudster pretends to be a legitimate customer and purchases goods using a stolen credit or debit card.

Non-deliveries: Customers falsely claim that goods dispatched from an online retailer have not been received.

Refunds: Customers steal goods from a retail outlet and then return the goods for a cash refund.

Employees

False or inflated supplier invoices:

Employees authorise payments for over-priced and/or non-existent goods or services and receive a 'kickback' (such as a cash payment) in return from the supplier.

This is particularly noticeable in the property management sector where service charges are calculated on a cost plus percentage mark-up basis.

Fictitious refunds or returns: Employees generate false refunds and either steal the cash value from the till or arrange for the amounts to be refunded directly to their personal credit card or bank account. Retailers are particularly susceptible to this type of fraud.

Ghost employees or contractors: Fictitious employees and/or contractors are added to the business' payroll and are paid wages and/or expenses.

Misappropriation of assets: Employees help themselves to cash, stock, IT equipment such as laptops, and stationery or submit false expense claims.

Theft or supply of confidential information: Employees steal confidential customer and/or client information and use it for fraudulent purposes.

Suppliers

False or inflated invoices: Suppliers invoice for more goods or services than were delivered or supplied, or invoice at a higher price than originally quoted. This may involve collusion with an employee to ensure that payments are authorised.

Long firm fraud: A business is set up with the purpose to defraud other legitimate businesses.

Property management: Over-charging by management companies using fictitious time records.

Other third parties

Corporate identity fraud: A fraudster sets up a false company to trade or steals an organisation's identity and/or financial information and uses it to purchase goods and services, obtain information or to access facilities in that organisation's name.

See our separate factsheet *Corporate Identity Fraud* for more information.

Online banking fraud: A fraudster gains access to the business' online bank account and manipulates funds such as setting up standing order payments to his/her own bank account. Businesses that do not have adequate firewall protection are particularly vulnerable to this type of fraud.

Fraud warning signs

There are a number of warning signs that can indicate that fraud may be occurring within your business. These include:

- Changes in employee behaviour
- Changes in cash flow
- Stock shrinkage
- Customer complaints
- High turnover of staff
- Computer and network problems

A full checklist is provided at the end of this factsheet.

Managing the risk of fraud

Your business can take a number of steps to reduce the risk of becoming a victim of fraud. The key elements of fraud risk management are:

Prevention

- Establish an ethical business culture. Develop an anti-fraud policy that clearly sets out the minimum standards of behaviour expected of employees (acceptance of gifts, use of assets, response to theft etc) and lead by example.
- Minimise the opportunities for fraud to occur within your business. Review your business activities; identify the areas most at risk to fraud and introduce controls to prevent it. These might include segregating finance duties, implementing authorisation thresholds, conducting

reference checks on new employees (see our separate factsheet *Pre-Employment Screening* for more information), and introducing IT systems access controls. Controls do not need to be complicated or expensive.

Detection

- Be aware of the indicators of fraud. Introduce procedures to detect the early warning signs that fraud is taking place. These might include educating staff to spot common frauds and scams, introducing a reporting hotline, conducting spot audits (of stock, sales and purchase ledgers etc) and reviewing profit and loss accounts on a regular basis.

Investigation

- Make sure you are prepared to respond to a fraud being discovered within your business. Smaller businesses should consider a policy that independent professional advice will be sought at the outset of any fraud investigation. Larger organisations should include fraud as part of their disaster recovery plan. This should cover the investigation process (who, when and how), legal or ethical duties to report (to your shareholders, customers, bank, insurance company and/or regulator(s)) and public relations.
- It is important to remember that there are different standards of proof that need to be met according to the type of action you wish to take against the fraudster – disciplinary, regulatory, civil or criminal.

Insurance

- Consider the need for fidelity or crime protection and/or directors' and officers' liability insurance.

Review

- Business practices and activities change over time. Regularly review the systems, processes and controls you have in place to manage the risk of fraud to ensure that they remain current, relevant and appropriate for your business' needs.

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.
Registered Charity No. 1108863

Disclaimer

Dissemination of the contents of this Fraud Fact Sheet is encouraged. Please give full acknowledgement of the source when reproducing extracts in other published works. Whilst every effort has been made in the construction of this Fraud Fact Sheet, compliance with it does not guarantee that you and/or your business will not be a victim of fraud or criminality aimed against you and/or your business. The Fraud Advisory Panel and the contributors to this Fraud Fact Sheet accept no responsibility for any action taken by parties as a result of any view expressed herein. Readers are strongly advised to seek and obtain the appropriate professional advice on the issues raised which affect them or their business.

© Fraud Advisory Panel, 2009

Indicators of fraud checklist

There are a number of behavioural and financial warning signs that can indicate that there may be a problem within your business. These should not be taken as definitive proof that there is a fraud; some employees will display one or more of these characteristics and be completely honest and trustworthy; others may display none but may be dishonest.

Employee behaviour:

- Increased levels of stress without a high workload
- Lifestyle not commensurate with salary
- Reluctant to take annual holidays
- Personal financial problems
- Tends to bend/break the rules
- Tends to be subject to complaints
- Works late or unusual hours
- Is unwilling to delegate
- Refuses promotion
- Cosy relationship with contractors and/or suppliers
- New staff resign quickly

Financial:

- Cash only transactions
- Large variation in expenses between offices/outlets
- 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 refunds to customers
- Unusually large inventories

What to do if your business suffers a fraud

Three steps that you should take are:

1. Report the matter to the police and other relevant organisations immediately. Depending upon the type of fraud this could include your bank, insurance company, suppliers and/or customers.
2. Consider seeking specialist professional advice.
3. Reassess the way your organisation conducts and manages its business to ensure it is adequately protected against this type of fraud occurring in future.

Further information

Business Link

www.businesslink.gov.uk

Card Watch

www.cardwatch.org.uk

Companies House

www.companieshouse.gov.uk

Federation of Small Businesses

www.fsb.org.uk

Fraud Advisory Panel

www.fraudadvisorypanel.org

Get Safe Online

www.getsafeonline.org

Identity Theft

www.identitytheft.org.uk

Information Commissioner's Office

www.ico.gov.uk

The Fraud Advisory Panel gratefully acknowledges the contribution of Graham Salmon (Beever and Struthers), Sanjay Mackintosh and Mia Campbell in the preparation of this Fraud Fact Sheet.

Distributed by